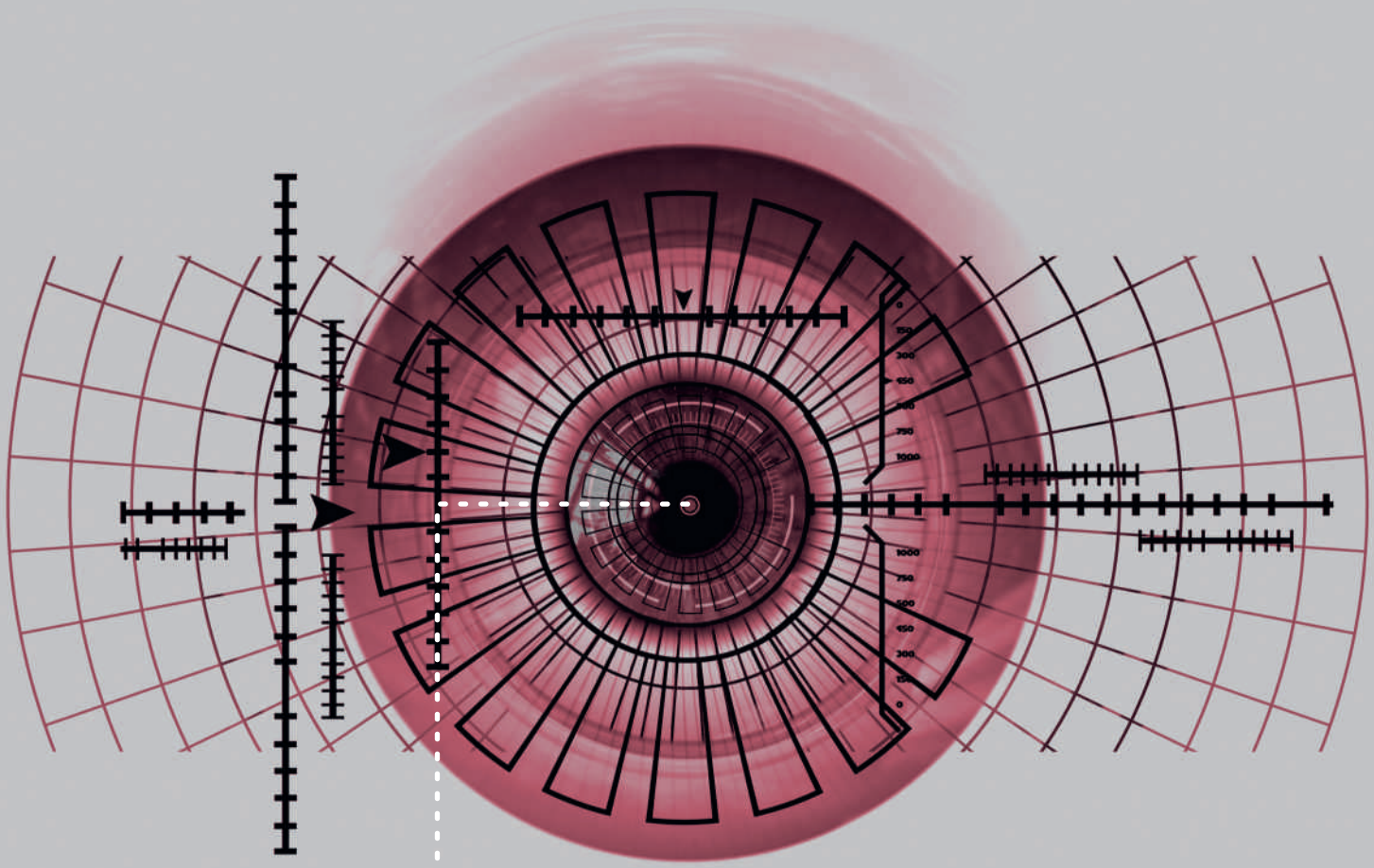


Tätigkeitsbericht 2022

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

Es ist bedenklich, dass kaum jemand weiß, welche Daten über ihn gespeichert sind. Es ist äußerst bedenklich, dass kaum jemand weiß, wer diese Daten gerade besitzt. Bedenklich ist es hingegen nicht, dass sich nur eine Minderheit dagegen wehrt. Das ist dramatisch.

Götz Hamann, Marcus Rohwetter, DIE ZEIT, 48/2004

7. Tätigkeitsbericht des Diözesandatenschutzbeauftragten

für

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

Berichtszeitraum 01.01.2022 bis 31.12.2022

Inhaltsverzeichnis

Inhaltsverzeichnis 1

Vorwort 5

1. Entwicklung des Datenschutzes 7

1.1 Entwicklung des Datenschutzes in Europa 7

1.1.1 Kündigungsschutz für betriebliche Datenschutzbeauftragte europarechtskonform 7

1.1.2 Zwangsweise Abgabe der Fingerabdrücke kommt vor den EuGH 9

1.2 Entwicklung des Datenschutzes in der Bundesrepublik 10

1.2.1 Änderung des Personenstandsgesetzes 10

1.2.2 Datenschutzkonformer Online Handel 13

1.2.3 Facebook Fanpages – weiterhin keine wirksame Rechtsgrundlage 14

1.2.4 EuGH Entscheidung über Vorratsdatenspeicherung in Deutschland 16

1.2.5 Nachlässiger Umgang mit Datenschutzvorschriften rechtfertigen Kündigung 17

1.2.6 Entscheidung zur Unzulässigkeit von Cloud- und IT-Dienstleistungen durch US-Tochterunternehmen in Deutschland – Vergabekommission 18

1.2.7 Arbeitsgericht Neuruppin verpflichtet Unternehmen zu Schadenersatz 20

1.2.8 Anschrift ohne Namen ist kein personenbezogenes Datum 21

1.3 Entwicklung des Datenschutzes in der Kirche (kirchlichen Einrichtungen) 22

1.3.1 „Nun sag`, wie hast du`s mit der Religion." 22

1.3.2 Datenschutzrisiko Pfarrbrief 23

2 Datenschutz allgemein 26

2.1 Datenerhebung beim Zensus 2022 ist rechtmäßig 26

2.2 Zugriff auf Sozialdaten im Ermittlungsverfahren 27

2.3 Assistenzsysteme im Fahrzeug – Ereignisbezogene Datenspeicherung 29

2.4 Datenschutz beim E-Rezept noch nicht ausreichend 31

3 Datenschutzaufsicht 33

3.1 Und immer wieder lässiger Umgang mit E-Mail-Adressen 33

3.2 Prüfaktionen der Datenschutzaufsicht 35

3.2.1 Querschnittsprüfungen Pfarreien 35

3.2.2 Caritas Regionalzentrum 38

3.2.3 Prüfung eines Seniorenzentrums 39
3.2.4 Benennung von betrieblichen Datenschutzbeauftragten in Kindertagesstätten 46
3.2.5 Datenschutzkontrolle im Kindergarten 50
3.3 Datenschutzvorfälle 53
3.3.1 Abschiedsmail im großen Stil 53
3.3.2 Bekannte aus früheren Zeiten 54
4 Datenschutz im Gesundheitswesen 54
4.1 Datentransparenzverfahren - Gesundheitsdaten in der Forschung 54
4.2 Die elektronische Arbeitsunfähigkeitsbescheinigung – was ist datenschutzrechtlich zu beachten? 58
4.3 Datenschutzvorfälle 60
4.3.1 Vermeintliche Kindswohlgefährdung / offensichtlich übers Ziel hinausgeschossen 60
4.3.2 Falsch versandte Patientenunterlagen – ein Dauerbrenner 68
4.3.3 SOS aus der Notaufnahme – E-Mail mit Patientendaten an alle Mitarbeiter 69
4.3.4 Neugierige Kollegen und der Datenschutz 70
4.3.5 Screenshot einer Pflegeakte als Statusmeldung 72
4.3.6 Fotos und Videoaufnahmen von Bewohnern 73
5 Datenschutz in Kita und Schule 73
5.1 Bundesverfassungsgericht bestätigt Masern-Impfpflicht 73
5.2 Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten in Kitas 75
5.3 Datenschutzvorfälle 77
5.3.1 Offenlegung von Daten – ein altbekanntes Thema 77
5.3.2 Sicherheitsrisiko Lernplattform - Namen der Schüler anstatt des Protokolls 78
5.3.3 Schulhilfekonferenz im Klassenverteiler 79
5.3.4 Unzensierte Jahrbücher 80
5.3.5 Aus gesundheitlichen Gründen nicht im Dienst 81
6 Datenschutz im Beschäftigungsverhältnis 82
6.1 Schutzkonzept und erweitertes Führungszeugnis 82
6.2 Anwendbarkeit des KDG im Beschäftigungskontext 83
6.3 Nebentätigkeitsgenehmigung und Datenschutz 85

6.4 Abbildungen von Beschäftigten – immer wieder ein Problem 87
6.5 Kündigung von Menschen mit Behinderung während der Probezeit 89
6.6 Datenschutz nur solange es keine Arbeit macht? 90
7 Technischer Datenschutz 92
7.1 Unterschied zwischen Authentisierung, Authentifizierung und Autorisierung 92
7.2 Microsoft 365 und Windows 94
7.2.1 Einsatz von Microsoft 365 – noch immer nicht ausreichend 94
7.2.2 BSI – Telemetrie-Komponente in Windows 95
7.3 Aus den sozialen Medien 96
7.3.1 Ich bin nicht bei WhatsApp, Instagram – oder doch? 96
7.3.2 Meta hat Apps identifiziert, die Facebook Zugangsdaten ausspionieren 97
7.4 Website – Vorbeugen vor Abmahnung 98
7.4.1 Abmahnwelle im Fall Google-Fonts 98
7.4.2 Website Überprüfungen und Selbstcheck 100
7.5 Schöne neue HR-Welt: Robot Recruiting und die rechtlichen Grenzen 101
7.6 Keine Daten – kein Datenschutzvorfall 103
7.6.1 Unlesbare Daten – nicht datenschutzrelevant 104
7.6.2 Schutz durch Datenverschlüsselung 104
7.6.3 Einfach und wirkungsvoll mit Windowsmitteln 105
Die Kirchliche Datenschutzaufsicht Ost 111
Öffentlichkeitsarbeit 112
Anhang 114
Microsoft Versionsinformationen 114
Abkürzungen 115

Vorwort

An der Technischen Universität Braunschweig haben zwei Psychologinnen eine Studie zum Thema Datenschutz in Unternehmen durchgeführt. Diese Studie sollte u. a. die Kenntnis von datenschutzrechtlichen Vorschriften und ihre Akzeptanz beleuchten.

Je häufiger die Befragten die Möglichkeit erhielten, an Datenschutzschulungen teilzunehmen, desto höher schätzten sie ihre Kenntnisse im Umgang mit personenbezogenen Daten ein. Jedoch ergab die Befragung auch, dass mit zunehmender Kenntnis die Akzeptanz datenschutzrechtlicher Vorschriften nicht steigt. Die Bereitschaft, sich an Regeln zu halten, war bei den Beschäftigten grundsätzlich hoch, sie sank aber dann, wenn Regelungen nicht verstanden oder nachvollzogen werden konnten.

Erschließt sich den Betroffenen der Sinn von Gesetzen nicht, werden Vorschriften nur als eine Einschränkung von Freiheiten empfunden und es tritt der gegenteilige Effekt ein. Die Normadressaten versuchen dann diese Einschränkung zu ignorieren oder sogar gegen sie anzuarbeiten.

Schulungen müssen also nicht nur Kenntnisse, sondern vor allem Verständnis vermitteln.

Als weiteres Hemmnis Regelungen umzusetzen, hat sich ein ambivalentes Verhalten von Vorgesetzten in Bezug auf datenschutzrechtliche Regelungen erwiesen. Das betrifft sowohl das Leitungspersonal, welches auf die Datenschutzgesetze mit einem Augenzwinkern und vielleicht dem Hinweis, dass alles nicht so heiß gegessen wird, wie es gekocht wird, hinweist, als auch die Vorgesetzten, die Beschäftigten Informationen mit dem Hinweis auf datenschutzrechtliche Verpflichtungen vorenthalten.

Datenschutz kann nur funktionieren, wenn verstanden wird, dass Datenschutz nicht Daten schützt, sondern Menschen und Persönlichkeitsrechte. Dafür ist es erforderlich in Schulungen nicht nur Rechtskenntnisse darzustellen, sondern den Sinn und Zweck der Vorschriften durch lebensnahe Beispiele zu vermitteln.

Unsere Behörde möchte diesem Anspruch gerecht werden. Deshalb haben wir auch im vergangenen Jahr auf unserer Homepage umfangreich und

aktuell datenschutzrechtliche Themen besprochen und zu Videosprechstunden eingeladen. Neu eingeführt haben wir offene Veranstaltungen, bei denen die Fachreferenten vor Ort in Präsenz Haupt- und Ehrenamtlichen sowie allen Interessierten für Datenschutzfragen und -beratungen zur Verfügung standen.

Diese Aktivitäten verdeutlichen unsere Einstellung zur Aufgabe einer Datenschutzaufsicht. Wir verstehen uns nicht nur als Strafverfolger, nachdem es zu Datenschutzverstößen gekommen ist, sondern arbeiten durch gezielte Prävention daran, die Verletzung von Persönlichkeitsrechten zu verhindern.

So möchten wir diesen Bericht vornehmlich als Informationsmittel verstanden wissen.

1 Entwicklung des Datenschutzes

1.1 Entwicklung des Datenschutzes in Europa

1.1.1 Kündigungsschutz für betriebliche Datenschutzbeauftragte europarechtskonform

Der Europäische Gerichtshof (EuGH) erklärt den besonderen Kündigungsschutz für interne betriebliche Datenschutzbeauftragte nach dem Bundesdatenschutzgesetz (BDSG) für europarechtskonform.

Das Bundesarbeitsgericht (BAG) hat mit einem Vorlagebeschluss vom 27.04.2021 (Az. 9 AZR 383/19 A) dem EuGH die Frage vorgelegt, ob der in § 38 Abs. 2 BDSG verankerte besondere Kündigungsschutz für betriebliche Datenschutzbeauftragte mit der Datenschutzgrundverordnung zu vereinbaren ist.

Nach Art. 38 Abs. 3 S. 2 DS-GVO darf der Datenschutzbeauftragte vom Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.

Die nationale Regelung im BDSG ist demgegenüber deutlich weiter gefasst. Nach § 38 Abs. 2 BDSG i.V.m. § 6 Abs. 4 BDSG ist die Kündigung eines internen Datenschutzbeauftragten nur dann möglich, wenn der Arbeitgeber zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist (§ 626 BGB) berechtigt ist. Nach den Regelungen des BDSG ist also eine ordentliche betriebsbedingte Kündigung ausgeschlossen. In diesem Zusammenhang ist es unerheblich, ob der Grund für die Kündigung wegen der Erfüllung der Aufgaben als betrieblicher Datenschutzbeauftragter erfolgt oder aus anderen Gründen.

Die DS-GVO will durch Harmonisierung der nationalen Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten den freien Verkehr dieser Daten zwischen Mitgliedstaaten sicherstellen. Wegen dieses Vollharmonisierungsgedankens könnten nach der Rechtsprechung des EuGHs auch verschärfende nationale Regelungen unzulässig sein. Um dies zu klären war der Vorlagenbeschluss des BAG an den EuGH erforderlich.

Der Gerichtshof stellt in seinem Urteil nunmehr aber fest, dass es bei der Festlegung von Vorschriften zum Kündigungsschutz eines bei einem Verantwortlichen oder einem Auftragsverarbeiter beschäftigten Datenschutzbeauftragten weder um den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten noch um den freien Datenverkehr, sondern um Sozialpolitik geht. In diesem Bereich steht es jedem Mitgliedstaat frei, in Ausübung seiner vorbehaltenen Zuständigkeit, besondere, strengere Vorschriften für die arbeitgeberseitige Kündigung eines Datenschutzbeauftragten vorzusehen, sofern diese mit dem Unionsrecht und insbesondere mit den Bestimmungen der DS-GVO, vor allem Art. 38 Abs. 3 Satz 2 DS-GVO, vereinbar sind. Ein strengerer Schutz des betrieblichen Datenschutzbeauftragten ist dementsprechend zulässig, solange die Verwirklichung der Ziele der DS-GVO dadurch nicht beeinträchtigt werden. Dies wäre aber der Fall, wenn dieser Schutz jede durch einen Verantwortlichen oder einen Auftragsverarbeiter ausgesprochene Kündigung eines Datenschutzbeauftragten verböte, der nicht mehr die für die Erfüllung seiner Aufgaben erforderlichen beruflichen Eigenschaften besitzt oder seine Aufgaben nicht im Einklang mit der DS-GVO erfüllt.

Durch den vom EuGH bestätigten Sonderkündigungsschutz des betrieblichen Datenschutzbeauftragten wird dessen Unabhängigkeit erheblich gestärkt. Dies ist gerechtfertigt, weil der interne Datenschutzbeauftragte als Arbeitnehmender in einer wirtschaftlichen Abhängigkeit zur Arbeitgeberin steht.

Will eine Arbeitgeberin eine Einschränkung ihrer Kündigungsmöglichkeiten vermeiden, steht es ihr frei, einen externen Datenschutzbeauftragten zu benennen. Der externe Datenschutzbeauftragte ist kein Beschäftigter des datenschutzrechtlich Verantwortlichen, so dass für ihn der Sonderkündigungsschutz nicht greift.

Auch wenn die Rechtsprechung des EuGHs keine direkte Auswirkung auf das kirchliche Datenschutzrecht (§ 37 Abs. 4 KDG, § 37 Abs. 2 DSG-EKD) hat, stellt das Urteil doch eine Stärkung der dort verankerten inhaltsgleichen Regelungen dar.

1.1.2 Zwangsweise Abgabe der Fingerabdrücke kommt vor den EuGH

Fingerabdrücke abgeben – das verbindet man erst einmal mit einer erkennungsdienstlichen Behandlung nach einer Festnahme wegen des Verdachts einer Straftat. Doch seit dem 2. August 2021 werden alle Bürger behandelt, als wären sie verdächtig:

Wer einen neuen Personalausweis beantragt, muss verpflichtend die Fingerabdrücke beider Zeigefinger scannen und speichern. Die Körpermerkmale werden zusammen mit dem biometrischen Gesichtsbild auf dem RFID-Chip des Dokuments gespeichert. Der Bundestag hatte dies zuvor mit dem Gesetz zur „Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen" beschlossen. Die Verpflichtung für über dreihundert Millionen EU-Bürger, zwei Fingerabdrücke auf dem Ausweis in digitaler Form speichern zu lassen, geht auf die EU-Verordnung 2019/1175 zurück.

Ein Bundesbürger wehrte sich gegen die biometrische Erfassung und reichte unterstützt durch die Datenschutzinitiative Digitalcourage Klage vor dem Verwaltungsgericht (VG) Wiesbaden ein. Das Gericht hatte erhebliche Zweifel daran, dass diese Pflicht zur Aufnahme von Fingerabdrücken in den Personalausweis, unionsrechtskonform ist. Die Richter führen bereits formale Gründe gegen die EU-Verordnung ins Feld. Ihnen zufolge wäre ein sogenanntes besonderes Gesetzgebungsverfahren nötig gewesen, welches nicht durchgeführt worden ist.

Nach Ansicht des Gerichts verletzt die Verordnung ferner Artikeln 7 und Artikel 8 der EU-Grundrechtecharta (GrCh), die das Recht zum Schutz der Privatsphäre festschreiben. Das Gericht hat das Verfahren daher ausgesetzt und den Fall dem Europäischen Gerichtshof (EuGH) zur Entscheidung vorgelegt.[1]

Das VG Wiesbaden führt aus, dass es sich bei den erfassten biometrischen Merkmalen um personenbezogene Daten handelt, die „objektiv unver-

1 VG Wiesbaden, Beschluss vom 13.01.2022 - 6 K 1563/21.WI

wechselbare Informationen über natürliche Personen enthalten und deren genaue Identifizierung ermöglichen“. Das Gericht argumentiert, die Grundrechte der Betroffenen dürften unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur eingeschränkt werden, wenn dies etwa dem Gemeinwohl diene oder „den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entspreche“. Zudem ist in Art. 8 Abs. 2 GrCh bestimmt, dass personenbezogene Daten nur mit Einwilligung der betroffenen Person oder aufgrund einer sonstigen gesetzlichen Regelung verarbeitet werden dürfen. Eine Einwilligung in die Erfassung der Fingerabdrücke liegt nach Auffassung des Gerichts nicht vor. Art. 3 Abs. 5 VO (EU) 2019/1157 bestimmt die Erfassung jedoch als gesetzliche Regelung. Das vorlegende Gericht hat jedoch Zweifel daran, ob diese Vorschrift unionsrechtskonform ist.

Das Verwaltungsgericht beanstandete, der Gesetzgeber habe keine Datenschutz-Folgenabschätzung gemacht, die aber angesichts des hohen Risikos hier notwendig gewesen wäre. Die Richter überwiesen den Fall zur Klärung an den Europäischen Gerichtshof.

Die Entscheidung des EuGHs bleibt abzuwarten.

1.2 Entwicklung des Datenschutzes in der Bundesrepublik

1.2.1 Änderung des Personenstandsgesetzes

Am 29.09.2022 hat die Bundesregierung den Entwurf für ein drittes Gesetz zur Änderung personenstandsrechtlicher Vorschriften gebilligt. Danach ist u. a. vorgesehen, den Eintrag der Religionszugehörigkeit in den Personenregistern abzuschaffen. Aus Sicht des Datenschutzes ist diese Entscheidung konsequent und erforderlich.

Personenstandsregister sind die bei den Standesämtern geführten öffentlichen Register, die über den Personenstand einer Person Auskunft geben. Rechtsgrundlage für die Führung dieser Register ist das Personenstandsgesetz (§ 3 PStG). Der „Personenstand“ ist die familienrechtliche Stellung eines Menschen innerhalb der Rechtsordnung. Er umfasst Daten über

Geburt, Eheschließung, Begründung einer Lebenspartnerschaft und Tod sowie alle damit in Verbindung stehenden familien- und namensrechtlichen Tatsachen (§ 1 PStG). Die Religionszugehörigkeit ist somit kein den Personenstand eines Menschen kennzeichnendes Element.

Zunächst hatten in Deutschland bis in das 19. Jahrhundert fast ausschließlich die Kirchenregister die Funktion öffentlicher Personenstandsregister. Da dort aber nur Eintragungen für Kirchenmitglieder vorgenommen wurden, ergab sich die Notwendigkeit ein allgemeines staatliches Register zu schaffen. Das im Jahr 1876 in Kraft getretene „Gesetz über die Beurkundung des Personenstandes und die Eheschließung“ erfüllte diese Aufgabe. Seinerzeit wurde der Personenstand weiter definiert und umfasste auch die Benennung von Beruf und Religion. In der Weimarer Republik wurde 1920 der Religionsvermerk im Geburtsregister, Eheregister und Sterberegister abgeschafft. Erst durch die Nationalsozialistische Regierung wurde im Rahmen einer Änderung des Personenstandsgesetzes 1937 der Religionsvermerk wieder eingeführt. Handlungsleitende Intention des Regimes war es seinerzeit, Angehörige vor allem jüdischen Glaubens kenntlich zu machen. Der bundesdeutsche Gesetzgeber hat unter dem Eindruck des Missbrauchs des Personenstandsregisters den Eintrag der Religion im Personenstandsgesetz 1957 von der Zustimmung der Betroffenen abhängig gestaltet (Opt-Out-Lösung). In einer weiteren Änderung im Jahr 2009 wurde der Eintrag der Zugehörigkeit zu einer Religionsgemeinschaft nur auf Wunsch Betroffener vorgenommen (Opt-In-Lösung). Gleichzeitig konnte nach dieser Änderung nur noch die Zugehörigkeit zu einer Religionsgemeinschaft verlangt werden, wenn diese öffentlich-rechtlich organisiert war.

Aus Sicht des Datenschutzes ist die gesetzliche Änderung zu begrüßen.

Die Eintragung der Religion stellt zunächst eine Verarbeitung in Form des Erfassens und Speicherns dar.

Dabei handelt es sich um personenbezogene Daten besonderer Kategorie gem. Art. 9 Abs. 1 DS-GVO, deren Verarbeitung grundsätzlich untersagt ist. Eine Ausnahme davon kann gegeben sein, wenn die betroffene Person in die Verarbeitung für einen oder mehrere Zwecke ausdrücklich einwilligt. Eine solche Einwilligung wird aber regelmäßig fehlen, da das Gesetz keinen Zweck für die Eintragung des Religionsmerkmals festlegt. Die Eintragung

der rechtlichen Zugehörigkeit zu einer Religionsgemeinschaft hat deshalb ausschließlich deklaratorischen Charakter[2]. Betroffene müssten also ausdrücklich darin einwilligen, ihre Religionszugehörigkeit deklarieren zu wollen. Eine solche Einwilligung müsste der Verantwortliche nachweisen können. Das Standesamt müsste also eine von anderen Sachverhalten klar zu unterscheidende Erklärung der Betroffenen verlangen. Eine konkludente Einwilligung im Zusammenhang mit der verpflichtenden Meldung wäre nicht zulässig.

Neben der Rechtmäßigkeit der Datenverarbeitung gem. Art. 11 Abs. 2 und Art. 6 Abs. 1 DS-GVO müssten aber auch die Grundsätze der Datenverarbeitung gem. Art. 5 DS-GVO gewährleistet sein. Danach dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Solche eindeutigen und konkret festgelegten Zwecke kennt das Personenstandsgesetz im Hinblick auf die Verarbeitung des Religionsmerkmals gerade nicht. Zweck des Gesetzes ist die Verarbeitung von Personenstandsmerkmalen. Die Religionszugehörigkeit ist aber kein den Personenstand des Menschen kennzeichnendes Element. Im Sinne der gesetzlich geforderten Datensparsamkeit ist die Verarbeitung dieses personenbezogenen Datums dem Zweck nicht angemessen und für diesen nicht erheblich (Art. 5 Abs. 1 lit. c DS-GVO). Bei den Angaben zur Religionszugehörigkeit in den Personenregistern handelt es sich um Daten, die für staatliche Zwecke nicht benötigt werden. Auch wenn eine wirksame Einwilligung Betroffener vorläge, wäre deshalb die Verarbeitung wegen des Verstoßes gegen Grundsätze der Datenverarbeitung unzulässig.

Konsequent ist deshalb auch die Streichung des Privilegs der öffentlich-rechtlich organisierten Religionsgemeinschaften, Einsicht in die Personenstandsregister zu nehmen. Eine solche Einsichtnahme ist für die Kirchen nicht erforderlich, weil durch die Datenübermittlung aus dem Melderegister gem. § 42 Bundesmeldegesetz (BMG) die Kirchen ohnehin Daten zu Namen, Geburten, Anschriften, Geburtsdatum und Geburtsort, Geschlecht, Familienstand und Sterbedaten ihrer Mitglieder mitgeteilt bekommen. Durch diese Datenübermittlung der Meldebehörden können Taufen, Ehe-

2 BT.-Drs.: 20/2294 S. 62

schließungen und Sterbefälle leicht dem Taufbuch der örtlich zuständigen Pfarrei zugeordnet werden.

Die Änderung des Personenstandsgesetzes war aus datenschutzrechtlichen Gründen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten mithin erforderlich.

1.2.2 Datenschutzkonformer Online Handel

Die Datenschutzkonferenz (DSK) hat am 24. März 2022 einen Beschluss[3] gefasst, um Nutzer im Online-Handel besser zu schützen.
Folgendes wurde beschlossen:

1. Jeder Verantwortliche, der Waren oder Dienstleistungen im Onlinehandel anbietet, muss gewährleisten, dass eine Bestellung auch über einen Gastzugang, d.h. ohne Registrierung eines Accounts/ Nutzungszugangs, möglich ist. Der wesentliche Unterschied besteht darin, dass beim Gastzugang kein Kundenkonto angelegt wird und nur die Daten erhoben und gespeichert werden dürfen, die für den unmittelbaren Bestellvorgang erforderlich sind. Eine Bestellhistorie oder Ähnliches dürfen hier nicht angelegt und gespeichert werden. Durch technisch-organisatorische Maßnahmen muss sichergestellt werden, dass die Daten z.B. nur noch für gesetzliche Aufbewahrungsfristen zur Verfügung stehen.

2. Kein Kunde darf benachteiligt werden, wenn er kein Kundenkonto anlegen möchte.
   Gastzugänge sind daher notwendig, um die Bedingungen an die Freiwilligkeit beim Anlegen eines Kundenkontos und der damit verbundenen Datenverarbeitung zu gewährleisten.

3. Für die Auswertungen der Bestellhistorie und weiterer Zwecke der Verarbeitung (z.B. Werbezwecke), die über den bloßen Bestellvorgang hinausgehen, muss eine informierte Einwilligung vom Kunden eingeholt werden.

4. Die registrierten Nutzer sowie auch die Nutzer der Gastzugänge müssen in transparenter Weise über die Verarbeitung ihrer Daten vor Vertragsabschluss informiert werden.

3 https://datenschutzkonferenz-online.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf, zuletzt aufgerufen am 30.01.2023

Ein fortlaufendes Kundenkonto ist nach Auffassung der Datenschutzaufsichtsbehörden nur zulässig, wenn eine Einwilligung des Betroffenen vorliegt. Eine Verarbeitung zur Erfüllung oder Anbahnung von Verträgen (§ 6 Abs. 1 lit. c KDG / Art. 6 Abs. 1 lit. b DS-GVO) soll allenfalls in Ausnahmefällen in Betracht kommen. Damit die Einwilligung in die Erstellung eines Kundenkontos tatsächlich freiwillig ist, muss es die Möglichkeit zur Bestellung über einen Gastzugang als gleichwertige Alternative geben.

1.2.3 Facebook Fanpages – weiterhin keine wirksame Rechtsgrundlage

Wiederholt hatten wir in unseren Tätigkeitsberichten und auf unserer Homepage über datenschutzrechtliche Probleme bei Verwendung von Facebook Fanpages hingewiesen. Technisch handelt es sich bei Fanpages um eine Art von Mini-Webeseite innerhalb von Facebook, die die URL der Facebook-Seite enthalten. Fanpages sind grundsätzlich öffentlich ausgerichtet, d. h., dass sie von allen Internetnutzern besucht werden können, unabhängig davon, ob diese im Facebook-Netzwerk registriert sind.

Betreiber einer Fanpage haben die Möglichkeit, ihre Fanpage mit Inhalt zu füllen, auf die technische Konfiguration der Fanpage haben sie jedoch keinen Einfluss. Bei Aufruf einer Fanpage werden Metadaten (u.a. auch die IP-Adresse) des Besuchers an Facebook-Server übermittelt. Außerdem platziert Facebook beim Aufruf von Fanpages sogenannte „Cookies“ und liest vorhandene Cookies des Besuchers aus. Die Übermittlung bestimmter Cookies ermöglicht es Facebook beispielsweise, die dort registrierten und angemeldeten Mitglieder zu erkennen und die Aktivität auf der Fanpage mit den sonstigen Informationen zu verknüpfen, die Facebook aufgrund des Anmeldevorgangs über das jeweilige Mitglied hat.

Bereits im letzten Jahr hat das OVG Schleswig-Holstein in einem Urteil[4] festgestellt, dass die Verwendung einer solchen Fanpage unter bestimmten Voraussetzungen unzulässig ist.

4 OVG Schleswig Holstein, Urteil vom 25.11.2021 - 4 LB 20/13

Das Gericht urteilte, dass die Verarbeitung personenbezogener Daten von registrierten Nutzerinnen und Nutzern (Registrierungsdaten) zur Erstellung der „Insights"-Statistik und die Verknüpfung und Speicherung dieser Daten zur Erstellung von Profilen und zu Werbezwecken eine zweckändernde Verarbeitung von Bestandsdaten nach dem damals geltenden Telemediengesetz darstellt, für die keine datenschutzrechtliche Erlaubnis vorlag.

Auch die Taskforce Facebook-Fanpages der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in einem Kurzgutachten[5] Kritik zur weiteren Verwendung von Facebook Fanpages geäußert und dabei festgestellt, dass für die beim Besuch einer Fanpage ausgelöste Speicherung von Informationen in den Endeinrichtungen der Endnutzer und den Zugriff auf Informationen, die bereits in der Endeinrichtungen gespeichert sind, sowie für die Verarbeitungen personenbezogener Daten, die von Seitenbetreibern verantwortet werden, keine wirksamen Rechtsgrundlagen gegeben sind. Darüber hinaus werden die Informationspflichten aus Art. 13 DS-GVO nicht erfüllt.

Unsere Dienststelle stimmt dieser Bewertung zu und forderte die Verantwortlichen in den kirchlichen Einrichtungen auf, ihre Facebook-Fanpages zu deaktivieren, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können.

Zum Nachweis gehört dabei insbesondere:

- der Abschluss einer Vereinbarung nach § 28 KDG (Art. 26 DS-GVO) über die gemeinsame Verantwortlichkeit mit Facebook,
- eine ausreichende Information über die gemeinsamen Datenverarbeitungen gegenüber den Fanpage Nutzenden gemäß §§ 14 ff KDG (Art. 12 DS-GVO),
- die Zulässigkeit zur Speicherung von Informationen in der Endeinrichtung des Endnutzers und der Zugriff auf die Informationen gem. § 25 TTDSG,
- und der Zugriff auf diese Informationen gemäß § 25 TTDSG.

5 Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages (datenschutzkonferenz-online.de), zuletzt aufgerufen am 30.01.2023

1.2.4 EuGH Entscheidung über Vorratsdatenspeicherung in Deutschland

Ohne Anlass dürften die Kommunikationsdaten aller Bürgerinnen und Bürger nicht gespeichert werden, entschied der Europäische Gerichtshof am 19.09.2022.[6] Die deutsche Vorratsdatenspeicherung ist mit EU-Recht nicht vereinbar.

Wer mit wem wann telefoniert hat und in welcher Funkzelle er dabei eingeloggt war und wie lange der Anruf gedauert hat – diese Informationen darf der Staat nicht einfach vorsorglich speichern. Nach Auffassung des EuGHs ist eine „allgemeine und unterschiedslose" Speicherung personenbezogener Daten unzulässig. Zulässig ist aber eine gezielte Speicherung bei schweren Verbrechen und „unter strikter Beachtung des Grundsatzes der Verhältnismäßigkeit".

Vorratsdatenspeicherung bedeutet, dass Telekommunikationsfirmen Telefon- und Internetverbindungsdaten ihrer Kunden für eine bestimmte Zeit sichern müssen, damit Ermittler bei Bedarf darauf zugreifen können. Seit Jahren wird in Deutschland darüber diskutiert, bei welchen möglichen Straftaten das erlaubt ist und wie lange die Daten gespeichert werden müssen. Die Speicherung wird vielfach als ein unverzichtbares Instrument im Kampf gegen Terrorismus oder organisierte Kriminalität gesehen, Bürgerrechtler hingegen halten sie für weitgehend unwirksam oder überzogen, da sie alle Menschen unter Generalverdacht stelle.

Die Richter am EuGH bleiben mit ihrer Entscheidung ihrer bisherigen Rechtsauffassung treu (über ähnliche Fälle in anderen Ländern wurde bereits entschieden). Personenbezogene Daten ohne einen konkreten Anlass zu speichern, verstößt gegen EU-Recht. Denn solche Daten ließen „sehr genaue Schlüsse auf das Privatleben" zu.

Aber: In mehreren Fällen erlauben die Richter jedoch eine Datenspeicherung, so z.B. bei einer ernsten, aktuellen oder vorhersehbaren Bedrohung für die nationale Sicherheit. Zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit dürften Telekommunikationsanbieter für einen

6 EuGH, Urteil vom 20.09.2022 - C 793/19, C-794/19

begrenzten Zeitraum dazu verpflichtet werden, bestimmte Daten zu speichern.

Mit der Entscheidung endet eine lange Debatte über die Zulässigkeit der Vorratsdatenspeicherung (vgl. Beitrag im Tätigkeitsbericht 2017, S. 11). Im Jahr 2015 sollte die Vorratsdatenspeicherung eingeführt werden. Ein Gesetz sah vor, dass Telekommunikationsunternehmen Standortdaten für vier Wochen und Verkehrsdaten für zehn Wochen zwischenspeichern sollten, um Verbrechen besser aufklären zu können.

Aus Sicht der Ermittlungsbehörden ein hilfreiches Mittel, doch Datenschützer und Telekommunikationsanbieter schlugen Alarm.

Jetzt hat der Europäische Gerichtshof nach seinem wegweisenden Urteil aus dem Jahr 2020[7] erneut klargestellt, dass die vorsorgliche Speicherung dieser sensiblen Informationen nur für den Fall, dass sie einmal nützlich sein könnten, rechtswidrig ist.

Das deutsche Gesetz aus dem Jahr 2015, das die Speicherung dieser Informationen erlaubte, ist damit passé. Obwohl es wegen der rechtlichen Unsicherheiten seit 2017 nicht mehr angewendet wurde, steht nun fest, dass es in dieser Form auch nicht zur Geltung kommen kann.

Wenn überhaupt ist eine neue Regelung notwendig, die die Vorgaben des EuGHs aus dem Urteil beachtet. Die Luxemburger Richterinnen und Richter haben deutlich gemacht, dass eine Speicherung der sensiblen Informationen nur in sehr eng umgrenzten Ausnahmefällen angeordnet werden darf.

1.2.5 Nachlässiger Umgang mit Datenschutzvorschriften rechtfertigen Kündigung

Das Landesarbeitsgericht (LAG) Sachsen[8] hat festgestellt, dass ein wiederholter Verstoß gegen datenschutzrechtliche Vorgaben des Arbeitgebers eine Kündigung rechtfertigen kann.

Im konkreten Fall existierten bei dem Arbeitgeber datenschutzrechtliche Regelungen, nach denen schützenswerte oder geheime Informationen

7 EuGH, Urteil vom 06.10.2020 - C-623/17
8 Sächsisches LAG, Urteil vom 07.04.2022 - 9 Sa 250/21

nicht durch Dritte eingesehen werden können. Danach sind Akten, Datenträger oder Hardware mit personenbezogenen Daten ordnungsgemäß wegzuschließen oder zu vernichten, wenn der Arbeitsplatz verlassen wird oder unbeaufsichtigt ist. Weiterhin ist in diesen Fällen das Arbeitsgerät immer zu sperren oder mindestens ein Bildschirmschoner zu aktivieren. Am Ende des Arbeitstages sind IT-Systeme abzumelden und herunterzufahren, gekippte oder offene Fenster sind zu verschließen. Ausdrucke oder Akten sind in einer Schublade oder einem Schrank wegzuschließen.

Die Arbeitnehmerin hat mehrfach gegen diese Vorschriften verstoßen und wurde deshalb wiederholt vom Arbeitgeber ermahnt und in der weiteren Folge abgemahnt.

Als ein erneuter Verstoß festgestellt wurde, kündigte der Arbeitgeber das Arbeitsverhältnis aus verhaltensbedingten Gründen.

Die Arbeitnehmerin führte zu ihrer Rechtfertigung an, die Etage, in der sich ihr Büro befindet, sei vom Kundenverkehr ausgenommen. In der gesamten Etage hielten sich ausschließlich Beschäftigte des Arbeitgebers auf und diese seien keine Dritten. Als Dritte seien nur externe Personen anzusehen. Wenn diese Zutritt zu dem Gebäude haben möchten, müssten sie sich an der Pforte melden und kämen dann nur über einen Zugangscode in die Geschäftsräume. Das LAG hielt dem entgegen, auch andere Beschäftigte desselben Arbeitgebers seien als Dritte anzusehen, solange sie nicht selbst im Rahmen ihrer Arbeitstätigkeit Zugriff auf dieselben Daten hätten. Auch auf den Datenschutz verpflichtete Mitarbeitende dürfen über Kunden nichts erfahren, für die sie nicht zuständig sind. Schließlich stellt das Gericht fest, dass ein Pflichtverstoß bereits dann vorliegt, wenn gegen die bestehenden Dienstvorschriften verstoßen wird, unabhängig davon, ob ein Schaden eingetreten ist.

1.2.6 Entscheidung zur Zulässigkeit von Cloud- und IT-Dienstleistungen durch US-Tochterunternehmen in Deutschland – Vergabekommission

Nach den Festlegungen der DS-GVO dürfen personenbezogene Daten nur in ein Drittland (außerhalb der EU) übermittelt werden, wenn der Verant-

wortliche geeignete Garantien vereinbart oder die EU-Kommission festgestellt hat, dass in dem Drittland ein angemessenes Datenschutzniveau besteht.

Im Fall der USA gab es mit dem „Safe Habour" und dem „Privacy-Shield-Abkommen" bereits zweimal entsprechende Abkommen, die ein geeignetes Datenschutzniveau regeln sollten. Beide Abkommen wurden jedoch vom Europäischen Gerichtshof als unzureichend eingestuft. In der Folge gingen US-amerikanische Unternehmen dazu über, Tochtergesellschaften in Europa zu gründen, die die Datenverarbeitung ausschließlich über Server abwickeln, die ihren Standort auf dem Gebiet der EU haben. Eine Datenübertragung in einen Drittstaat findet danach zunächst nicht statt.

Mit Beschluss vom 13. Juli 2022 hatte die Vergabekammer Baden-Württemberg[9] entschieden, dass Aufträge an solche europäischen Tochtergesellschaften von US-Anbietern, die digitale Server- und Cloudleistungen erbringen, unzulässig seien, auch wenn die Server in Europa betrieben werden.

Die Vergabekammer Baden-Württemberg sieht in der Möglichkeit, dass die nichteuropäische Muttergesellschaft auf personenbezogene Daten zugreifen kann, eine datenschutzrechtlich unzulässige Übermittlung von personenbezogenen Daten in ein Drittland. Allein die Möglichkeit stelle eine „Weitergabe" im Sinne der DS-GVO dar, unabhängig davon, ob ein solcher Zugriff durch die US-Muttergesellschaft tatsächlich erfolgt.

Hintergrund dieser strengen Auslegung dürfte das Bestehen des sog. „Cloud Act" sein. Nach dieser Vorschrift dürfen US-Geheimdienste Zugriff auf die bei US-Unternehmen gespeicherten Daten erhalten. Nach dem „Cloud Act" gilt ein solches Zugriffsrecht immer, sobald sich der Hauptsitz des Anbieters in den USA befindet, unabhängig davon, wo sich die Tochtergesellschaften und deren Server befinden, auf denen die Daten gehostet werden.

Die Entscheidung der Vergabekammer wurde am 07.09.2022 vom Oberlandesgericht Karlsruhe[10] aufgehoben. Nach dessen Entscheidung begründet

9 Vergabekammer Baden-Württemberg, Beschluss vom 13.07.2022 - 1 VK 23/22
10 OLG Karlsruhe, Beschluss vom 07.09.2022 - 15 Verg 8/22

allein die Tatsache, dass ein Unternehmen Tochtergesellschaft eines US-amerikanischen Konzerns ist, keinen begründeten Zweifel daran, dass das Unternehmen seine Leistungsversprechen erfüllt. Allein aufgrund der Konzernbindung sei nicht davon auszugehen, dass es zu rechts- und vertragswidrigen Weisungen an das Tochterunternehmen kommen wird bzw. das europäische Tochterunternehmen durch seine Geschäftsführer gesetzeswidrigen Anweisungen der US-amerikanischen Muttergesellschaft Folge leisten wird.

Die Auswirkungen der Rechtsansicht des OLG Karlsruhe können weit über die Vergabeentscheidung hinausgehen. Bislang ist das Bestehen des Cloud-Acts das Hauptargument von Datenschützern gegen die Verarbeitung von Daten bei amerikanischen Unternehmen, selbst wenn diese die Verarbeitung von personenbezogenen Daten ausschließlich auf Servern innerhalb der EU zusichern.

1.2.7 Arbeitsgericht Neuruppin verpflichtet Unternehmen zu Schadenersatz

Das Arbeitsgericht (ArbG) Neuruppin[11] verpflichtete ein Unternehmen zu Schadenersatz, weil Daten einer ausgeschiedenen Mitarbeiterin nicht von der Firmenhomepage gelöscht wurden. Löscht ein Unternehmen die Daten von ausgeschiedenen Mitarbeitern nicht von seiner Homepage, handelt es sich um einen unzulässigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Dies begründet nach Ansicht des Gerichts im vorliegenden Fall einen Anspruch auf Schadensersatz i. H. v. 1.000 €.

Das Gericht ist davon ausgegangen, der Klägerin stehe ein Schadensersatzanspruch in der ausgeurteilten Höhe zu, da die Beklagte trotz des entsprechenden Begehrens der Klägerin über mehrere Monate hin deren Daten auf ihrer Internetseite nicht gelöscht hat. Der Anspruch besteht unbeschadet der Tatsache, dass die Klägerin keine immateriellen Beeinträchtigungen vorgetragen hat.

Bei dem Anspruch aus Art. 82 DS-GVO handelt es sich um einen Schadensersatzanspruch des Betroffenen gegenüber dem Verantwortlichen, der

11 ArbG Neuruppin, Urteil vom 14.12.2021 - 2 Ca 554/21

dann geltend gemacht werden kann, wenn datenschutzrechtliche Pflichten verletzt und dadurch materielle und immaterielle Schäden entstanden sind.

Der Betroffene muss lediglich beweisen, dass die Anspruchsgegnerin, hier die Beklagte als Arbeitgeberin, an dem datenschutzrechtlichen Verstoß beteiligt war, dadurch ein Schaden entstanden ist und die konkrete Verarbeitung der Daten dazu geeignet war, den Schaden hervorzurufen.

Interessant an der Entscheidung des Gerichts ist: Ein immaterieller Schaden muss nicht dargelegt werden. Obwohl die Klägerin keine erhebliche Beeinträchtigung ihrer Persönlichkeitsrechte vorgetragen hatte, sprach das Gericht ihr einen immateriellen Schadensersatzanspruch auf Grundlage des Art. 82 DS-GVO in Höhe von 1.000 € zu.

Die Entscheidung wurde damit begründet, dass der Art. 82 DS-GVO **eine Warn- und Abschreckfunktion** beinhalte. Das heißt, es soll dem Verantwortlichen weh tun. Die bloße Verletzung der Bestimmungen der DS-GVO durch den Beklagten schien dem Gericht ausreichend. Damit setzt sich das ArbG Neuruppin von einigen anderen ergangenen Urteilen ab, die zögerlicher mit derartigen Ansprüchen umgegangen sind.

Die Frage, ob eine Recht auf Ersatz des immateriellen Schadens bereits dann vorliegt, wenn personenbezogene Daten entgegen den Vorschriften der DS-GVO verarbeitet werden oder ob es darüber hinaus eines erlittenen Schadens von einigem Gewicht bedarf, ist vom BAG dem EuGH zur Vorabentscheidung vorgelegt worden.

Fazit: Die Daten, wie Name, Funktion und auch Bilder sind sicherheitshalber zeitnah nach dem Ausscheiden von Webseiten zu löschen. Am besten unmittelbar mit dem Ausscheiden, bestenfalls ein paar Werktage danach.

1.2.8 Anschrift ohne Namen ist kein personenbezogenes Datum

Der Begriff der personenbezogenen Daten ist das entscheidende Kriterium zur Anwendung der DS-GVO bzw. des KDG und meint alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person

beziehen. Dass ein hinreichender Personenbezug nicht vorliegt und der Anwendungsbereich der DS-GVO mithin nicht eröffnet ist, entschied das Landgericht (LG) Berlin[12] in Anbetracht der Eingabe einer bloßen Wohnadresse ohne Namensbezug bei „Google Maps" und wies die Klage als unbegründet ab. Der Klägerin stehe kein Schadensersatzanspruch gemäß Art. 82 DS-GVO zu, da kein Verstoß gegen geltendes Datenschutzrecht vorliegt. Nach Ansicht des LG habe die Beklagte weder personenbezogene Daten entgegen Art. 5 DS-GVO nicht rechtmäßig verarbeitet, noch liege eine unzulässige Übermittlung von personenbezogenen Daten in ein Drittland gemäß Art. 44 DS-GVO vor. Bei der Eingabe bloßer Adressdaten ohne konkreten Personenbezug handelt es sich nicht um ein personenbezogenes Datum i. S. v. Art. 4 Nr. 1 DS-GVO und damit ist die DS-GVO nicht anwendbar. „Denn die bloße Adresse ohne Bezugnahme auf eine Person – sei es durch namentliche Nennung, sei es durch die Bezugnahme auf ein diese Adresse betreffendes Eigentums-, Besitz- oder Mietverhältnis – stellt keinen hinreichenden Personenbezug dar". Demzufolge steht der Klägerin kein Schadensersatzanspruch zu, so das LG Berlin, das die Klage abwies.

1.3 Entwicklung des Datenschutzes in der Kirche (kirchlichen Einrichtungen)

1.3.1 „Nun sag`, wie hast du`s mit der Religion."

Seit der Entscheidung des Europäischen Gerichtshofs in der Sache „Egenberger" ist die Frage nach der Religionszugehörigkeit im kirchlichen Beschäftigungskontext nicht mehr in jedem Fall zulässig. Nach Ansicht des EuGHs muss vielmehr ein objektiv überprüfbarer direkter Zusammenhang zwischen der Religionszugehörigkeit und der ausgeschriebenen Tätigkeit bestehen, um die Zulässigkeit einer solchen Frage zu begründen. Das trifft nur für Tätigkeiten im Bereich der Verkündigung und für Leitungspositionen, die die Position der Kirche glaubhaft vertreten müssen, zu.

Das Bundesarbeitsgericht hat mit dem Beschluss[13] vom 27.01.2022 dem EuGH nunmehr die weitergehende Frage vorgelegt, ob eine der katho-

12 LG Berlin, Urteil vom 27.01.2022 - 26 O 177/21
13 BAG, Beschluss vom 21. Juli 2022 - 2 AZR 130/21 (A)

lischen Kirche zugeordnete Arbeitgeberin Beschäftigte allein deshalb als ungeeignet für eine Tätigkeit ansehen darf, weil diese vor Beginn des Arbeitsverhältnisses aus der katholischen Kirche ausgetreten sind, auch wenn die Arbeitgeberin von anderen bei ihr tätigen Mitarbeitenden im Übrigen nicht verlangt, dass sie der katholischen Kirche angehören.

Eine Ablehnung in diesen Fällen ist gängige Praxis katholischer Stellen. Die Bischöfe begründen diese strengen Maßnahmen damit, dass der Austritt „eine willentliche und wissentliche Distanzierung von der Kirche" darstelle und eine „schwere Verfehlung gegenüber der kirchlichen Gemeinschaft" sei.

Demgegenüber vertritt der Päpstliche Rat für die Gesetzestexte in einer Bekanntmachung an alle Präsidenten der Bischofskonferenzen eine deutlich differenziertere Ansicht in dem er feststellt: „Der rechtlich-administrative Akt des Abfalls von der Kirche kann aus sich nicht einen formalen Akt des Glaubensabfalls in dem vom CIC (Codex Juris Canonici) verstandenen Sinn konstituieren, weil der Wille zum Verbleiben in der Glaubensgemeinschaft bestehen bleiben könnte". Nicht allen, die aus der Kirche austreten, sollte also pauschal unterstellt werden, sich durch einen „öffentlichen Akt" von der Kirche distanzieren zu wollen. Vielmehr ist nach dem Grund des Austritts zu differenzieren.

Die Entscheidung des EuGHs zu dieser Vorlage hat direkte Auswirkungen auf das Fragerecht katholischer Einrichtungen im Zusammenhang mit Stellenbesetzungen. Künftig wird darüber hinaus, das Fragerecht auch durch die am 22.11.2022 von der Vollversammlung des VDD beschlossene neue Grundordnung eingeschränkt werden.

1.3.2 Datenschutzrisiko Pfarrbrief

Veröffentlichung persönlicher Daten in Pfarrbrief

Nach einer Erhebung des statistischen Bundesamtes werden deutschlandweit noch immer ca. 6,75 Mio. Pfarrbriefe verschickt. Aus Sicht der Datenschutzaufsicht ist dies einmal mehr Anlass, zu der Überlegung, was in diesem Zusammenhang rechtlich nach dem Kirchlichen Datenschutzgesetz (KDG) erlaubt ist?

Diese Frage ist nicht immer einheitlich zu beantworten. Entscheidend ist auf jeden Fall, um welchen Anlass es sich handelt und welche rechtlichen Regelungen in dem Bistum, in dem die Veröffentlichung stattfinden soll, gelten.

Alters- und Ehejubiläen

Für die Veröffentlichung von Geburtstagen und Ehejubiläen braucht es grundsätzlich die vorherige Einwilligung der Betroffenen, es sei denn, das jeweilige Bistum hat eine rechtliche Grundlage, z.B. in Form einer Jubiläumsordnung geschaffen, nach der entsprechende Veröffentlichungen auch ohne eine Einwilligung zulässig sind.

Die Bistümer sind hier aber unterschiedlich aufgestellt, es ist daher ratsam beim betrieblichen Datenschutzbeauftragten des jeweiligen Bistums nachzufragen.

Teilweise wird auch die Ansicht vertreten, eine rechtliche Grundlage für eine Veröffentlichung von Alters- und Ehejubiläen in den Pfarrbriefen der Pfarreien bestehe aufgrund von § 50 Abs. 2 des Bundesmeldegesetzes (BMG). Das Gesetz erlaubt einer Meldebehörde, den Mandatsträgern, der Presse und dem Rundfunk Auskunft bei bestimmten Alters- und Ehejubiläen zu erteilen. Auch wenn man die Pfarrbriefredaktionen als Teil der Presse betrachtet, stellt diese Vorschrift keine Rechtsgrundlage für die Veröffentlichung bestimmter Alters- und Ehejubiläen im gedruckten Pfarrbrief oder auf der Homepage dar. § 50 Abs. 2 BMG erlaubt nur einer Meldebehörde, also einer durch Landesrecht dazu bestimmten Behörde, den genannten Personen oder Einrichtungen Auskunft über bestimmte Alters- oder Ehejubiläen zu erteilen. Die kirchlichen Meldestellen stellen keine Meldebehörden im Sinne des Bundesmeldegesetzes dar.

Nach der von unserer Aufsicht vertretenen Auffassung bedarf es einer Einwilligung Betroffener immer dann, wenn nicht eine gültige Jubiläumsordnung etwas anderes festschreibt.

Was darf veröffentlicht werden?

Veröffentlicht werden dürfen Name, der Anlass, der Tag und der Hauptort der Kirchengemeinde/Pfarreiengemeinschaft, allerdings nicht der konkrete Wohnort der betroffenen Person und nicht deren Anschrift.

Sakramentsspendungen

Dieses Thema betrifft die Frage, ob personenbezogene Daten aus Anlass einer Taufe, Erstkommunion, Firmung oder Hochzeit veröffentlicht werden dürfen.

Die teilweise dazu vertretene Rechtsauffassung, es handele sich dabei um Amtshandlungen, die bekannt geben werden dürfen, soweit keine Personenstandsdaten veröffentlicht werden, ist abzulehnen.

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn einer der Bedingungen des § 6 Abs. 1 KDG erfüllt ist. Die Tatsache der Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist ein personenbezogenes Datum, über dessen Veröffentlichung jeder selbst entscheiden kann. Ein übergeordnetes kirchliches Interesse ist demgegenüber nicht anzuerkennen. Dies gilt umso mehr, als es möglich ist, bei den Vorbereitungen zu den Sakramentsspendungen, die Betroffenen um ihre Zustimmung zur Veröffentlichung von persönlichen Daten zu bitten. Wird eine solche Zustimmung abgelehnt, ist eine Veröffentlichung unzulässig.

Sterbefälle

Datenschutz schützt Persönlichkeitsrechte. Über solche verfügen Verstorbene grundsätzlich nicht mehr. Mit dem Tod einer Person genießt diese deshalb auch keinen Datenschutz mehr.

Veröffentlicht werden dürfen sowohl im gedruckten Pfarrbrief als auch online auf der Pfarrei-Homepage der Name des Verstorbenen, das Alter, der Todestag und der Hauptort der Kirchengemeinde/Pfarreiengemeinschaft. Aus Sicherheitsgründen sollte jedoch auf die Angabe des ehemaligen konkreten Wohnortes und der Anschrift verzichtet werden.

Dienstpläne

Für die Veröffentlichung von Dienstplänen, z. B. für Ministranten, Lektoren o. A., im Pfarrbrief besteht keine Erforderlichkeit. Die Mitteilung darüber, wer einen entsprechenden Dienst wann wahrnimmt, ist für die Pfarrangehörigen nicht erforderlich. Den Betroffenen selbst kann die Diensteinteilung persönlich bekanntgegeben werden.

Unsere Tipps:

- Fragen Sie beim betrieblichen Datenschutzbeauftragten Ihres Bistums nach, ob Jubiläumsordnungen existieren und welche Regelungen diese enthalten.
- Klären Sie mit der jeweiligen Pfarrei, für welche Anlässe sie überhaupt persönliche Daten in welchen Medien veröffentlichen möchten.
- Bedenken Sie, dass bei einer Veröffentlichung von persönlichen Daten im Internet die Gefahr eines Missbrauchs viel größer ist.
- Bitten Sie bei der Anmeldung oder den Vorbereitungstreffen zu den Sakramenten schriftlich um die Zustimmung, den Namen (der Täuflinge, der Erstkommunionkinder, der Firmlinge oder des Brautpaares) und den Tag des Ereignisses veröffentlichen zu dürfen. Machen Sie deutlich, welche Medien Sie nutzen wollen. Weisen Sie auf die Möglichkeit des Widerrufs der Einwilligung hin.

2 Datenschutz allgemein

2.1 Datenerhebung beim Zensus 2022 ist rechtmäßig

Das Verwaltungsgericht Neustadt hat festgestellt, dass die Auskunftspflichten der Gebäude- und Wohnungszählung im Zensus 2022 die herangezogenen Eigentümer nicht in eigenen Rechten verletzten[14]. Aus datenschutzrechtlicher Sicht ist an der Entscheidung besonders interessant, dass das Gericht auch den Einsatz von Cloudflare auf der Webseite zum Zensus 2022 zu beurteilen hatte. Das Gericht stellte hierzu fest, dass das Hosting einer amtlichen Homepage für den Zensus 2022 durch ein US-amerikanisches Unternehmen nicht automatisch zur Rechtswidrigkeit des Zensus 2022 führt. Zur Begründung führt das Gericht aus: *„[…] dass die Datenverarbeitung durch Cloudflare gerade nicht die Befragungsdaten der Auskunftspflichtigen zum Zensus, sondern lediglich allgemein zugängliche Informationen auf der Webseite […]“* betrifft. Unter Bezugnahme auf den Beschluss

14 VG Neustadt, Beschluss vom 27. Oktober 2022 - Az. 3 L 763/22.NW

des OLG Koblenz[15] stellte das Gericht zudem fest, dass der Verantwortliche auf die vertraglichen Zusagen von Cloudflare vertrauen darf und Einlassungen der Antragsteller zu einem denkbaren Zugriff US-amerikanischer Sicherheitsbehörden (z.B. über den „CLOUD-Act“) spekulativ bleiben.

2.2 Zugriff auf Sozialdaten im Ermittlungsverfahren

Arbeitgeber, aber auch Behörden werden regelmäßig mit der Situation konfrontiert, dass eine Strafverfolgungsbehörde personenbezogene Daten und sogar besonders sensible Sozialdaten anfragt. Hierbei steht dem Auskunftsgesuch der anfragenden Behörde das gesetzlich normierte Sozialgeheimnis gegenüber, weshalb eine Übermittlung von Sozialdaten nur unter speziellen datenschutzrechtlichen Voraussetzungen erfolgen darf.

Hintergrund

Sozialdaten stellen nach § 67 Abs. 2 S. 1 SGB X (Zehntes Sozialgesetzbuch) personenbezogene Daten (Art. 4 Nr. 1 DS-GVO) dar, die von einer in § 35 SGB I (Erstes Sozialgesetzbuch) genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Ein Sozialdatum ist hierbei nicht nur durch den Personenbezug, sondern zusätzlich durch einen Sachbezug in der Weise gekennzeichnet, dass es von einem Sozialleistungsträger für dessen Aufgabenerfüllung verwendet wird[16]. Somit kann jedes Datum – auch ein Aktenzeichen oder eine E-Mail-Adresse – ein Sozialdatum im Sinne des § 67 Abs. 2 S. 1 SGB X sein, sofern es von einer in § 35 SGB I genannten Stelle (z. B. Jobcenter) zur Erfüllung ihrer Aufgaben nach dem SGB verarbeitet wird.

Sozialgeheimnis

§ 35 Abs. 1 SGB I regelt den Rechtsanspruch der Bürger darauf, dass die eigenen Sozialdaten nicht ohne entsprechende Befugnis verarbeitet werden; das schließt den Anspruch auf Wahrung des Sozialgeheimnisses bezüglich der sie betreffenden Daten durch die Leistungsträger und deren Verbände ein[17]. Die betreffende Stelle darf also Sozialdaten nur an befugte Personen bzw. Stellen übermitteln.

15 OLG Koblenz, Beschluss vom 7. September 2022 - 15 Verg. 8/22
16 LPK-SGB X/Thomas P. Stähler, 5. Aufl. 2019, SGB X § 67 Rn. 4
17 LPK-SGB I/Utz Krahmer, 4. Aufl. 2020, SGB I § 35 Rn. 2

Wann dürfen Sozialdaten im Rahmen eines Ermittlungsverfahrens herausgegeben werden?

§ 67b Abs. 1 S. 1 SGB X gibt vor, dass die Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten durch die in § 35 SGB I genannten Stellen zulässig ist, soweit die nachfolgenden Vorschriften oder eine andere Rechtsvorschrift in diesem Gesetzbuch es erlauben oder anordnen. Hierbei sind die Übermittlungsgrundsätze nach § 67d SGB X einzuhalten, die insbesondere vorschreiben, dass die Verantwortung für die Zulässigkeit der Bekanntgabe von Sozialdaten die übermittelnde Stelle trägt (diese muss die Übermittlungsvoraussetzungen prüfen).

Danach wäre zunächst das Vorliegen einer schriftlichen oder elektronischen Einwilligung der betroffenen Person nach § 67b Abs. 2 S. 1 SGB X als Rechtsgrundlage für eine Übermittlung an die anfragende Stelle zu nennen.

Im Rahmen der Amtshilfe und zur Erfüllung von Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr und der Justizvollzugsanstalten dürfen im Einzelfall und auf Ersuchen der anfragenden Behörde gewisse Sozialdaten der betroffenen Person übermittelt werden, soweit kein Grund zu der Annahme besteht, dass dadurch deren schutzwürdige Interessen beeinträchtigt werden. Zudem gilt eine zeitliche Beschränkung für das Auskunftsersuchen (sechs Monate, § 68 Abs. 1 S. 1 SGB X). Wichtig: § 68 SGB X begründet für Sozialdaten lediglich eine Befugnis, nicht aber eine Pflicht zur Übermittlung[18]; über das Übermittlungsersuchen entscheidet der Leiter oder die Leiterin (u. a.) der ersuchten Stelle, § 68 Abs. 2 SGB X.

Für Auskünfte über Sozialdaten im Rahmen eines Ermittlungsverfahrens ist zudem § 73 SGB X von großer Bedeutung: Gem. § 73 Abs. 1 SGB X ist eine Übermittlung von Sozialdaten zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens (§ 12 Abs. 1 StGB) oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist und diesbezüglich eine richterliche Anordnung vorliegt (§ 73 Abs. 3 SGB X). Unter Straftaten von erheblicher Bedeutung können u. a. Straftaten auf

18 LPK-SGB X/Thomas P. Stähler, 5. Aufl. 2019, SGB X § 68 Rn. 7

dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung, Straftaten gegen die sexuelle Selbstbestimmung oder die persönliche Freiheit fallen[19]. In diesen Fällen ist die Auskunft uneingeschränkt zulässig und gilt nicht nur bzgl. der Sozialdaten des Beschuldigten, sondern auch von Dritten wie z. B. Zeugen[20]. Die Übermittlungsbefugnis besteht hingegen nicht für Zwecke der Strafvollstreckung und Verfolgung von Ordnungswidrigkeiten[21].

Wichtig: Sofern eine gesetzliche Übermittlungsgrundlage nach §§ 68-75 SGB X in Betracht kommt, ist stets die Einschränkung nach § 76 SGB X zu prüfen, die dem Schutz besonders schutzwürdiger Sozialdaten dient. Auch unterliegen die Übermittlungsbefugnisse im Rahmen der Kinder- und Jugendhilfe bestimmten Voraussetzungen (§ 65 SGB VIII).

Mit den dargestellten Regelungen wird ein Interessenausgleich zwischen dem Sozialgeheimnis und der Strafverfolgung ermöglicht, unter gleichzeitiger Berücksichtigung besonders schutzwürdiger Sozialdaten und Betroffener (Minderjährige). Im Falle einer entsprechenden Auskunftsanfrage sollten die gesetzlichen Voraussetzungen und insbesondere die Regelungen zur Übermittlungseinschränkungen aber genauestens geprüft und im Zweifel noch einmal rechtskundiger Rat eingeholt werden.

2.3 Assistenzsysteme im Fahrzeug – Ereignisbezogene Datenspeicherung

Im Rahmen zur verpflichtenden Einführung von Fahrzeugsicherheitssystemen (EU-Verordnung Nr. 2019/2144) sollen in allen neuen Fahrzeugen laut dieser Verordnung zur Erhöhung der Verkehrssicherheit u. a. „Ereignisbezogene Daten" gespeichert werden. Ab dem 6. Juli 2022 müssen Fahrzeuge mit einem ereignisbezogenen Datenspeicher ausgerüstet sein. Laut den Vorgaben sollen die Fahrdaten des Fahrzeugs, die bei einem Unfall in anonymisierter Form gespeichert werden, im Einklang mit den EU-Datenschutzvorschriften stehen und keinen Bezug zum Fahrer oder zum Halter ermöglichen.

19 HK-SozDatenschutzR/Judith Ahrend, 4. Aufl. 2020, SGB X § 73 Rn. 7
20 OLG Karlsruhe, Beschluss vom 11.10.2006 – 3 Ss 374/06
21 HK-SozDatenschutzR/Judith Ahrend, 4. Aufl. 2020, SGB X § 73 Rn. 5

Eine Deaktivierung ist nicht möglich: Damit bei der Datenaufnahme die Integrität und die Verfügbarkeit gewährleistet sind und auch kein Datenverlust entsteht, kann das System nicht vom Fahrer deaktiviert werden.

Die Wichtigkeit von Unfalldaten ist unbestritten. Laut den Vorgaben dürfen die gesammelten Daten ausschließlich für die Unfallforschung sowie für die Typgenehmigung von technischen Systemen oder Fahrzeugen verwendet werden. Ein ungutes Gefühl zur Fahrer-Überwachung kann jedoch damit nicht beschwichtigt werden.

Hinzu kommt, dass in den neueren Fahrzeugmodellen weitere Metadaten verfügbar sind und ggf. mit zur Auswertung herangezogen werden könnten, wie z.B. Geo- und Navigationsdaten sowie Kommunikationsdaten.

Es ist abzuwarten, wie es im Praxiseinsatz mit der Transparenz bei der Datenverarbeitung und/oder der Übermittlung von ereignisbezogenen Daten z.B. an andere Stellen weitergeht. Die Praxis hat bisher gezeigt, dass beim Speichern von Daten auch Begehrlichkeiten für andere Verarbeitungszwecke geweckt und neue Geschäftsmodelle erschlossen werden.

Zum Beispiel könnte bei einer Verarbeitung von Fahrzeugdaten des Assistenzsystems mit den Umgebungs-Daten ein automatisches Tempolimit ausgelöst werden. Auch eine Vernetzung der eigenen biometrischen Daten (z.B. Fingerprint, Körpertemperatur, Puls) durch Sensoren im Lenkrad oder Sitz mit den Fahrzeug-Assistenzsystemen ist denkbar.

Ob unsere persönlichen Daten durch regulatorisch getriebene Entwicklungen immer mehr ins Visier von Wirtschaft und Behörden gelangen, sollte beobachtet werden.

Interessant ist in diesem Zusammenhang auch, an welchen Stellen unsere persönlichen Daten verarbeitet und ggf. zu unserem Nachteil angewendet werden.

2.4 Datenschutz beim E-Rezept noch nicht ausreichend

Der Rollout des E-Rezepts ist vorerst gestoppt. Der Chaos Computer Club (CCC) kritisierte bereits in der Vergangenheit die elektronische Gesundheitskarte (eGK) sowie die elektronische Patientenakte (ePA). Eine ausführliche Darstellung der Kritikpunkte findet sich auf unserer Webseite unter: Startseite/Aktuelles: „Chaos-Computer Club (CCC) kritisiert Datenschutz beim E-Rezept/Gematik kontert CCC." In der Kritik standen neben der Architektur des Fachdienstes auch vorhandene Sicherheitslücken beim Zugriff der Apotheken.

„Digitalisierung im Gesundheitssektor muss richtig umgesetzt werden: Sicher, datenschutzkonform und bequem zu nutzen", fordert der BfDI in einer Pressemitteilung vom 07. November 2022. „Unzureichend gesicherte Lösungen" kämen für ihn nicht in Frage. Deshalb werde er ihnen auch weiterhin eine „datenschutzrechtliche Absage erteilen" – so wie den aktuellen Entwicklungen beim E-Rezept.

Elektronische Rezepte sollen dafür sorgen, dass „die Behandlung mit Arzneimitteln sicherer wird, Abläufe in der Arztpraxis und der Apotheke vereinfacht werden und auch die Zettelwirtschaft im Gesundheitswesen aufhört", schrieb das Bundesgesundheitsministerium auf seiner Themen-Webseite.

Die gesetzliche Grundlage dafür ist das „Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (PDSG)", das am 20. Oktober 2020 in Kraft trat.

Verschiedene Wege führen zum E-Rezept

Zurzeit kann das E-Rezept über verschieden Wege genutzt werden. Es gibt die Möglichkeit eines QR-Codes, den man ausdrucken muss. Ärzte können den QR-Code auch per verschlüsselter E-Mail versenden. E-Rezepte können zudem über die E-Rezept-App der Nationalen Agentur für digitale Medizin, der Gematik, eingelöst werden.

In Betracht gezogen wurde eine weitere Möglichkeit: Dazu soll man mit einer elektronischen Gesundheitskarte selbst ohne dazugehörige PIN in

eine Apotheke gehen können, die Karte in ein Lesegerät stecken, um dann anschließend sein Medikament zu bekommen.

Pilotversuche gescheitert

Alle Verfahren sollten in zwei Pilotversuchen getestet werden. Doch beide Partnerorganisationen – die Kassenärztlichen Vereinigung Schleswig-Holstein (KVSH) und die Kassenärztliche Vereinigung Westfalen-Lippe (KVWL) – stiegen aus dem Projekt aus. Die KVSH im August 2022 und die KVWL Anfang November.

Grund des Ausstieges ist die Entscheidung des Bundesdatenschutzbeauftragten (BfDI) gegen die Einlösung von E-Rezepten über die elektronische Gesundheitskarte.

Grundsätzlich bestehen gegen das E-Rezept als solches und die ursprünglich vorgesehen Einlösungswege und gegen die nun zusätzliche geplante Funktionalität der Einlösung durch Stecken der eGK ohne Eingabe einer PIN keine Bedenken. Allerdings erteilten der BfDI und das Bundesamt für die Sicherheit in der Informationstechnik (BSI) der bisher geplanten Schnittstelle keine Zustimmung.

Nach Ansicht des BfDI verstößt sie gegen die DS-GVO. „Die geplante Datenverarbeitung mit der zunächst von der Gematik vorgelegten Umsetzung verursacht (…) ein großes Risiko für die Rechte und Freiheiten aller Nutzerinnen und Nutzer des E-Rezepts, bundesweit und bei allen Arztpraxen und Apotheken“, so der BfDI. Alternativ schlägt der BfDI „eine sichere, für die Versicherten, Ärzte und Apotheker vollkommen funktionsgleiche Alternative vor, bei der im Hintergrund andere Verfahren genutzt werden.“ Der BfDI äußert in seiner Pressemitteilung, dass er von allen Beteiligten erwartet, „dass bis zum Sommer 2023 eine sichere Lösung für das Abholen von E-Rezepten durch Stecken der eGK zur Verfügung steht“. Diese Lösung müsse die Standardanforderungen an IT-Sicherheit erfüllen und dürfe nicht „dem unberechtigten Zugriff auf den gesamten Bestand der E-Rezepte Tür und Tor öffnen“.

BfDI fordert sichere Authentisierungsmittel

Gefordert wird vom BfDI ferner, dass das BSI und der Deutsche Bundestag durchsetzen, „dass vorhandene sichere und bequeme Authentisierungsmit-

tel zum Standard werden, wie beispielsweise eine PIN für die Gesundheitskarte oder den elektronischen Personalausweis."

Insoweit bleibt die Entwicklung abzuwarten.

3 Datenschutzaufsicht

3.1 Und immer wieder lässiger Umgang mit E-Mail-Adressen

Ein Klassiker unter den Datenschutzverletzungen und eine der gängigsten Datenpannen: Die offene Empfängerliste im E-Mailverkehr. Auch im vergangenen Berichtsjahr wurden uns mehrere derartige Datenschutzverstöße gemeldet, bei denen personenbezogene Daten bzw. personenbezogene Daten besonderer Kategorie auf diesem Weg versandt und somit offengelegt worden sind, was zeigt, dass eine vollständige Sensibilisierung noch nicht vorhanden ist.

Empfänger im „CC"-Feld (Kopie) können – genau wie die regulären Adressaten der E-Mail aus der Adresszeile "AN" – sehen, an welche **E-Mail-Adressen** die Nachricht versandt wurde. Zudem ist der gesamte **Verlauf** einsehbar. Zu Problemen führt das immer dann, wenn es Adressaten gibt, die

- E-Mail-Adressen der anderen Empfänger nicht kennen sollten oder
- der Verlauf personenbezogene Informationen enthält.

E-Mail-Adressen setzen sich häufig aus Vornamen und/oder Nachnamen zusammen. Aus Datenschutzsicht sind solche E-Mail-Adressen als personenbezogene Daten nach § 4 Nr. 1 KDG (Art. 4 Nr. 1 DS-GVO) anzusehen, die nur dann an Dritte übermittelt werden dürfen, wenn eine Einwilligung vorliegt oder eine gesetzliche Grundlage gegeben ist. Eine solche gibt es für den Verfasser der Mail nicht in jedem Fall.

Selbst wenn die Nutzung einer E-Mail-Adresse im Rahmen der Kommunikation mit dem Empfänger vom Betroffenen erlaubt worden ist, kann nicht darauf geschlossen werden, dass der Empfänger berechtigt ist, diese an Dritte weiterzugeben.

Im Falle der Verletzung der Regeln zum Schutz personenbezogener Daten im Sinne von § 4 Nr. 14 KDG (Art. 4 Nr. 12 DS-GVO) sieht § 33 KDG (Art. 33 DS-GVO) eine sofortige Meldepflicht des Verantwortlichen vor. Dieser muss spätestens binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde anzeigen, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Beurteilung, ob diese Kriterien erfüllt sind, ist im Einzelfall schwierig. Kriterien für die Beurteilung sind:

- die Art der betroffenen personenbezogenen Daten (besonders sensibel, Gesundheitsdaten, Kontoinformationen und Ähnliches),
- die Zahl der betroffenen Personen sowie
- die Schwere eines möglichen Schadens (unbefugte Kontoabbuchungen, Ansehensverluste).

Zu beachten ist, dass der Betroffene unverzüglich zu informieren ist, falls für diesen ein hohes Risiko festzustellen ist. Die Benachrichtigungspflicht entfällt, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat (z.B. durch eine effektive Datenverschlüsselung) oder in sonstiger Weise dafür gesorgt hat, dass das Risiko für die Rechte der betroffenen Person aller Wahrscheinlichkeit nach nicht besteht.

Verstöße lassen sich vermeiden

Datenschutzverstöße bei der Nutzung von E-Mail-Verteilern geschehen oft nicht absichtlich, sondern **aus Unkenntnis oder Unachtsamkeit.** Einigen Nutzern ist offensichtlich immer noch nicht bewusst, dass es sich bei E-Mail-Adressen regelmäßig um personenbezogene Daten handelt. Schnell werden Adressen in das „An"-Feld oder „CC"-Feld eingetragen und sind so für jeden Empfänger sichtbar. Nur bei Eintragung ins „BCC"-Feld wird die Zieladresse ausgeblendet.

Hinweis: Ein Versand von E-Mails an einen größeren Empfängerkreis (z.B. ein Newsletter) ohne Verwendung der BCC-Funktion ist unabhängig von der Tatsache, ob die eigentliche Nachricht personenbezogene Daten enthält, eine meldepflichtige Datenpanne, wenn die Empfänger sich unter-

einander nicht kennen. In diesem Fall können nicht berechtigte Personen unter Nutzung der offenen Empfängerliste u. U. mit geringem Aufwand die Identitäten der anderen E-Mail- Empfänger feststellen.

3.2 Prüfaktionen der Datenschutzaufsicht

3.2.1 Querschnittsprüfungen Pfarreien

Bereits im 6. Tätigkeitsbericht 2021 ist berichtet worden, dass eine Querschnittsprüfung bei ausgewählten Pfarreien im Zuständigkeitsbereich der KDSA Ost durchgeführt wurde. Im Berichtszeitraum konnte diese Prüfung nun erfolgreich abgeschlossen werden. Es wurden 41 Pfarreien bzw. Kirchengemeinden aus den 5 Bistümern in die Prüfaktion eingebunden. Ziel dieser Prüfaktion war es, die Einhaltung der Vorschriften des KDG und KDG-DVO bei der Datenverarbeitung im Bereich der Gemeindearbeit zu testen.

Abgefragt wurden die allgemeinen Rahmenbedingungen, u.a. ob die Pfarreien einen Datenschutzbeauftragten bestellt haben, ein Datenschutzkonzept/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 regelt, wie mit Datenschutzbeschwerden umzugehen ist. Ferner wurde geprüft, ob die Informationspflichten und Betroffenenrechte bekannt sind. Auch die Einhaltung der technischen und organisatorischen Maßnahmen, wie z. B. die Einhaltung von Löschfristen wurden erfragt. Abgefragt wurde, ob private Endgeräte für betriebliche/dienstliche Zwecke verwendet werden und ob es, wenn dies der Fall ist, Regelungen zur Nutzung gibt.

Ergebnis der Prüfaktion / Feststellungen

Allgemein

Die Überprüfung hat ergeben, dass im Großen und Ganzen keine nennenswerten Beanstandungen in 4 Bistümern zu verzeichnen waren.

In einem Bistum wurden jedoch gravierende Mängel festgestellt:

Von den ausgewählten Pfarreien hatten nicht alle den übersandten Fragebogen zurückgesandt. Zu bemängeln war bei den Übrigen, dass nicht alle Pfarreien einen Datenschutzbeauftragten bestellt hatten. Verzeichnisse von Verarbeitungstätigkeiten waren auch nicht in allen Pfarreien vorhanden. Nur in einer Pfarrei existiert eine Datenschutzdokumentation. Ebenfalls nur eine der geprüften Pfarreien in diesem Bistum hat angegeben, dass ein Prozess zum Umgang mit Datenschutzvorfällen und Datenschutzbeschwerden implementiert ist. Mitgeteilt worden ist, dass Datenschutzschulungen für die Mitarbeitenden nicht bzw. unregelmäßig stattfinden.

Auch waren die vorgelegten Verpflichtungserklärungen auf den Datenschutz nicht ausreichend ausgestaltet. Verpflichtungserklärungen sollten einen Hinweis auf die Lesefassung des Gesetzes enthalten sowie die Angabe, wo diese zu erhalten ist. Hinzu kam, dass die verwendeten Einwilligungserklärungen (Foto) ebenfalls nicht den Anforderungen entsprachen. Einwilligungserklärungen müssen u.a. eine Widerrufsbelehrung sowie Hinweise auf den Datenschutz enthalten. Ebenfalls soll in den Einwilligungserklärungen auf die Gefahren bei einer Veröffentlichung im Internet hingewiesen werden. Das war nicht der Fall.

In den angefragten Pfarreien erfolgt eine Nutzung privater Endgeräte zu dienstlichen Zwecken ohne eine entsprechende Vereinbarung oder Richtline. Gem. § 20 KDG-DVO ist die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken grundsätzlich unzulässig. Sie kann als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden. Gemäß Abs. 2 der Vorschrift muss die Zulassung schriftlich erfolgen und u. a. die Gründe enthalten, aus denen die Nutzung des privaten IT-Systems erforderlich ist.

Die Nutzung privater Endgeräte zu dienstlichen Zwecken ist mangels konkreter Regelungen bzw. Vereinbarungen derzeit gem. § 20 KDG-DVO unzulässig. Das zuständige Ordinariat wurde auf die festgestellten Missstände hingewiesen.

Für die weiteren überprüften Kirchengemeinden und Pfarreien der anderen Bistümer ergab sich folgendes Ergebnis:

Einen Datenschutzbeauftragten hatten fast alle geprüften Pfarreien bestellt. Nichtbestellung war die Ausnahme. Verfahrensverzeichnisse lagen in der Regel vor. Ebenso Verpflichtungserklärungen auf den Datenschutz, Merkblätter zu datenschutzrechtliche Betroffenenanfragen sowie Fotoeinwilligungserklärungen.

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

Angegeben wurde, dass private Endgeräte grundsätzlich nicht dienstlich genutzt werden. Im Ausnahmefall findet dies nur nach vorheriger Absprache statt. Eine schriftliche Regelung zur Nutzung bestand in vielen Fällen nicht, wobei jedoch angegeben worden ist, dass eine entsprechende Richtlinie erarbeitet wird. Es gab jedoch auch Pfarreien, die eine dienstliche Nutzung zulassen und eine entsprechende Richtlinie bzw. Vereinbarung nutzen.

Technisch organisatorische Maßnahmen (TOMs)

Nach den Angaben der Verantwortlichen werden Daten regelmäßig gelöscht. Löschkonzepte bestehen, Datensicherungen werden vorgenommen und getrennt aufbewahrt. Datenverarbeitungssysteme und PC-Programme werden vor unberechtigtem Zugriff geschützt durch: personifizierte Zugangsdaten und Berechtigungssysteme. Angegeben wurde, dass Datenzugriffe nur zur Aufgabenerfüllung und im dafür notwendigen Umfang erfolgen. Zutrittsbeschränkungen, zu Räumen in den sich Dokumente mit personenbezogenen Daten befinden, bestehen. Für die Sicherung von IT-Geräten kommt eine Schutzsoftware zum Einsatz.

Ergebnis:

Insgesamt kann festgehalten werden, dass zumindest nach Auswertung der Fragebögen, bis auf wenige Ausnahmen, keine gravierenden Verstöße oder Mängel feststellbar waren.

Positiv hervorzuheben ist, dass die meisten Pfarreien innerhalb der gesetzten Frist den beantworteten Fragebogen zurückgesandt oder aber

eine Fristverlängerung beantragt hatten, der in den meisten Fällen auch wunschgemäß stattgeben werden konnte.

Alle überprüften Pfarreien erhielten eine Auswertungsschreiben. Den jeweiligen Generalvikaren wurde eine Gesamteinschätzung übermittelt.

Die Datenschutzaufsicht hat sich vorbehalten, im Nachgang dieser formalen Prüfaktion ausgewählte Pfarreien vor Ort zu überprüfen, was im Jahr 2024 erfolgen soll.

3.2.2 Caritas Regionalzentrum

Durch eine angekündigte Vorortprüfung wurde im Berichtzeitraum auch ein Caritas Regionalzentrum überprüft. Über das Regionalzentrum werden u.a. verschiedene Leistungen, wie z. B. eine Schuldnerberatung, Betreuungen über einen Betreuungsverein, die Ukraine-Hilfe und ein ambulanter Hospizdienst angeboten. Eine allgemeine soziale Beratungsstelle befindet sich im Aufbau.

Mitgeteilt worden ist, dass die Verzeichnisse für Verarbeitungstätigkeiten derzeit aktualisiert werden und über das Privacy-Trail-einsehbar sind.

Folgende Feststellungen wurden getroffen bzw. Hinweise erteilt:

Hauptamtliche und ehrenamtliche Mitarbeiter müssen auf das Datengeheimnis nach § 5 KDG verpflichtet werden. Problematisch erschien die regelmäßige Schulung der Mitarbeiter auf den Datenschutz. Dies gilt für alle Bereiche. Schulungen finden nicht regelmäßig statt. Bei den ehrenamtlichen Mitarbeitern erfolgen regelmäßige Schulungen noch seltener. Dies gilt insbesondere bei den ehrenamtlichen Betreuern und bei den im Hospizbereich tätigen Personen. Gerade diese Mitarbeiter verarbeiten jedoch ebenfalls personenbezogene Daten und personenbezogene Daten besonderer Kategorie. Daher müssen diese Mitarbeiter, auch wenn sie ehrenamtlich tätig sind, regelmäßig Datenschutzschulungen erhalten. Diese Hinweise wurden angenommen. Angegeben worden ist, dass ein Seminar zur Auskunfts-/ Schweigepflicht für Juni 2022 geplant (online) ist. Nach den Angaben des Datenschutzbeauftragten sind entsprechende Module für Online Schulungen vorhanden und können jederzeit eingesetzt werden.

Teilweise befanden sich Drucker auf den Fluren der Einrichtung. In solchen Fällen muss eine passwortgesicherte Ausgabe der Dokumente erfolgen.

Die Datensicherung erfolgt zentral im Rechenzentrum. Daten befinden sich ausschließlich auf dem Server, nicht lokal auf den Geräten.

Technisch-Organisatorische Maßnahmen sind umgesetzt

Es gelten die Regelungen, dass beim Verlassen des Arbeitsplatzes der Bildschirmschutz aktiviert werden muss sowie das Büro bei Abwesenheit abzuschließen ist. Diensthandys sind vorhanden. Auf keinem Diensthandy sind Messanger oder Social Media Dienste installiert, die die Kriterienliste der Konferenz der DDSB nicht erfüllen.

Umgang mit Personalunterlagen

Personalakten befinden sich nicht vor Ort. Arbeitsunfähigkeits-Bescheinigungen werden in die Verwaltung geschickt; entweder vom Mitarbeiter selbst oder die in der Einrichtung abgegebenen AU-Bescheinigungen werden dorthin weitergeleitet. Eine Kopie verbleibt nicht in der Einrichtung.

Ergebnis:

Die Prüfung verlief insgesamt positiv. Aus dem Gespräch mit den Anwesenden ergab sich der Eindruck, dass eine hohe Akzeptanz zur Umsetzung des kirchlichen Datenschutzes in der Einrichtung besteht. Wenn auch nicht alle Erfordernisse erfüllt worden sind, kam die KDSA zu der Feststellung, dass die Bereitschaft zur Umsetzung der gesetzlichen Vorgaben im hohen Maß vorhanden ist. Die Hinweise zur Erforderlichkeit der regelmäßigen Schulung aller Mitarbeiter auf den Datenschutz wurden angenommen.

3.2.3 Prüfung eines Seniorenzentrums

Auch in diesem Berichtszeitraum haben wir anlasslos ein Seniorenzentrum vor Ort geprüft. Die Prüfung war angemeldet und fand im Beisein des Datenschutzbeauftragten der Einrichtung statt. Geprüft wurden die datenschutzrechtlich relevanten Abläufe im Zusammenhang mit dem Betrieb des Seniorenheimes, insbesondere die Verwaltung und Aufbewahrung der Bewohnerakten, der Pflegedokumentation und der Personalakten.

1. Datenschutzkonzept und Verzeichnis von Verarbeitungstätigkeiten (VVT)

Im Termin wurde nach einem Verzeichnis von Verarbeitungstätigkeiten und einem Datenschutzkonzept gefragt. Mitgeteilt wurde, dass sowohl das Verzeichnis als auch das Datenschutzkonzept in der Geschäftsstelle des Einrichtungsträgers vorliegt. Im Seniorenzentrum selbst liegen keine Exemplare in Papierform vor. Zugriff darauf ist über den Server des Trägers möglich, aber nur durch den Leiter des Seniorenzentrums.

2. Auskünfte über Bewohner an Angehörige

Nachgefragt wurde der Umgang mit Auskunftsersuchen von Angehörigen und anderen Dritten hinsichtlich des Aufenthaltes und des Gesundheitszustandes von Bewohnern. Hier zeigten sich Unsicherheiten. Insbesondere wurde dargelegt, dass zumindest eine Abfrage konkreter Daten, die auf eine engere Beziehung zu dem/der Patienten hinweisen, unterbleibt. Klare Anweisungen, wem und unter welchen Bedingungen Auskünfte gegeben werden dürfen, waren nicht vorhanden. Klargestellt wurde, dass eine diesbezügliche datenschutzrechtliche Unterweisung der Mitarbeiter zeitnah erfolgen muss.

3. Umgang mit Führungszeugnissen

Angegeben wurde, dass erweiterte Führungszeugnisse an die Geschäftsstelle des Trägers gesandt, dort eingesehen und an die Mitarbeiter zurückgesandt werden. Eine Kopie wird im Seniorenzentrum nicht aufbewahrt.

4. Besucherlisten (Corona-Zettel)

Festgestellt wurde, dass der Umgang datenschutzkonform erfolgte. Besucher mussten am Empfang ein Formular ausfüllen und dieses in den vorhandenen Briefkasten einwerfen. Die Formulare wurden 4 Wochen aufbewahrt und dann datenschutzkonform vernichtet (geschreddert).

5. Impfnachweise (3-G-Regelung)

Die Prüfung hat ergeben, dass der Impf-bzw. Genesenenstatus der Mitarbeiter in einer Datei (mit Ablaufdatum) digital erfasst wurde. Kopien von Impfnachweisen bzw. Genesenennachweisen wurden nicht angefertigt.

6. Private Endgeräte

Private Endgeräte werden nach Angabe des Verantwortlichen nicht für dienstliche Zwecke genutzt. Es ist ein Bereitschaftshandy vorhanden, welches ausschließlich zum Einsatz kommt. Mitarbeiter werden nicht über einen privaten Anschluss in den Dienst gerufen.

7. Nutzung vom Messangerdiensten

Es erfolgt keine Nutzung von Messanger oder Social Media Diensten, die die Kriterienliste der Konferenz der DDSB nicht erfüllen, im dienstlichen Kontext. Eine Nutzung der Luca-App erfolgte nicht, zum Einsatz kam die CovPass-App.

8. Bewerbungsverfahren (Bewohner)

Die potentiellen Bewohner erhalten einen Anmeldebogen (ein Muster wurde ausgehändigt). Die Anmeldebögen wurden dem Grundsatz der Datensparsamkeit gerecht. Daten, die für die Erfüllung des Versorgungsauftrages nicht erforderlich sind, wurden nicht erhoben.

Die Notwendigkeit der Nachfrage nach der Konfession konnte nicht plausibel erklärt werden. Es wurde darauf hingewiesen, dass sofern keine Gründe für die Erhebung des Religionsmerkmals benannt werden können, diese Abfrage zukünftig zu unterlassen ist.

Nach dem Zustandekommen des Heimvertrages wird der Anmeldebogen zeitnah vernichtet. Der Heimvertrag wird in der „Abrechnungsakte" aufbewahrt.

9. Pflegedokumentation

Es werden keine digitalen Pflegeakten geführt. Die Pflegedokumentation erfolgt schriftlich in Papierform. Die Akten werden in den jeweiligen Dienstzimmern in sog. Pflegewagen (kleiner Aktenschrank auf Rollen) aufbewahrt, der abschließbar ist. In diesen Akten befinden sich die Dokumentationen der letzten 2 Monate. Ältere Dokumentationen werden in Aktenordnern aufbewahrt, die wiederum in Schränken gelagert werden, die nicht abschließbar sind. Versichert wurde jedoch, dass keine unbefugten Personen Zugriff haben, da die Büros verschlossen werden, sofern sich darin kein Mitarbeiter aufhält.

Auch das Reinigungspersonal betritt die Räume nur zu Zeiten, in denen sich in den Stationsräumen Mitarbeiter aufhalten. Es erfolgt eine Trennung der Pflegedokumentation von den Abrechnungsunterlagen.

Angegeben wurde, dass Akten nach 6 Jahren vernichtet werden. Die Löschfrist von Abrechnungsunterlagen war unklar. Hier soll eine Klärung herbeigeführt werden. Alle 2-3 Jahre erfolgt eine Aussortierung.

Pflegeakten, die im aktuellen Geschäftsablauf nicht mehr benötigt werden, werden in einem Archiv gelagert. Das Archiv ist in einem Kellerraum untergebracht und erscheint sicher gegen Vernichtung durch Feuer und Wasser. Zugang für Dritte ist ebenso ausgeschlossen. Zugang hat nur der Archivverantwortliche. Die Ablage im Archiv ist übersichtlich und nachvollziehbar.

Nach Aussage des Leiters gab es bisher kaum Verlangen auf Einsichtnahme in die Pflegedokumentation durch Angehörige, zumindest sei ihm davon nichts bekannt. Der Ablauf des Verfahrens schien jedoch bekannt. Bekannt war, dass der Angehörige, seine Berechtigung z.B. Verwandtschaftsverhältnis nachweisen muss. Sofern personenbezogene Daten per Mail versandt werden, erfolgt dies verschlüsselt.

10. Fotos

Bewohner

Eine Einverständniserklärung für Foto- und Filmaufnahmen wird bei den Bewohnern sowohl für Fotos aus dem sozialen Bereich als auch für Fotos für die Pflegedokumentation eingeholt. Ein Muster wurde uns übergeben.

Es wurde erörtert, ob das für jede Verarbeitung (Aufnahmen für die Webseite, Aushang im Pflegeheim etc.) gesondert erfolgen muss oder ob eine generelle Einwilligung erfolgen kann. § 4 Nr. 13 KDG definiert eine Einwilligung als eine für den bestimmten Einzelfall abgegebene Willensbekundung. Danach ist eine Einwilligung regelmäßig für jedes bestimmte Foto einzuholen. Sollte eine konkrete schriftliche Einwilligung im Einzelfall nicht erforderlich sein, sind entsprechende Wahlmöglichkeiten für unterschiedliche Zwecke der Veröffentlichung aufzuführen (keine Generaleinwilligung!). Die Einwilligung sollte den Hinweis enthalten, dass bei Veröffent-

lichung im Internet (Druckmedien, Webseite) Fotos im Internet weltweit von beliebigen Personen abgerufen oder weiterverwendet werden können. Vereinbart wurde, dass die Einwilligungserklärung entsprechend anzupassen ist.

Mitarbeiter

Auch die Mitarbeitenden geben eine Einwilligungserklärung ab.

Fotos werden mit dienstlichen Kameras erstellt. Die darauf befindlichen Fotos werden zeitnah heruntergeladen und auf einem externen Medium gespeichert. Die Speicherkarte der Kamera wird gelöscht. Die Speicherkarte und der Fotoapparat werden jedoch nicht getrennt voneinander aufbewahrt. Die Speicherkarte verbleibt im Apparat. Es besteht kein Löschkonzept für die Fotos. Der Apparat wird auch nicht gesichert gelagert. Wir haben entsprechende Hinweise erteilt.

Wunddokumentation (Fotos)

Die Wunddokumentation erfolgt durch die Wundschwester (externer Anbieter). Diese verfügt über eine eigene Fotoausrüstung. Das Vertragsverhältnis über die Wundversorgung besteht zwischen dem externen Anbieter und den Bewohnern, nicht mit dem Seniorenzentrum.

11. Datenpannen und Betroffenenrechte

Nach den Angaben des Einrichtungsleiters gab es noch keine Datenschutzverletzung in der Einrichtung. Die Meldefrist (§ 33 KDG) ist jedoch bekannt.

Mit der Informationspflicht des Verantwortlichen geht das Recht des Betroffenen auf Auskunft über die Verarbeitung der sie betreffenden personenbezogenen Daten einher. Die Einrichtung hat angegeben, dass es bisher keine Anfragen Betroffener oder deren Angehöriger zur Verarbeitung ihrer personenbezogenen Daten gegeben hat. Es wurde kurz das allgemeine Vorgehen bei Anfragen Betroffener besprochen.

12. Auftragsverarbeitung / externe Dienstleister

Auftragsverarbeitungsverträge hat die Einrichtung nicht geschlossen. Verträge laufen über den Verband bzw. Träger der Einrichtung.

13. IT Sicherheit

Nach den Angaben des Verantwortlichen schalten sich Bildschirme automatisch aus, wenn das Gerät nicht genutzt wird. Geräte stehen in abschließbaren Büros. Server stehen nicht vor Ort. Die Datensicherung erfolgt am Standort des Servers.

Personenbezogene Daten werden per Mail verschlüsselt versandt. Die Passwortübersendung erfolgt gesondert auf anderem Weg. Die Pflegeakten werden nicht digital geführt.

14. Videoüberwachung

Im Eingangsbereich sind 2 Kameras vorhanden, wobei es sich bei einer um eine Attrappe handelt. Die andere überwacht den Eingang am Empfangsbereich. Die Kamera läuft den ganzen Tag. Es erfolgt keine Aufzeichnung, sondern nur ein reines Monitoring.

Zweck ist die Überwachung des Zugangs in den Abendstunden. Besucher bzw. Personen, die Zutritt bekommen möchten, müssen klingeln, die Mitarbeiterin kann über den Monitor im Stationszimmer die Personen sehen und die Tür öffnen. Angeregt wurde zu prüfen, ob die Kamera auch am Tag eingeschaltet sein muss oder erst ab dem Zeitpunkt, ab dem der Empfang nicht mehr besetzt ist.

Eine weitere Kamera existiert in der Kapelle und dient der Übertragung des Gottesdienstes.

Ob die Zustimmung der MAV eingeholt worden ist, bevor die Kameras aufgehängt worden sind, war nicht bekannt.

15. Weitere Punkte

- Die **Dienstpläne** können von den Mitarbeitern über den Server eingesehen werden. Gründe für Abwesenheit enthalten diese nicht.
- Die **Arbeitszeiterfassung** erfolgt digital.
- **AU-Bescheinigungen** werden in der Einrichtung nicht aufbewahrt, sondern sollen von den Mitarbeitern an die Personalabteilung am Sitz des Trägers geschickt werden. Im Fall der Abgabe vor Ort,

werden diese direkt dorthin weitergeleitet. Eine Kopie wird nicht gefertigt.

- **Namensschilder:** Die Mitarbeiter tragen Namensschilder mit Vor- und Zunamen sowie Dienstbezeichnung. Diesbezüglich wurde durch die KDSA dargelegt, dass dies aus ihrer Sicht nicht erforderlich ist. Vorname oder Nachname oder der erste Buchstabe des Vornamens und der Nachnahme sind ausreichend. Ausgeführt wurde, dass die Mitarbeiter mit dem Tragen der Namenschilder in dieser Form einverstanden sind, worin eine Einwilligung zu sehen ist.
- Nachgefragt wurde, ob Mitarbeitende während ihrer Dienste **private Smartphones** bei sich führen dürfen. Eine konkrete Aussage konnte dazu nicht getroffen werden. Seitens der KDSA wurde darauf hingewiesen, dass Bild- und Tonaufnahmen von den Bewohnern unzulässig sind und gerade in der jüngeren Vergangenheit zu beobachten war, dass solche aber angefertigt und ins Internet gestellt wurden.

Ergebnis:

Die Prüfung des Seniorenzentrum verlief insgesamt positiv. Aus dem Gespräch mit dem Einrichtungsleiter ergab sich der Eindruck, dass eine hohe Akzeptanz zur Umsetzung des kirchlichen Datenschutzes in der Einrichtung besteht. Wenn auch hier nicht alle Erfordernisse erfüllt worden sind, kam die KDSA zu der Feststellung, dass die Bereitschaft zur Umsetzung der gesetzlichen Vorgaben im hohen Maß vorhanden ist.

Vereinbart worden ist, dass der KDSA ein überarbeitetes Muster der Foto-Einwilligung für die Bewohner (Auswahlmöglichkeiten bzgl. der Medien, über die die Veröffentlichung erfolgt) und ein Muster der Fotoeinwilligung für die Mitarbeitenden vorzulegen sind, was erfolgt ist.

Es sollte eine Überprüfung der Vorlage der Zustimmungserklärung der MAV für die Videoüberwachung ggf. Nachholung der Einwilligung und Vorlage der Zustimmung erfolgen. Vereinbart wurde auch die Auslage einer gedruckten Version des KDG und der Hinweis auf diese Auslage an alle Mitarbeitenden. Alle Auflagen wurden umgesetzt.

3.2.4 Benennung von betrieblichen Datenschutzbeauftragten in Kindertagesstätten

1. Ziel, Umfang und Ablauf

In der Prüfaktion, welche im 2. und 3. Quartal 2022 durchgeführt worden ist, sollte festgestellt werden, welche Kindertagesstätten bzw. Träger von Kindertageseinrichtungen der Pflicht nachgekommen waren, einen betrieblichen Datenschutzbeauftragten zu benennen und die Bestellung anzuzeigen. Unsere Dienststelle kommt mit dieser Prüfaktion ihren Aufgaben gemäß § 44 Abs. 1 KDG nach, wonach die Aufsicht über die Einhaltung der Vorschriften des KDGs wacht.

Weiterhin sollte ermittelt werden inwieweit die Einrichtungen die Grundsätze für die Verarbeitung personenbezogener Daten Datensparsamkeit und Zweckbindung erfüllen. Deshalb waren die Einrichtungen aufgefordert worden, die Anmelde- und Aufnahmeformulare sowie der Einwilligungserklärung zum Anfertigen und Veröffentlichen von Fotos (sog. Fotoerlaubnis) zu übersenden.

Die Vergangenheit hatte gezeigt, dass gerade bei diesen Formularen die Grundsätze für die Verarbeitung personenbezogener Daten nach § 7 Abs. 1 KDG sowie die Anforderungen an eine gültige Einwilligungserklärung gemäß § 8 KDG nicht eingehalten werden.

In unserem Tätigkeitsbericht 2020[22] hatten wir im Bereich der Schulen ausgeführt, dass in den Aufnahmeunterlagen (Anmeldung und Vertrag) eines Kindes in einer Einrichtung nur die Daten abgefragt (erfasst) werden dürfen, für die es eine Rechtmäßigkeit gemäß § 6 KDG gibt. Daten, die für diesen Zweck nicht erforderlich sind, dürfen somit nicht erfasst werden. Ebenso sind wir in unseren letzten Berichten mehrfach auf die Themen Fotografieren und Einwilligungserklärungen eingegangen und haben Tipps sowie Muster zur Verfügung gestellt.

Im Rahmen der Prüfaktion wurden 33 Kindertagesstätten in einem Bistum unserer Zuständigkeit ausgewählt und per Brief angeschrieben. Für die Beantwortung unseres Schreibens bzw. die Übersendung der geforderten

22 TB 2020, Pkt. 5.3.1 Aufnahmebögen

Unterlagen gab es eine Frist (4 Wochen für Unterlagen, bzw. 12 Wochen für Benennung). Die Hälfte der Einrichtungen konnte kurzfristig reagieren und die geforderten Unterlagen übersenden. Ein weiterer größerer Teil der Einrichtungen hat die Unterlagen innerhalb einer Fristverlängerung übersandt und einige wenige Einrichtungen haben bis dato nicht reagiert.

2. Ergebnisse der Prüfaktion

Betriebliche Datenschutzbeauftragte in den Kindertageseinrichtungen

Der Pflicht einen betrieblichen Datenschutzbeauftragten zu benennen sind zu Beginn der Prüfaktion bzw. nach dem ersten Rücklauf die Hälfte der Kindertageseinrichtung nachgekommen. Weitere Einrichtungen haben die Prüfaktion zum Anlass genommen einen Datenschutzbeauftragten für ihre Einrichtung zu benennen. Mithin kommen die Einrichtungen, bis auf wenige Ausnahmen, dieser Verpflichtung nach.

Anmelde- und Aufnahmeformulare

In den meisten Kindertageseinrichtungen werden für Anfragen nach einem Betreuungsplatz Anmeldeformulare genutzt. In einigen Einrichtungen ist dieser Prozess zentral über Onlineportale der Kommunen organisiert. Ist die Platzanfrage positiv, so kommt es in der Folge zum Abschluss eines Betreuungsvertrages. In diesem Schritt werden dann sog. Aufnahmeformulare verwendet, die Teil des Betreuungsvertrages sind.

In der Hälfte der Kindertageseinrichtungen gaben die verwendeten Anmelde- und Aufnahmeformulare keinen Anlass zur Beanstandung. In einigen Formularen sahen wir Nachbesserungsbedarf und haben dies gegenüber den Einrichtungen entsprechend angemerkt, Anpassungen angeregt und teilweise auch um Wiedervorlage der Formulare gebeten.

Häufig festzustellen war, dass im Aufnahmebogen der Einrichtungen Angaben zur Krankenversicherung, Versicherungsnehmer, Kinderarzt und überstandenen Krankheiten abgefragt werden. Diese Angaben sind nach Maßgabe des § 6 KDG nicht erforderlich. Für die Betreuung des Kindes ist es ausreichend, dass die Erzieher die gesundheitlichen Einschränkungen und ggf. Besonderheiten kennen.

Im Weiteren wurden häufig Angaben zu Geschwisterkindern und deren Geburtsdatum erhoben, wobei diese Abfrage nur erforderlich ist, wenn danach die Kostenbeiträge berechnet oder Geschwisterkinder bevorzugt aufgenommen werden. Zudem dürfte die Angabe des Geburtsjahrs bei entsprechender Notwendigkeit ausreichend sein.

Vereinzelt wurde auch nach dem Familienstand der Sorgeberechtigten, dem Beruf, dem Arbeitgeber und dem Umfang der Erwerbstätigkeit gefragt. Für diese Abfragen sehen wir keine Erforderlichkeit. Aus dem Familienstand lässt sich bei Weitem keine Aussage darüber ableiten, ob die Sorgeberechtigten zusammen oder getrennt leben bzw. ob es nur einen Sorgeberechtigten gibt. Daher ist es empfehlenswert nach der Wohnadresse der Sorgeberechtigten zu fragen. Diese Abfrage ist für den Abschluss eines Betreuungsvertrages erlaubt und notwendig.

Die Konfession des Kindes bzw. der Sorgeberechtigten darf abgefragt werden, wenn bei der Platzvergabe aufgrund der Konzeption der Einrichtung konfessionsangehörige Familien bevorzugt werden. In diesem Fall gilt nach § 6 Abs. 1 lit. f KDG das kirchliche Interesse als Zweck für diese Abfrage.

Fotoerlaubnis / Einwilligungserklärung

Bei der Überprüfung der Einwilligungserklärungen zum Anfertigen und Veröffentlichen von Fotos war auffällig, dass einige Einrichtungen mehrere Einwilligungserklärungen für unterschiedliche Verarbeitungs- und Veröffentlichungszwecke verwendet haben. So nutzen die Einrichtungen eine Erklärung für Bilder innerhalb einer Betreuungs- und Entwicklungsdokumentation, eine Erklärung für die Bilder außerhalb dieser Dokumentation und eine zusätzliche Erklärung zum Veröffentlichen in Pfarrbriefen, Zeitungen, Webseiten etc.. Aus datenschutzrechtlicher Sicht wurde dieses nicht beanstandet. Vermutlich sind diese Dokumente historisch gewachsen, d.h. mit neuen Verarbeitungs- oder Veröffentlichungszwecken wurden bereits bestehende Einwilligungserklärungen nicht überarbeitet, sondern neue Erklärungen zusätzlich ausgegeben. Viel hilft jedoch nicht immer viel, so dass bei vielen Erklärungen es auch für den Verantwortlichen schwieriger wird den Überblick zu behalten, wer in was eingewilligt hat. Entsprechende Hinweise sind erfolgt.

In einigen Formularen fehlte ein Hinweis für die Veröffentlichung im Internet. Denn trotz aller technischen Vorkehrungen kann nicht ausgeschlossen werden, dass die Fotos im Internet weltweit von beliebigen Personen abgerufen und weiterverwendet werden können. Die Veröffentlichung im Internet kann auch eintreten, wenn Fotos der Presse zur Verfügung gestellt werden. Daher sollte auch hier der Internet-Hinweis erfolgen oder sichergestellt werden, dass die Fotos nur in der gedruckten Presse veröffentlicht werden.

Weiterhin wurde in einigen Formularen nicht auf einen möglichen Widerruf gem. § 8 Abs. 6 KDG hingewiesen.

Ferner halten wir eine redaktionelle Nutzung von Fotos ohne zeitliche Begrenzung auch mit Zustimmung der Personensorgeberechtigten für nicht erforderlich, da der Zweck, zu dem diese angefertigt worden sind, nach Beendigung der Betreuungszeit entfällt.

In einigen Einrichtungen war kein Fotoverbot für Sorgeberechtigte und Abholende ausgesprochen worden. Um die Persönlichkeitsrechte aller zu wahren, ist zu empfehlen, dieser Personengruppe über die Hausordnung oder die Fotoerlaubnis ein Fotoverbot auszusprechen[23].

Viele Einrichtungen löschen Fotos und Unterlagen bzw. händigen diese an die Sorgeberechtigten aus, sobald der Zweck erfüllt ist oder das Kind aus der Einrichtung ausscheidet. Eine solche Verfahrensweise ist zu begrüßen. Sie wird dem Datenschutz sowie den Interessen der Sorgeberechtigten gerecht.

Fazit: In einigen Einrichtungen gibt es noch Nachbesserungsbedarf in der Gestaltung der Anmelde- und Aufnahmeformulare sowie den Fotoeinwilligungserklärungen. Die entsprechenden Einrichtungen worden unter Setzung einer Frist zur Abstellung dieser Mängel aufgefordert. Diese Mängel wurden bis dato zum Großteil behoben.

Jedoch gab es auch einige Einrichtungen, die nicht auf unsere Schreiben und Mahnungen reagiert haben. In diesen Fällen haben wir die Träger bzw. Trägervertretung aus dem bischöflichen Ordinariat konsultiert. Aufgrund

23 TB 2019, Pkt. 4

der bis zum Jahresende 2022 geführten Kommunikation zeichnet sich auch hier eine Lösung ab.

Die schriftliche Prüfaktion in den Katholischen Kindertagesstätte verlief insgesamt positiv. Aus den Rückläufen, Gesprächen mit den Einrichtungsleitungen, Trägern, Datenschutzbeauftragten oder Trägervertretern ergab sich der Eindruck, dass der Datenschutz einen hohen Stellenwert in den Einrichtungen hat. Hinweise und Handlungsempfehlungen unsererseits wurden angenommen und umgesetzt. Auch wenn nicht alle Unterlagen im ersten Rücklauf datenschutzrechtlich korrekt waren, kamen wir zu dem Ergebnis, dass die Bereitschaft zur Umsetzung der gesetzlichen Vorgaben im hohen Maß vorhanden ist.

3.2.5 Datenschutzkontrolle im Kindergarten

Zusätzlich zur Prüfaktion zur Benennung von betrieblichen Datenschutzbeauftragten in Kindertagesstätten hat unsere Dienststelle 2 weitere Kindertagesstätten vor Ort geprüft. Somit waren die Kindertagesstätten im Berichtszeitraum 2022 eindeutiger Schwerpunkt im Bereich des Referates Kinder und Jugend.

Der Vorteil von Vorortterminen ist, dass unsere Dienststelle einen Eindruck über die örtlichen Gegebenheiten der Einrichtung bekommt, der das Ermessen der datenschutzrechtlichen Bewertung beeinflussen kann. Zudem halten wir es für sinnvoll mit den Verantwortlichen und sonstigen Beteiligten über den Datenschutz ins Gespräch zu kommen, um Hemmnisse und Vorbehalte abzubauen.

Verantwortlicher

Die beiden geprüften Einrichtungen sind jeweils in Trägerschaft einer Pfarrei. Datenschutzrechtlich verantwortlich sind jedoch die beiden Kindertagesstätten selbst bzw. die Einrichtungsleitung, da diese über Zweck und Mittel der Datenverarbeitung entscheiden und Weisungen gegenüber Mitarbeitenden und Betroffenen sowie auch Sorgeberechtigten aussprechen.

Verpflichtungserklärungen und Schulungen der Mitarbeitenden

In beiden Kindertagesstätten hatten alle Mitarbeitenden die Verpflichtungserklärung auf das Datengeheimnis unterzeichnet. Auch die Leitungen waren im Datenschutz geschult. Beiden Einrichtungen wurde jedoch die Empfehlung ausgesprochen auch die Mitarbeitenden in grundlegenden Datenschutzangelegenheiten zu schulen bzw. das Thema Datenschutz in die Dienstbesprechungen aufzunehmen.

Einwilligungserklärung (Fotoerlaubnis)

Die Einwilligungserklärungen der Einrichtungen wiesen einige Mängel auf, die wir im direkten Gespräch angesprochen und erklärt haben. Im Nachgang unserer Prüfung wurde die Erklärungen den Erfordernissen einer gültigen Einwilligungserklärung angepasst.

In der ersten Einrichtung wurde bemängelt, dass ein Hinweis für die Veröffentlichung im Internet auf den Formularen nicht vorhanden ist. Werden Fotos der Kinder durch die Auswahl der Zweckbestimmung auch im Internet veröffentlicht, so muss der Hinweis erfolgen, dass Fotos im Internet weltweit von beliebigen Personen abgerufen werden können und es trotz aller technischen Vorkehrungen nicht ausgeschlossen werden kann, dass die Fotos weiterverwendet werden.

In der anderen Einrichtung war die Zweckbestimmung für die Verwendung der Fotos nicht eindeutig differenziert genug. Auch hier haben wir entsprechende Hinweise zur Verbesserung erteilt.

Anmelde- / Aufnahmeprozess

In beiden Einrichtungen gab es seitens unserer Dienststelle im Anmelde- und Aufnahmeprozess nichts zu beanstanden. Unterlagen angemeldeter Kinder, die keinen Platz in der Einrichtung bekommen haben, werden nach Ende einer Nachrückzeit vernichtet.

Bei der Aufnahme werden nur die für das Vertragsverhältnis erforderlichen Angaben erfragt.

Erreichbarkeit im Feierabend / Diensthandy

In einer Einrichtung sind Diensthandys im Einsatz, über die die Mitarbeitenden kommunizieren können. Die Diensthandys sind mit einem geeig-

neten Messanger ausgestattet, über den u.a. Dienstzeiten abgesprochen oder kurzfristige Vertretungen arrangiert werden.

In der zweiten Einrichtung hatten die Mitarbeitenden zusammen mit der Leitung eine private Chat-Gruppe gegründet. In der Chatgruppe wurde mit der privaten Rufnummer sowie mit dem privaten Handy kommuniziert. Als Grund nannte man uns die kurzfristige Organisation von Vertretungen im Krankheitsfall. Die Einrichtungsleitung selbst war von dieser Lösung nur wenig überzeugt, da diese sich im wohlverdienten Wochenende bereits Gedanken über die Dienstorganisation der nächsten Woche machte, wenn Krankmeldungen beispielsweise am Wochenende eintrafen. Unsere Dienststelle hat angeregt eine Frühdienst- oder Vertretungsregelung einzuführen, die dann nur die entsprechenden Mitarbeiter betrifft. Dienstliche Angelegenheiten jedoch über private Geräte und Messanger zu klären, sollte unterbleiben.

Videoüberwachung

Da eine der Kindertageseinrichtungen ruhig am Waldrand gelegen war, war diese leider häufig Ziel von Einbrüchen und Vandalismus. Aus diesem Grund wurden Videoüberwachungskameras angebracht. Ein Konzept zur Videoüberwachung ist vorhanden und wurde uns vorgelegt. Die Videokameras werden erst nach Feierabend aktiviert, die Speicherdauer beträgt maximal 72 h, mit Ausnahme in der Schließzeit. Die Videoüberwachung sahen wir begründet und gut umgesetzt. Empfehlungen wurden noch zur Ergänzung der Hinweisschilder ausgesprochen.

Fazit: Auch die Vorortttermine in den Einrichtungen verliefen insgesamt positiv. Die Einrichtungsleitungen sind sehr bestrebt die datenschutzrechtlichen Vorgaben umzusetzen und einzuhalten. Manchmal sind noch Unsicherheiten vorhanden, wie bestimmte Dinge umgesetzt oder eingehalten werden können. Wir haben dies bezüglich angeboten regelmäßig Videosprechstunden zum Thema Datenschutz im Kindergarten anzubieten, um Verantwortlichen und auch den Datenschutzbeauftragten eine Möglichkeit des Austauschs anzubieten.

3.3 Datenschutzvorfälle

3.3.1 Abschiedsmail im großen Stil

Ein ehemaliger Mitarbeitender einer Einrichtung hat unter dem Betreff „Ende meiner Tätigkeit“ eine E-Mail an 367 Empfänger versendet. In der E-Mail teilte der Mitarbeitende mit, dass das Dienstverhältnis mit der Arbeitgeberin endet.

Den Empfängerkreis hatte der Mitarbeitende in das Feld „CC“ eingetragen. Durch den Eintrag an dieser Stelle war allen Empfängern ersichtlich, wer diese E-Mail erhalten hat. Darüber hinaus waren dienstliche und private E-Mail-Adressen von allen Adressaten für alle Empfänger offenkundig.

E-Mail-Adressen sind personenbezogene Daten. Die Verarbeitung personenbezogener Daten ist grundsätzlich nicht erlaubt, soweit nicht eine der Bedingungen des § 6 Abs. 1 KDG erfüllt ist. Vorliegend käme als eine solche Bedingung des § 6 Abs. 1 KDG eine vom Betroffenen erteilte Einwilligung in Betracht.

Die im Anhörungsverfahren vorgelegte Einwilligungserklärung autorisierte die Nutzung der privaten E-Mail-Adressen ausschließlich zur Kommunikation im Rahmen der ehrenamtlichen Tätigkeit. Einwilligende erklären sich damit also nur bereit, dass ihre private E-Mail-Adresse zur Informations- und Postübermittlung an sie verwendet werden darf, soweit diese das Ehrenamt betreffen.

Keineswegs ist damit eine Einwilligung zur Offenlegung ihrer personenbezogenen Daten gegenüber allen Mitarbeitenden des Verantwortlichen und weiteren Ehrenamtlichen erteilt.

Weiterhin sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und der Aufwand nicht außer Verhältnis zum angestrebten Schutzzweck steht. Vorliegend wäre es ohne zusätzlichen Aufwand möglich gewesen, die E-Mail-Adressen im Feld „BCC“ einzutragen und somit nicht allen Empfängern offen zu legen.

Dieser Datenschutzverstoß wurde durch die Datenschutzaufsicht beanstandet und Auflagen für durchzuführende Sensibilisierungsmaßnahmen erteilt.

3.3.2 Bekannte aus früheren Zeiten

Im Rahmen eines kurzen Zeitfensters war es autorisierten Benutzern der kirchlichen Meldewesen-Anwendung (e-mip) aufgrund einer Fehlkonfiguration möglich, ohne Mandatierung auch Personen anderer Diözesen einzusehen. Dieses „Leck" war den Benutzern erst aufgefallen, nachdem in ihren Suchergebnissen auch Personen außerhalb ihres erlaubten Zugriffsbereich „auftauchten".

Obwohl es den Benutzern klar war, dass für diese Einsichtnahme keine Berechtigung vorlag, verspürten einige Nutzer doch eine große Neugier, um nach Bekannten oder Weggefährten aus früheren Zeiten zu suchen.

Der unautorisierte Zugriff war ausschließlich lesend möglich, wurde jedoch protokolliert, so dass die unzulässigen Nutzeranwendungen zurückverfolgt werden konnten.

Da die Ursache für diesen Datenschutzverstoß nicht Vorsatz war, sondern Fahrlässigkeit aufgrund von mangelndem Wissen sowie Unachtsamkeit im Rahmen der Aufgabenerfüllung, wurden die Verantwortlichen beauflagt, alle Mitarbeitenden, die diese Anwendung nutzen, anlassbezogen zu schulen.

4 Datenschutz im Gesundheitswesen

4.1 Datentransparenzverfahren - Gesundheitsdaten in der Forschung

Gesundheitsdaten gehören zu den sensibelsten Daten einer Person. Sie geben aber auch Einblick in aktuelle gesellschaftliche Entwicklungen, die Häufigkeit von Krankheiten oder den Bedarf an bestimmten Medikamenten. Das Datentransparenzverfahren soll die pseudonymisierte Weitergabe von Gesundheitsdaten an die Forschung möglichen machen.

Das Wichtigste kurz und knapp

- Das Datentransparenzverfahren sieht vor, dass gesetzliche Krankenkassen als Datensammelstelle handeln und Gesundheitsdaten aller Versicherten den Forschungsinstituten zur Verfügung stellen.
- Die Datensätze und Patientenakten sollen pseudonymisiert werden, um keine Rückschlüsse auf einzelne Patienten ziehen zu können. Kritiker sehen trotzdem den Datenschutz gefährdet.
- Einzelne Datensätze werden zwar nicht an die Forschungsinstitute herausgegeben, die Daten geben aber Aufschluss über den Gesundheitsverlauf. Patienten mit seltenen Erkrankungen haben bereits Klagen eingereicht, weil sie Rückschlüsse auf ihre Person befürchten. Eine Klage erreichte bereits das Bundesverfassungsgericht.

Was ist das Datentransparenzverfahren[24]?

Aktuell sind rund 73 Millionen Menschen bei einer gesetzlichen Krankenkasse registriert - es handelt sich also um eine erhebliche Datenmenge, die der Forschung zur Verfügung gestellt werden soll. Werden diese Daten nicht ausreichend geschützt, sind tiefe Einblicke in die privatesten Bereiche der Versicherten möglich.

Ziel des Datentransparenzverfahrens ist es, Gesundheitsdaten durch die Krankenkassen zu sammeln und der Forschung zur Verfügung zu stellen, um wichtige Erkenntnisse für die gesundheitliche Versorgung der Bevölkerung zugewinnen.

Gesundheitsdaten stehen jedoch unter einem besonderen Schutz (Art. 9 Abs. 1 DS-GVO / § 11 Abs. 1 KDG). Das hierzu in Kraft getretene Gesetz (Digitale-Versorgung-Gesetz [DVG]), weicht diesen Schutz jedoch deutlich auf, um der Forschung repräsentative Daten zur Verfügung stellen zu können.

Das Bundesministerium für Gesundheit, damals unter der Leitung von Jens Spahn, stellte im September 2020 eine sog. Roadmap vor.

24 Rechtsquellen: Datentransparenzverordnung, in Neufassung vom 19.Juni 2020; Digitale-Versorgung-Gesetz (DVG), mit dem die Transparenzverordnung geändert wurde

Neben dem Ziel, Gesundheitsdaten der Bevölkerung für die Forschung nutzbar zu machen, waren darin noch drei weitere Ziele verankert:

1. Durch wissenschaftsbasierte Auswertung die **Patientenversorgung verbessern**,
2. durch die Analyse der Daten den medizinischen **Fortschritt vorantreiben**,
3. die Innovationskraft Deutschlands steigern und dadurch **Arbeitsplätze sichern** und **Wohlstand** ausbauen.

Um dieses Ziel zu erreichen, soll **bis 2025** die Strukturen zur digitalen Gesundheitsversorgung und -forschung weiter ausgebaut werden, aber auch die Datensicherheit vorangetrieben werden.

Datenschutz durch Pseudonymisierung ausreichend?

Festgeschrieben ist, dass Patientendaten bereits bei den Krankenkassen pseudonymisiert werden. Gesundheitsdaten können so ohne Namen und Krankenversichertennummer an das Robert-Koch-Institut (RKI) weitergegeben werden. Forschungszentren dürfen keine Einzeldatensätze, sondern nur gesammelte Datensätze erhalten. Die pseudonymisierten Gesundheitsdaten sollen keine Rückschlüsse auf einzelne Patienten zulassen.

In der Kritik steht, dass die weitergegebenen Daten von den Krankenkassen lediglich pseudonymisiert werden:

Bei einer **Pseudonymisierung** werden nur der Name und andere Angaben durch eine Kennziffer oder ein Kennzeichen ersetzt, um eine Identifizierung zu erschweren. Anders als bei einer Anonymisierung ist es aber nicht unmöglich, die betroffene Person zu identifizieren.

Nur bei einer **Anonymisierung** lassen sich Informationen nicht mehr auf eine Person beziehen. Rückschlüsse auf die Identität einer Person sind hier also wesentlich unwahrscheinlicher als bei einer Pseudonymisierung.

Bei den meisten Menschen fällt das Risiko einer Identifizierung eher gering aus. Anders ist das Identifizierungsrisiko jedoch bei Menschen mit seltenen Erkrankungen. Hier ist das Risiko signifikant erhöht. Es ist daher anzunehmen, dass insbesondere diese Menschen von einem erhöhten Missbrauchsrisiko im Hinblick auf ihre Daten betroffen sind.

Ob das Datentransparenzverfahren mit der DS-GVO und den Werten auf EU-Ebene in Einklang steht, ist unklar.

Folgende Punkte werden kritisiert:

- **fehlende Anonymisierung**
- Betroffenen steht **kein Widerspruchsrecht** zu, welches nach der DSGVO für Datenverarbeitungen jeglicher Art jedoch zwingend vorgeschrieben ist.
- **fehlenden Auskunftsrechte,** wodurch auch der grundrechtliche Schutz der informationellen Selbstbestimmung zumindest eingeschränkt ist.

DVG vor Gericht: Klagen gegen das Datentransparenzverfahren

Bereits im März 2020 wurde ein Eilverfahren beim Bundesverfassungsgericht (BVerfG) anhängig gemacht[25]. Der Antragsteller befürchtete, durch das DVG trotz Pseudonymisierung identifiziert zu werden. Er begründete seine Bedenken damit, dass er an einer seltenen Erbkrankheit leide, die in Kombination mit anderen Angaben in seiner Patientenakte zu seiner Identifikation führen könne.

Das BVerfG hat den Erlass einer einstweiligen Anordnung mit folgender Begründung abgelehnt:

- Nicht ausgeschlossen werden kann, dass tiefe Eingriffe in das Persönlichkeitsrecht möglich seien, jedoch fehle es an einer konkreten Betroffenheit des Antragstellers, da es noch nicht zu einer Identifizierung anhand der Daten gekommen sei.
- Erst wenn die Pseudonymisierung im konkreten Fall fehlschlagen würde, sei ein erheblicher Grundrechtseingriff gegeben. Für das Gericht überwogen die drohenden Nachteile für die Forschung, sollte die Regelung vorläufig außer Kraft gesetzt werden.
- Das BVerfG stellte aber klar, dass die Entscheidung im Eilverfahren vorläufig sei und es erst im Hauptsacheverfahren (Verfassungsbeschwerde) umfassende Abwägungen treffen und das Gesetz endgültig beurteilt könne.

25 BVerfG, Beschluss vom 19. März 2020 - 1 BvQ 1/20

Eine weitere Klage wurde durch ein Mitglied des Chaos-Computer-Clubs vor dem Sozialgericht Berlin eingereicht.

- Seit Mitte Oktober 2022 wird darüber verhandelt, ob die Gesundheitsdaten aller gesetzlich Versicherten in Deutschland der Forschung zur Verfügung gestellt werden dürfen.
- Die Klägerin befürchtet, dass durch Datenlecks und unzureichende Datenschutzmechanismen ihre Daten in falsche Hände gelangen könnten. Sie sieht nicht die Datensammlung als solche, sondern den zu erwartenden Mangel an Datenschutz, kritisch.
- Das Sozialgericht machte deutlich, erst einmal selbst den Fall behandeln zu wollen, statt den Fall direkt an den Europäischen Gerichtshof weiterzugeben. Wie das Urteil ausfällt, ist derzeit noch unklar.

Fazit: Der Zweck des Datentransparenzverfahrens ist klar und zum Teil auch nachvollziehbar, denn nur durch Forschung können die Medizin und die Patientenversorgung in Deutschland weiter vorangetrieben werden. Anonymisierte Gesundheitsdaten könnten der Forschung wichtige Informationen liefern. Eine Voraussetzung dabei ist, dass es sich um große bzw. repräsentative Datenmengen handeln muss, die eine ordentliche Grundlage für wissenschaftliche Erkenntnisse bietet. Dabei darf jedoch nicht der Datenschutz vernachlässigt werden. Wenn Gesundheitsdaten in falsche Hände gelangen, sind nicht nur einzelne Personen gefährdet, sondern u. U. auch die aus der Forschung gewonnenen Erkenntnisse.

4.2 Die elektronische Arbeitsunfähigkeitsbescheinigung – was ist datenschutzrechtlich zu beachten?

Die Digitalisierung im Gesundheitswesen schreitet voran. Am 01.01.2020 trat das Bürokratieentlastungsgesetz III in Kraft. Dieses Gesetz nutzt die Chance der Digitalisierung, um die „Zettelwirtschaft" in vielen Bereichen abzuschaffen. Ab dem **01.01.2023** werden Arbeitgebern die Arbeitsunfä-

higkeitsbescheinigungen Ihrer Mitarbeiter durch die Krankenkassen nur noch elektronisch bereitgestellt.

Die Datenübermittlung erfolgt in zwei Schritten:

1. Die Daten zur Arbeitsunfähigkeit werden durch den Arzt an die zuständige gesetzliche Krankenkasse übermittelt.
2. Nach Eingang der Arbeitsunfähigkeitsdaten bei der Krankenkasse erstellt diese eine Meldung für den Arbeitgeber zum Abruf dieser Daten.

Welche Daten werden durch die Krankenkasse an den Arbeitgeber übermittelt?

Gem. § 109 Abs. 1 SGB IV werden folgende Daten an den Arbeitgeber übermittelt:

- Name des Beschäftigten
- Beginn und Ende der AU
- Datum der ärztlichen Feststellung der AU
- Kennzeichnung als Erst- oder Folgemeldung
- Angabe, ob Anhaltspunkte dafür vorliegen, dass die Erteilung der AU auf einen Arbeitsunfall oder sonstigen Unfall zurückzuführen ist oder auf den Folgen eines Arbeitsunfalls oder sonstigen Unfalls beruht.

Es werden mithin nur noch die wirklich wesentlichen Informationen zur Arbeitsunfähigkeit übermittelt. Der Arbeitgeber kann daher nicht mehr anhand des Stempels des Facharztes auf der AU-Bescheinigung Rückschlüsse auf die Art der Erkrankung ziehen. Aus datenschutzrechtlicher Sicht ist dies zu begrüßen.

Worauf müssen Arbeitgeber achten?

Bei der Implementierung des Tools muss die Sicherheit der Daten nach Art. 32 DS-GVO durch geeignete technische- und organisatorische Maßnahmen gewährleistet werden. Folgendes ist zu beachten:

- Ein Abruf dieser Daten durch den Arbeitgeber kann dann erfolgen, wenn der Arbeitnehmer bei ihm beschäftigt ist und er diesen über seine Arbeitsunfähigkeit in Kenntnis gesetzt hat.

- Um ein angemessenes Schutzniveau zu erhalten ist eine verschlüsselte Datenübertragung sicherzustellen.
- Das Tool muss die Umsetzung der Betroffenenrechte nach Art. 12 – 23 DS-GVO sowie die Ausführung der Löschung nach Art. 17 DS-GVO ermöglichen.

Das Mitbestimmungsrecht von Mitarbeitervertretungen ist aufgrund der gesetzlichen Vorgaben zum Inhalt eingeschränkt (§ 109 I SGB IV n. F.).

Fazit: Die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) ist ein digitales Verfahren für Krankmeldungen von gesetzlich Krankenversicherten – und zwar bundesweit. „Gelbe Scheine" gehören somit der Vergangenheit an. Krankenkassen und Arbeitgebern bekommen die Arbeitsunfähigkeitsbescheinigungen schneller übermittelt. Der Arbeitnehmer selbst muss sich nicht mehr um die Zustellung der AU kümmern. Arbeitnehmende haben jedoch weiterhin einen Anspruch auf Ausstellung der AU-Bescheinigung in Papierform, um z.B. im Störfall - wie etwa bei einer fehlgeschlagenen Übermittlung im elektronischen Verfahren - das Vorliegen der Arbeitsunfähigkeit, die Voraussetzung für die Entgeltfortzahlung ist, sicher nachzuweisen. Daran soll festgehalten werden, bis ein für den Nachweis der Arbeitsunfähigkeit gegenüber dem Arbeitgeber geeignetes elektronisches Äquivalent mit gleich hohem Beweiswert zur Verfügung steht. Die eAU bedeutet eine Erleichterung für alle Seiten.

4.3 Datenschutzvorfälle

4.3.1 Vermeintliche Kindswohlgefährdung / offensichtlich übers Ziel hinausgeschossen

Bereits im Jahr 2020 beschwerte sich eine Petentin über die Art und Weise der Behandlung in einem Krankenhaus und bat um rechtliche Überprüfung. Nach den Schilderungen der Verantwortlichen und der Petentin lag dem gemeldeten Datenschutzverstoß folgender Sachverhalt zugrunde.

Die Petentin begab sich nach einer Hausgeburt mit einem Neugeborenen in den Nachtstunden in das Klinikum. Aufgrund der Tatsache, dass die Pla-

zenta noch nicht abgegangen war, war eine operative Entfernung erforderlich. Nach dem Eingriff wollte die Petentin das Klinikum umgehend wieder verlassen, womit die diensthabende Ärztin nicht einverstanden war, da sie es als medizinisch nicht vertretbar ansah. Hinzu kam, dass eine Untersuchung des Kindes (U 1) durch einen Kinderarzt der Klinik erfolgen sollte.

Nachdem die Petentin einige Stunden auf die angekündigte Untersuchung gewartet hatte, wurde ihr auf Nachfrage mitgeteilt, dass sie noch warten müsse, da die Kinderärztin noch nicht im Dienst ist. Die Petentin erklärt daraufhin, nicht länger warten zu wollen. Die U-Untersuchung wurde dann von einer Hebamme der Klinik durchgeführt. Während des Aufenthalts in der Klinik erwähnte die Petentin, dass sie einen 7-jährigen Sohn habe, der zu Hause sei. Die Petentin hat nach der U-Untersuchung die Klinik verlassen, wobei die diensthabende Ärztin deutlich ihr Missfallen zeigte.

Im Mutterpass der Petentin waren die Kontaktdaten einer Hebamme hinterlegt. Dies hat die zuständige Oberärztin dazu genutzt, telefonisch Kontakt zu dieser Hebamme aufzunehmen und sie über die Geburt zu informieren. In einer ersten Einlassung hat die Verantwortlichen angegeben, dass bekannt war, dass die Betreuung durch diese Hebamme lediglich kurzzeitig vor der Geburt erfolgte. Ob die Petentin ausdrücklich darauf hingewiesen hatte, dass der Betreuungsvertrag mit der Hebamme beendet war, konnte im Laufe des Verfahrens nicht eindeutig geklärt werden.

Die Hebamme hat sodann der Petentin mitgeteilt, dass die Klinik sie über die Geburt telefonisch informiert habe. Die Verantwortliche hat zwar eingeräumt, dass eine Kontaktaufnahme stattgefunden hat, aber behauptet, das Gespräch sei sofort beendet worden, als die Hebamme darauf hingewiesen hat, dass sie die Petentin nicht mehr betreut. Das dies nicht der Wahrheit entsprach, hat die Petentin im Laufe des Verfahrens, nach dem sie Einblick in ihre Patientenakte genommen hatte, festgestellt, da diese einen längeren Gesprächsvermerk über dieses Telefonat enthielt. Unbestritten lag jedoch eine Einwilligung zur Datenübermittlung an Vor- und Weiterbehandler, d. h. auch an die Hebamme, nicht vor.

Die Verantwortliche hat zudem auch das Jugendamt eingeschaltet und dieses über den Verdacht einer Kindswohlgefährdung informiert. Begründet wurde dies u.a. mit der „angeblichen“ Weigerung die U-1-Untersu-

chung des Neugeborenen in der Klinik durchführen zu lassen sowie damit, dass der Aufenthaltsort des 7-jährigen Erstgeborenen und dessen Aufsichtsperson, während des Klinikaufenthaltes der Mutter, nicht bekannt gewesen sei, da diese trotz Nachfragen hierzu keine Angaben gemacht hatte. Auch der Umstand, dass die Petentin keine Angaben zum Kinderarzt des Neugeborenen gemacht hatte, wurde als Rechtfertigungsgrund für die Einschaltung des Jugendamtes angeführt.

Die Verantwortliche hat sowohl im Ermittlungsverfahren als auch im Verfahren vor dem Datenschutzgericht behauptet, die Petentin habe die U-Untersuchung ihres Kindes in der Klinik verweigert. Dem konnte jedoch durch Vorlage des U-Heftes entgegengetreten und mithin der Nachweis erbracht werden, dass diese Untersuchung von einer Hebamme der Klinik vorgenommen worden ist.

Der im Sachverhalt geschilderte Vorgang stellte aus Sicht unserer Aufsicht eine meldepflichtige Verletzung gegen Regelungen des KDG dar, weil mit dieser Verletzung eine Gefahr für die Rechte und Freiheiten der Betroffenen verbunden ist. Nach Ansicht unserer Aufsicht waren die Einbeziehung der Hebamme und des Jugendamtes rechtswidrig. Die Verletzung wurde seitens unserer Aufsicht beanstandet. Gegen diese Entscheidung hat die Verantwortliche Rechtsmittel eingelegt. Das IDSG hat sich unserer Rechtsauffassung angeschlossen.

Kontaktaufnahme mit der Hebamme

Die Information an die Hebamme über die Entbindung stellt eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts in der Ausprägung des Rechts auf informationelle Selbstbestimmung dar, da ein Dritter, die für die Betroffene relevanten Informationen, die dem persönlichen Bereich der Betroffenen zuzuordnen sind, erhält. Diese Nachricht enthält darüber hinaus personenbezogene Daten besonderer Kategorie gem. § 4 Nr. 2 KDG. Zu dieser Kategorie der personenbezogenen Daten zählen u.a. auch persönliche Gesundheitsdaten im Sinne des § 4 Nr. 17 KDG, mithin auch die Information über die Geburt eines Kindes.

Da eine Zustimmung zur Datenübermittlung an Vor- und Weiterbehandlung (Hebamme) nicht erteilt worden war, hätte eine Kontaktaufnahme mit

der Hebamme in keinem Fall erfolgen dürfen. Wir haben in der Übermittlung dieser Information (Geburt eines Kindes) einen Datenschutzverstoß gesehen. Dieser Auffassung hat sich das IDSG angeschlossen. Der Verantwortliche der Klinik hatte zwar einen Verstoß gegen die ärztliche Schweigepflicht gem. § 203 StGB zugestanden, das Vorliegen eines damit verbundenen Datenschutzverstoßes jedoch abgelehnt.

Die Offenbarung von Patientendaten gegenüber der Hebamme stellt eine Verarbeitung i.S. v. § 4 Nr. 3 KDG dar. Ein Verarbeiten personenbezogener Daten bzw. personenbezogener Daten besonderer Kategorie ist gem. § 6 Abs. 1 KDG, § 11 Abs. 1 KDG nur zulässig, wenn eine der dort genannten Bedingungen erfüllt ist, es sei denn einer der in § 6 Abs. 2, § 11 Abs. 2 KDG benannten Erlaubnistatbestände ist einschlägig.

Auch das IDSG sah keine Rechtmäßigkeit für die Verarbeitung der Daten durch Offenlegen gegenüber der Hebamme, da keiner der Erlaubnistatbestände erfüllt war und auch keine Einwilligung der Betroffenen vorlag. Die Kontaktaufnahme mit der Hebamme war deshalb rechtswidrig.

Benachrichtigung des Jugendamtes

Das IDSG sah auch in der Benachrichtigung des Jugendamtes einen Datenschutzverstoß. Die von der Klinik angeführten Gründe, die angebliche Verweigerung der Untersuchung des Neugeborenen durch einen Kinderarzt der Klinik, der Umstand, dass die Betroffenen keine Angaben zum nachbehandelnden Kinderarzt und keine Angaben zur Betreuung ihres Erstgeborenen gemacht hatte sowie das Argument, dass keine Unterlagen vorgelegt worden sind, aus denen sich eine ausreichende Schwangerschaftsvorsorge, Feindiagnostik und ambulante ärztliche Versorgung ergab, ließ das Gericht nicht als Rechtfertigung zu.

Die dem Jugendamt überlassenen Informationen enthalten, wie bereits ausgeführt, personenbezogene Daten und personenbezogene Daten der besonderen Kategorien. Die Verarbeitung dieser Daten ist nur unter strengen Voraussetzungen zulässig. Von der Verantwortlichen wurde als Rechtsgrundlage für die Weitergabe der Daten an das Jugendamt § 6 Abs. 1 lit. d KDG i. V. m. § 4 Abs. 3 des Gesetzes zur Kooperation und Information im Kinderschutz (KKG) benannt.

Nach § 4 Abs. 3 KKG sind die Berufsgeheimnisträgerinnen und Berufsgeheimnisträger für den Fall, dass das Gespräch nach § 4 Abs.1 KKG die Gefährdung nicht abwenden konnte oder ein solches Gespräch nicht in Betracht kommt, befugt, das Jugendamt ohne Einwilligung der Betroffenen zu informieren, wenn das für erforderlich gehalten wird. Hierauf sind die Betroffenen vorab hinzuweisen, es sei denn ein solches Vorgehen würde den wirksamen Schutz des Kindes bzw. des Jugendlichen infrage stellen.

Das bedeutet, dass Berufsgeheimnisträger das Jugendamt informieren können, wenn gewichtige Anhaltspunkte für die Gefährdung eines Kindes vorliegen und die Gefährdung nicht anders abgewendet werden kann. Die Annahme muss auf konkreten Tatsachen beruhen und eine Information des Jugendamtes muss den Grundsatz der Verhältnismäßigkeit wahren. Eingriffe in elterliche Rechtspositionen sind nicht schon dann gerechtfertigt, wenn damit eine optimale Betreuung gewährleistet werden soll, sondern erst wenn das körperliche, geistige oder seelische Wohl des Kindes tatsächlich gefährdet ist. Die durch Art. 6 Abs. 2 Satz 1 GG garantierte primäre Zuständigkeit der Eltern beruht darauf, dass angenommen wird, die Eltern können die Interessen des Kindes in der Regel am besten wahrnehmen.

Das Gericht vertrat insoweit - wie unsere Aufsicht auch – die Ansicht, dass in derartigen Fallkonstellationen keinen Ermessenspielraum besteht und die Vorgaben des § 4 Abs. 3 KKG zwingend einzuhalten sind.

Auch das Gericht konnte eine akute Kindswohlgefährdungslage, die die Einschaltung des Jugendamtes -zudem ohne Benachrichtigung der Petentin-, aufgrund der vorgebrachten Gründe nicht erkennen. Die Petentin war nicht verpflichtet alle medizinisch möglichen Vorsorgeuntersuchungen wahrzunehmen, Angaben dazu zu machen, wo sich ihr 7-jähriges Kind aufhält und durch wen es betreut wird. Gleiches gilt für die Angaben zum Kinderarzt des Neugeborenen.

Die Einschaltung des Jugendamtes ohne Benachrichtigung der Betroffenen ist die letztmögliche und eingreifendste Maßnahme. Das Gericht wies in der mündlichen Verhandlung die Prozessvertreter der verantwortlichen Klinik darauf hin, dass die Verfahrensabläufe, wie sie in § 4 KKG festgelegt sind, zwingend einzuhalten sind und eine Ermessensspielraum nicht besteht. Das Gericht schloss sich der Auffassung unserer Aufsicht an und

sah die Einschaltung des Jugendamtes als unverhältnismäßig und mithin rechtswidrig an.

Organisationsmangel

Das Gericht hat auch unsere Ansicht bestätigt, dass das von unserer Aufsicht gerügte Fehlen von Anweisungen, wie im Fall des Verdachtes einer Kindswohlgefährdung vorzugehen ist, den Verstoß ermöglicht hat und mithin ein Verstoß gegen § 26 KDG (Organisationsverschulden) gegeben ist. Da dadurch personenbezogene und personenbezogene Daten der besonderen Kategorie sowohl der Hebamme als auch Mitarbeitern des Jugendamtes bekannt gegeben worden sind, deren Rechtmäßigkeit nicht gegeben ist, sah es das Gericht als erforderlich an, dass eine interne Anweisung zu implementieren ist, die regelt, wie in Fällen des Verdachts einer Kindswohlgefährdung vorzugehen ist, um zu verhindern, dass personenbezogene und personenbezogene Daten besonderer Kategorie wie geschehen, unberechtigt offengelegt werden.

Die Speicherung, Nutzung und Verarbeitung personenbezogener Daten ist nur unter eng gesteckten Grenzen zulässig, da das Recht auf informationelle Selbstbestimmung, das sich aus dem allgemeinen Persönlichkeitsrecht herleiten lässt, personenbezogenen Daten unter besonderen Schutz stellt. Nur wenn der Betroffene zustimmt oder eine rechtliche Vorgabe dies erlaubt, können öffentliche und nicht öffentliche Stellen personenbezogenen Daten erheben, speichern, nutzen und verarbeiten.

Sie müssen sich dabei jedoch maßgeblich an die Datenschutzgrundsätze halten. Ein wichtiger Aspekt hierbei sind die Prinzipien von Datensparsamkeit und Datenvermeidung.

Gem. § 26 Abs. 1 KDG ist der Verantwortliche verpflichtet unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können. Gem. § 26 Abs. 2 KDG sind bei der Beurteilung des angemes-

senen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Insofern ist es erforderlich, dass der Verantwortliche verbindliche Handlungsanweisungen festlegt, wie im Fall einer Kindswohlgefährdung zu verfahren ist.

Zu regeln ist in einem Ablaufplan Folgendes:

1. Wer ist zu informieren/einzubeziehen?
2. Wer gehört zu meiner kollegialen Beratungsgruppe?
3. Wen kann ich ansprechen?
4. Wer ist meine insoweit erfahrene Fachkraft im Sinne von § 4 Abs. 1 Nr. 2 KKG?
5. Wer hat die Verantwortung für den Fall?
6. Wer dokumentiert den Fallverlauf?

Daher sind Vordrucke bzw. Checklisten, Risiko-Checkbogen entsprechend des Prüfschemas des Nationalen Zentrum Frühe Hilfen zu erstellen und den Mitarbeitenden zur Verfügung zu stellen.

Zurechnung des Datenschutzverstoßes

Das Verhalten der Mitarbeiter der Klinik ist dieser über die Anwendung des Funktionsträgerprinzips zuzurechnen. Nach der Auffassung der Datenschutzkonferenz des Bundes und der Länder (DSK) ist der funktionale Unternehmensbegriff und das Funktionsträgerprinzip aufgrund des Willen des europäischen Gesetzgebers (vgl. Erwägungsgrund 150 Satz 3 DS-GVO) von den Datenschutzaufsichtsbehörden bei der Bußgeldverhängung anzuwenden.

Auch nach der ständigen Rechtsprechung des Interdiözesanen Datenschutzgerichts (IDSG) haftet eine juristische Person als Verantwortliche für schuldhafte Datenschutzverstöße ihrer Beschäftigten, auch wenn diese

keine Organstellung -etwa als Geschäftsführer einer GmbH- oder sonstige Führungsposition innehat[26].

Eine Haftung einzelner Beschäftigter scheidet danach aus. Datenschutzrechtliche Sanktionen (Beanstandungen und auch Bußgelder) können deshalb nur gegen Verantwortliche und Auftragsverarbeiter verhängt werden.

Das Prekäre an diesem Fall bestand nicht allein in dem geschilderten Sachverhalt. Gegen den von unserer Behörde erlassenen Bescheid hat die Verantwortliche, wie bereits ausgeführt, Klage vor dem IDSG erhoben. Im Klageverfahren wurde der Sachverhalt von der Verantwortlichen vorsätzlich wahrheitswidrig dargestellt, um ihr Handeln zu rechtfertigen. Die Verantwortliche hatte ausgeführt, dass die Betroffene die U-Untersuchung verweigert hatte, was nachweislich nicht der Fall war, da diese noch in der Klinik vorgenommen worden war. Da die Betroffene Einsicht in ihre Patientenakte verlangt und eine Kopie dieser Akte angefordert (gem. § 17 KDG) hatte, konnte auch die Behauptung der Verantwortlichen im Verfahren (auch noch vor dem IDSG), das Gespräch mit der Hebamme der Petentin sei unmittelbar, nachdem diese mitgeteilt hat, dass der Betreuungsvertrag nicht mehr besteht, beendet worden, widerlegt werden. Diese Patientenakte enthielt eine ausführliche Gesprächsnotiz von dem Telefonat zwischen einer Ärztin der Klinik und der Hebamme.

Auch gegenüber unserer Behörde hatte die Betroffene einen Antrag auf Auskunft gestellt. Daraufhin wurde ihr eine Kopie der bei uns geführten Akte zur Verfügung gestellt. Wir sind dabei einer gesetzlichen Verpflichtung nachgekommen. Diese Transparenz ging der Verantwortlichen aber zu weit. Sie ließ deshalb durch ihren Prozessbevollmächtigten im Verfahren vor dem IDSG vortragen, der Diözesandatenschutzbeauftragte habe sehenden Auges gegen geltendes Strafrecht und gegen die freiheitlich demokratische Grundordnung verstoßen. Wegen dieser Behauptung ist Strafanzeige gegen den Prozessbevollmächtigten erstattet worden. Weiterhin ist ein Verfahren vor der zuständigen Rechtsanwaltskammer beantragt worden.

Neben dem eigentlichen Datenschutzverstoß betrachten wir das Verhalten der Verantwortlichen als einen massiven Verstoß gegen die Grundsätze und

26 IDSG, Beschluss vom 27. September 2021 - IDSG 08/2021

das Leitbild der Verantwortlichen. Darüber hinaus wird der Versuch durch verleumderische Behauptungen auf die Datenschutzaufsicht Einfluss zu nehmen von uns als ein Angriff auf die Unabhängigkeit unserer Behörde betrachtet.

4.3.2 Falsch versandte Patientenunterlagen – ein Dauerbrenner

Alles geregelt und trotzdem - Tücken im Arbeitsalltag

Wie jedes Jahr wieder wurden uns auch in diesem Berichtszeitraum mehrere Fälle gemeldet, in denen Entlassberichte, Arztbriefe, Rechnungen falsch versandt worden sind. Die Offenlegung erfolgte auch in diesen Fällen durch Übersendung an falsche Empfänger oder durch das Verbinden von nicht zusammengehörigen Unterlagen und damit Herausgabe von Daten an unberechtigte Empfänger. In einem Fall befanden sich Unterlagen eines Patienten in der Patienten Akte einer anderen Patientin. Festgestellt wurde dies von der Patientin selbst, als sie Einsicht in ihre Patientenakte genommen hatte.

Unsere Ermittlungen haben ergeben, dass in den meisten Fällen in den Einrichtungen entsprechende Datenschutzunterlagen vorhanden und die Verantwortlichen ihren Verpflichtungen gem. § 26 KDG nachgekommen waren. Die Verantwortlichen haben zugesagt, ihre Mitarbeiter nochmals auf die Einhaltung der vorhandenen Regelungen zur Herausgabe und Übersendung von Unterlagen, die Gesundheitsdaten enthalten zu schulen und entsprechend zu sensibilisieren.

In 3 Fällen wurden förmliche Beanstandungen ausgesprochen. Die Bescheide sind rechtskräftig.

Wenn konkrete Regelungen fehlen

In einem Fall waren die vorhandenen Regelungen nicht ausreichend. In diesem Fall wurden Unterlagen nicht an andere Patienten versandt oder herausgegeben, sondern ein Entlassungsbericht wurde an eine nicht mit der Behandlung betraute Ärztin versandt. Die Datenschutzverletzung wurde durch die Patientin festgestellt, nach dem diese selbst Einblick in ihre

Patientenakte genommen hatte. Der Entlassungsbericht enthielt Informationen über einen stationären Aufenthalt samt Gesundheitsdaten. Aus dem Bericht waren der Namen, das Geburtsdatum sowie die Adresse der Patientin erkennbar. Die Patientin hat die Klinik über den Vorfall informiert. Diese hat umgehend die Ärztin, an die der Entlassungsbericht fälschlicherweise versandt worden ist, kontaktiert und um Vernichtung gebeten. Die Klinikleitung hat angegeben, eine Prüfung des Vorfalles habe ergeben, dass bereits bei der Anlage der Patientenakte, die zuständige Ärztin im Krankenhausinformationssystem (KIS) fehlerhaft hinterlegt worden ist. Aufgrund des Zeitablaufs konnte eine Klärung, wer für die fehlerhafte Erfassung verantwortlich war, nicht mehr erfolgen. Die Verantwortlichen zeigten sich kooperativ und waren einsichtig. Vereinbart wurde, den Vorfall zum Anlass zu nehmen, den Entlassungsprozess zu optimieren. Es soll eine Regelung aufgenommen werden, die u. a. auch vorsieht, dass bei der Entlassung nochmals abgefragt wird, wer der weiterbehandelnde Arzt bzw. der Hausarzt ist, damit ein derartiger Falschversand künftig vermieden wird. Unbeschadet dessen haben wir uns mit dem Verantwortlichen aufgrund der fehlenden Regelungen auf die Zahlung einer Geldbuße verständigt. Das Entlassungsmanagement wurde entsprechend überarbeitet und uns vorgelegt.

4.3.3 SOS aus der Notaufnahme – E-Mail mit Patientendaten an alle Mitarbeiter

In einem anderen Fall hatte ein Arzt der Notaufnahme in einer krankenhausinternen E-Mail (Rundmail) die Namen, die Geburtsdaten und das Geschlecht von 17 Patienten offengelegt, in dem er einen Screenshot der Warteliste (Bildschirm) angefertigt und verbreitet hatte. Preisgegeben wurden zudem die Gesundheitsdaten der Patienten, wie z. B. Verdachtsdiagnosen und anstehender Maßnahmen. Angegeben wurde, dass der Arzt angeführt hatte, damit auf die bestehende Belastungssituation der Mitarbeiter der Notaufnahme aufmerksam machen zu wollen. Der Verursacher war sich zum Zeitpunkt des Verfassens der E-Mail der Datenschutzproblematik nicht bewusst. Die E-Mail wurde an ca. 1.200 Mitarbeiter versandt. Der vom Arzt genutzte Verteiler enthielt neben den persönlichen E-Mail-Adressen sämtlicher Mitarbeiter auch Gruppen- und Abteilungsadressen.

Der Datenschutzvorfall wurde uns von der Klinikleitung umgehend gemeldet. Mitgeteilt worden ist in der Meldung, dass der Datenschutzvorfall mit dem verursachenden Arzt ausgewertet worden ist. Angezeigt worden ist zudem, dass der Vorfall zum Anlass genommen wird, die Belastungssituation des Personals zu analysieren. Die betroffenen Patienten waren zum Zeitpunkt der Meldung an uns bereits über den Datenschutzverstoß informiert worden. Auch die Empfänger der E-Mail hatten bereits eine E-Mail mit der Aufforderung erhalten, die „besagte" Mail auf keinen Fall weiterzuleiten, sondern umgehend zu löschen. Im Nachgang hat die Verantwortliche stichprobenartig kontrolliert, ob die Löschungsaufforderung umgesetzt worden ist. Nachdem festgestellt worden war, dass dieser nur in geringem Maße nachgekommen worden bzw. die E-Mail noch in den „gelöschten Elementen" verblieben war, wurde seitens der Klinikleitung entschieden, die betroffene E-Mail per Script vom Server zu löschen. Die Klinik hat in ihrer Stellungnahme Erfolg vermeldet: alle 1247 E-Mails sind gelöscht (auch auf dem Server). Eine nächste standartmäßige Synchronisierung der Mailclients entfernte die Mails auch von den Endgeräten. Auch dies wurde exemplarisch geprüft.

Auch in den Regularien der Klinik zum Umgang mit E-Mails sind Regelungen für Mitarbeiter vorgegeben. In der Datenschutzrichtlinie für den ärztlichen Dienst ist u.a. festgelegt, dass Gesundheitsdaten nicht über Standartmails unverschlüsselt übertragen werden dürfen.

Aufgrund der Tatsache, dass Gesundheitsdaten von Patienten einer Vielzahl von unberechtigten Empfängern bekanntgegeben worden sind, wurde der Klinik unter Anwendung des Funktionsträgerprinzip eine förmliche Beanstandung ausgesprochen. Versäumnisse der Klinikleitung konnten nicht festgestellt werden. Der Beanstandungsbescheid ist rechtskräftig.

4.3.4 Neugierige Kollegen und der Datenschutz

Unserer Aufsicht wurde durch eine Mitarbeiterin eines Krankenhauses ein sie selbst betreffender Datenschutzverstoß gemeldet.

Die Petentin teilte mit, sie sei selbst Mitarbeiterin des Krankenhauses, in dem sie als Patientin behandelt worden ist. Nach längerer krankheitsbe-

dingter Abwesenheit kehrte sie zum Dienst auf ihre Station zurück. Dabei musste sie feststellen, dass zahlreiche Kolleginnen Kenntnis über ihre Behandlung hatten. Durch Einsicht in die Patientenakte war den Mitarbeitern u. a. ein Histologiebefund und ein OP-Bericht bekannt geworden. Sie gab an, dass 5 Mitarbeiter der Station, auf der sie tätig war, Einsicht in ihre Patientenakte genommen hatten.

Die Petentin hatte die stellvertretenden Pflegedienstleiterin und die Stationsleiterin über diesen Vorfall informiert. Da beide Mitarbeiterinnen Führungsverantwortung haben, hätten sie erkennen müssen, dass es sich bei der Mitteilung der Petentin, um die Anzeige eines Datenschutzverstoßes handelt. Beide Mitarbeiterinnen haben jedoch keine Konsequenzen aus dieser Mitteilung gezogen und auch keinerlei Handlungen eingeleitet, um diesen Vorgang zu verfolgen. Die stellvertretende Pflegedienstleiterin wurde darüber hinaus von der Petentin mit der Aussage zitiert. *„ … dass es doch ganz normal wäre, dass man mal reinschaut …“*. Die Petentin hatte auch die Mitarbeitervertretung über den Vorgang in Kenntnis gesetzt.

Der Vorfall stellt eine meldepflichtige Verletzung gegen Regelungen des KDG dar, weil mit dieser Verletzung eine Gefahr für die Rechte und Freiheiten der Betroffenen verbunden ist. Die Grundsätze für die Verarbeitung personenbezogener Daten wurden nicht eingehalten. Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht vereinbarenden Weise verarbeitet werden. Patientenakten enthalten generell personenbezogenen Daten sowie personenbezogenen Daten besonderer Kategorie. Das Einsehen in eine Patientenakte stellt eine Verarbeitung im Sinne des § 4 Abs. 3 KDG durch Auslesen dar.

Auch innerhalb eines Krankenhauses dürfen nur die Personen auf die Krankendaten Zugriff haben, die diese Daten zur Diagnose, Therapie und Pflege des Patienten benötigen – need to know-Prinzip. Die einsehenden Mitarbeiter waren nicht berechtigt, in die Patientenakte der Petentin Einsicht zunehmen.

Die Krankenhausleitung hat im Rahmen eines Vortortermins den Verstoß zugestanden und mitgeteilt, dass mit den Betroffenen Mitarbeiter/innen

Gespräche geführt und disziplinarische Schritte eingeleitet worden sind. Auch in diesem Verfahren konnten wir uns mit der Verantwortlichen auf die Zahlung einer Geldbuße einigen.

4.3.5 Screenshot einer Pflegeakte als Statusmeldung

In großer Vorfreude auf den bevorstehenden Urlaub hat eine Mitarbeiterin eines Pflegeheims an ihrem letzten Arbeitstag ein Screenshot vom Arbeitsplatzmonitor gemacht und diesen anschließend als Statusmeldung in ihrem Messenger eingestellt.

Da zu diesem Zeitpunkt die Software des Pflegeverwaltungsprogramms geöffnet war, enthielt der Screenshot den Vor- und Zunamen, das Geburtsdatum sowie anstehende Behandlungen eines Bewohners, demzufolge personenbezogene Daten sowie personenbezogene Daten besonderer Kategorie.

Der Vorfall wurde durch einen anderen Mitarbeitenden bemerkt, da dieser die eingestellte Statusmeldung über den Messangerdienst gesehen hatte.

Das Erstellen des Screenshots sowie das Einstellen in den Status stellen jeweils Verarbeitungen personenbezogene Daten sowie personenbezogene Daten besonderer Kategorie 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 besonderer Kategorie unzulässig. Eine Ausnahme besteht nur für den Fall, dass eine der in Abs. 2 dieser Vorschrift genannten Bedingungen zutrifft. Das Vorliegen der Voraussetzungen einer Ausnahmevorschrift war nicht ersichtlich. Die Verarbeitung war mithin unzulässig und wurde durch unsere Dienststelle beanstandet.

Der Verantwortliche hat gegenüber der Mitarbeiterin arbeitsrechtliche Maßnahmen eingeleitet und diesen Vorfall für weitere Sensibilisierungen im Rahmen von Schulungen zum Anlass genommen.

4.3.6 Fotos und Videoaufnahmen von Bewohnern

Unserer Dienstelle wurde gemeldet, dass eine Auszubildende, die sowohl in einer Pflegeeinrichtung und auch in einem Krankenhaus eingesetzt war, Fotos und Videoaufnahmen von Patienten bzw. Bewohner erstellt und diese über Messengerdienste veröffentlicht hat. In der Einrichtung bestand ein Verbot private Endgeräte dienstlich zu nutzen sowie ein Verbot der privaten Nutzung von dienstlichen Geräten. Der Verantwortliche hat den Vorfall zum Anlass genommen, die Mitarbeiter nochmals auf die Einhaltung des Datenschutzes zu sensibilisieren. Zudem wurden die Mitarbeiter auf das Verbot private Mobiltelefone/Smartphone während der Arbeitszeit mit sich zuführen nochmals ausdrücklich hingewiesen. Die Einrichtungsleitung wurde um Stellungnahme gebeten, dass Verfahren ist noch nicht abgeschlossen.

5 Datenschutz in Kita und Schule

5.1 Bundesverfassungsgericht bestätigt Masern-Impfpflicht

Nachweis der Masernimpfung ist seit dem 31. Juli 2022 verpflichtend

Die Corona-Impfpflicht im Gesundheitsbereich hat in den vergangenen 2 Jahren für erhebliche Aufregung und Diskussionen gesorgt. Unbeachtet geblieben ist dagegen die Masern-Impfpflicht in Gemeinschaftseinrichtungen.

Betroffener Personenkreis (§ 20 Abs. 9 IfSG):

Eine Masernimpfung muss von allen Personen nachgewiesen werden, die in

- Kita, Kinderhort, Kindertagespflege oder in einer Schule betreut werden (es besteht faktisch eine Impfpflicht für alle Kinder), aber auch von allen Personen, die in diesen Einrichtungen tätig sind,
- den in § 23 Abs. 3 IfSG genannten Gesundheitseinrichtungen tätig sind, dazu zählen etwa Krankenhäuser, Arztpraxen, ambulanter Pflegedienst sowie auch der Rettungsdienst,

- Einrichtungen tätig sind, in denen Asylbewerber, Geflüchtete und Ausreisepflichtige untergebracht sind (§ 36 Absatz 1 Nr. 4. IfSG).

Den Nachweis müssen Personen erbringen, die nach dem 31.12.1970 geboren wurden und mindestens ein Jahr alt sind. Vorzulegen ist

- ein Nachweis der Impfung (bei Kindern ab einem Jahr eine Schutzimpfung, bei Kindern ab zwei Jahren und Erwachsenen zwei Masern-Schutzimpfungen),
- ein ärztliches Zeugnis über eine Masern-Immunität, diese kann mithilfe einer Blutuntersuchung festgestellt werden, oder
- ein ärztliches Attest, dass aufgrund einer medizinischen Kontraindikation nicht geimpft werden kann.

Der Nachweis kann aber auch durch Vorlage einer Bestätigung einer staatlichen Stelle oder anderen Einrichtung, dass dort bereits ein Nachweis vorgelegt wurde, erbracht werden (§ 20 Abs. 9 Nr. 3 IfSG).

Die bisherige Schonfrist ist abgelaufen. Die Nachweise müssen seit dem 31. Juli 2022 vorgelegt werden.

Umgang mit den Nachweisen?
Aus der Debatte um die Corona-Impflicht im Gesundheitswesen dürfte allgemein bekannt sein, dass es sich bei Informationen zum Impfstatus um hochsensible Gesundheitsdaten handelt und deshalb im Umgang mit den Nachweisen eine besondere Sorgfalt geboten ist.

Auch bei den Masern-Impfnachweisen gilt:
Die Nachweise dürfen lediglich eingesehen werden. Das Anfertigen von Kopien ist nicht erlaubt. Es sollte lediglich dokumentiert werden, dass ein entsprechender Nachweis vorgelegen hat und eingesehen wurde. Diese Dokumentation darf für die gesamte Dauer der Tätigkeit bzw. Betreuung in der Einrichtung aufbewahrt werden. Die zum Nachweis notwendigen Daten werden nur so lange gespeichert, wie dies unter Beachtung gesetzlicher Aufbewahrungsfristen zur Aufgabenerfüllung erforderlich ist.

Was ist zu beachten, wenn kein Nachweis vorgelegt wird?
Personen, die neu in die Einrichtung kommen und keinen Nachweis vorlegen, dürfen nicht betreut bzw. nicht in der Einrichtung beschäftigt werden.

Das hat aber nicht zur Folge, dass schulpflichtigen Kindern der Schulbesuch wegen einer fehlenden Impfung verweigert werden darf. Sofern für ein ungeimpfte Kind kein ärztliches Zeugnis bzw. Attest vorgelegt wird, welches bestätigt, dass das Kind eine Immunität gegen Masern besitzt bzw. nicht geimpft werden kann, muss das zuständige Gesundheitsamt informiert werden (§ 20 Abs. 9 S. 2 IfSG). Das Gesundheitsamt ist dann für die Einleitung weiterer Schritte verantwortlich.

Dies gilt auch, wenn Zweifel an der Echtheit eines Nachweises bestehen. Die erforderlichen Daten dürfen in diesen Fällen an das Gesundheitsamt übermittelt werden. Das Gesetz bestimmt nicht, welche Daten dies konkret sind. Ratsam ist es die Vorschrift sehr restriktiv auszulegen und zunächst nur den Namen und die Anschrift der betroffenen Person zu übermitteln.

Soweit für die Datenübermittlung an das Gesundheitsamt keine technische Lösung für eine gesicherte Datenübertragung zur Verfügung steht, die die technischen und organisatorischen Maßnahmen zum Schutz von Gesundheitsdaten gewährleistet, sollte die Datenübermittlung auf dem Postweg per Brief erfolgen. Es wird jedoch empfohlen, sich mit dem zuständigen Gesundheitsamt diesbezüglich vorab abzustimmen.

Das Bundesverfassungsgericht[27] wies mehrere Klagen betroffener Familien zurück, die gegen die Masern-Impflicht sowie daraus resultierenden Folgen bei Nichterbringung der entsprechenden Nachweise Verfassungsbeschwerde eingereicht hatten.

Die Grundrechtseingriffe seien nicht unerheblich, aber zumutbar, um besonders gefährdete Menschen vor einer Infektion zu schützen, so die Verfassungsrichter. Die Impfpflicht bleibt damit in Kraft.

5.2 Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten in Kitas

Kirchliche Stellen im Sinne des § 3 Abs. 1 KDG müssen nach § 36 Abs. 2 KDG einen betrieblichen Datenschutzbeauftragten benennen, wenn eine der dort vorliegenden Bedingungen erfüllt ist.

27 BVG, 21.07.2022 - 1 BvR 469/20, 1 BvR 472/20, 1 BvR 471/20, 1 BvR 470/20

Katholische Kindertagesstätten, die zum Deutschen Caritasverband, zum Diözesan-Caritasverband oder zu einem Unterverband gehören, fallen gemäß § 3 Abs. 1 lit. b KDG unter die Regelungen des Kirchlichen Datenschutzrechts. Kindertagesstätten, die in Trägerschaft einer Kirchengemeinde sind, von einem kirchlichen (katholischen) Trägerverein oder einem anderen katholischen Werk (z.B. Kolpingwerk, Bonifatiuswerk) betrieben werden, sind entsprechend § 3 Abs. 1 lit. c KDG kirchliche Einrichtungen, für die dieses Gesetz maßgebend ist.

Welche Benennungsvoraussetzungen gemäß § 36 Abs. 2 KDG werden erfüllt?

Kleinere Kindertagesstätten könnten darauf abheben, dass die Voraussetzung § 36 Abs. 2 lit. a KDG nicht erfüllt sein dürfte, da dort weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.

Da jedoch unabhängig von der Anzahl der Personen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, sensible, gesundheitliche, entwicklungsbezogene, sozialpädagogische Daten, dementsprechend besondere Kategorien personenbezogener Daten verarbeitet werden[28], greift in jeder Kindertagesstätte, unabhängig von deren Größe oder Mitarbeiterzahl, die Benennungsvoraussetzung des § 36 Abs. 2 lit. c. KDG.

Insbesondere bei der Erstellung und Bearbeitung der Portfolios sowie des Führens der Entwicklungsdokumentation, die durch entsprechende Bildungsprogramme oder gesetzlichen Regelungen für Kindertageseinrichtungen verpflichtend ist, werden personenbezogene Daten i. S. v. § 4 Nr. 1 KDG und personenbezogene Daten besonderer Kategorie i. S. v. § 4 Nr. 2 und Nr. 17 KDG der Kinder durch die pädagogische Fachkraft verarbeitet.

Die pädagogischen Mitarbeitenden sind auch verpflichtet, Entwicklungsgespräche mit den Sorgeberechtigten zu führen. In Entwicklungsgesprächen werden u.U. auch personenbezogene Daten besonderer Kategorien (z.B. Gesundheitsdaten) verarbeitet. Üblicherweise kommt es in Kindertagesstätten auch zu Krankmeldungen von Kindern, die je nach Erkrankung eine Meldepflicht nach IfSG an das Gesundheitsamt auslösen können.

28 Schulten, in: Sydow, Kirchliches Datenschutzrecht Handkommentar, 1. Auflage 2021, § 36 KDG, Rn. 47

Auch muss bei Aufnahme des Kindes gem. § 20 Abs. 9 IfSG dokumentiert werden, ob eine ausreichende Immunität gegen Masern vorliegt. Ebenfalls muss eine ärztliche Bescheinigung über die gesundheitliche Eignung eines Kindes bei Aufnahme in die Kindertagesstätte vorgelegt werden.

Zudem können Einrichtungen – je nach Bundesland – auch angehalten sein, für eine begleitende ärztliche und zahnärztliche Untersuchung der Kinder zu sorgen. Beispielsweise werden in vielen Kindertagesstätten Reihen-Zahnuntersuchungen durchgeführt.

Ferner können die Einrichtungen auch verpflichtet sein, sich mit den Frühförderstellen in Verbindung zu setzen, um die erforderlichen therapeutischen Angebote für Kinder mit Behinderungen oder Beeinträchtigungen sicherzustellen.

Ein weiterer Aspekt für die Erfüllung der Voraussetzungen zur Benennung eines betrieblichen Datenschutzbeauftragten ist, dass die Kerntätigkeit des Verantwortlichen, also der Kindertagesstätte, in der systematischen Beobachtung und Dokumentation der kindlichen Entwicklung besteht und somit Bestandteil der Arbeit der pädagogischen Fachkräfte ist. Dieses systematische Beobachten und Dokumentieren stellen aufgrund ihres Umfangs eine umfangreiche und ständige Überwachung von betroffenen Personen (Kindern) dar, die die Benennung eines betrieblichen Datenschutzbeauftragten erforderlich machen[29]. Somit ist auch § 36 Abs. 2 lit. b KDG erfüllt.

Auch wenn eine Kindertagesstätte von einer Katholischen Pfarrei getragen wird, sehen wir die Verantwortlichkeit zur Bestellung eines Datenschutzbeauftragten bei der Leitung, da diese in der Regel über Zweck und Mittel der Datenverarbeitung entscheidet.

5.3 Datenschutzvorfälle

5.3.1 Offenlegung von Daten – ein altbekanntes Thema

Unter den Datenschutzvorfällen im Schulbereich waren im Berichtsjahr 2022 mehrfach Vorkommnisse, bei denen personenbezogene Daten sowie

29 37. TB, 2017/2018, Abschnitt 5.4.3, Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein

personenbezogene Daten besonderer Kategorie unbeabsichtigt offengelegt wurden, obwohl allen Beteiligten bekannt war, welche Grundsätze sie beim Verarbeiten personenbezogener Daten zu beachten haben. Entsprechende Verpflichtungserklärungen wurden uns auf Verlangen vorgelegt und im Weiteren konnte uns glaubhaft dargelegt werden, dass regelmäßig Unterweisungen zum Datenschutz stattfinden. Auch die entsprechenden Verträge, Vereinbarungen oder Anweisungen lagen ausnahmslos vor.

Woran hat es dann gelegen?

Diese Vorfälle gehen allesamt auf Bedienfehler, Fehleinschätzungen, Unachtsamkeit oder schlichtweg menschliches Versehen zurück. Eine zunehmend unterschätze Gefahr, auch für den Datenschutz.

5.3.2 Sicherheitsrisiko Lernplattform - Namen der Schüler anstatt des Protokolls

Unserer Dienststelle wurde eine Beschwerde eines Elternteils eingereicht, in der angenommen wurde, dass eine Lernplattform Sicherheitslücken und unzureichend geschützte Schnittstellen hätte. Grund für diese Mutmaßung war, dass anstatt eines Protokolls eines Elternabends, welches von der Lehrerin über die Elternvertretung an die Elternschaft einer Klasse weitergeleitet werden sollte, aus Versehen gekürzte Ausschnitte aus dem Mailverkehr der Kinder mit der Lehrerin verschickt worden sind. Aus dem Mailverkehr gingen die Namen der Kinder als personenbezogene Daten hervor. Der Lehrerin ist dieses Versehen sofort aufgefallen. Sie hat umgehend die Elternvertretung kontaktiert und darum gebeten, die Mail zu löschen sowie den richtigen Anhang weiterzuleiten.

Da die Elternschaft umgehend aufgefordert wurde die Mail zu löschen, sahen wir die Rechte und Freiheiten der betroffenen Schüler nicht als gefährdet an. Eine Lernplattform dient zur Kommunikation der Lehrenden mit den Schülern. Daher ist es unabdingbar, dass die Schüler personalisierte E-Mailadressen nutzen. Die Lernplattform basiert auf einem schlüssigen Rollen- und Rechte Konzept. Eine Sicherheitslücke oder unzureichend geschützte Schnittstellen ließen dieser Vorfall nicht vermuten. Trotz aller technischen und organisatorischen Maßnahmen sind jedoch menschliche Fehler nicht ausgeschlossen.

Weiterhin begehrte der Beschwerdeführer für die Zukunft eine Einverständniserklärung der Sorgeberechtigten zur Nutzung der Lernplattform durch die Schüler, da ja personenbezogene Daten verarbeitet werden. Eine Prüfung durch unsere Dienststelle ergab, dass eine Einverständniserklärung zur Nutzung der Lernplattform nicht erforderlich ist, da diese aufgrund der Regelung im Schulgesetz Teil der pädagogischen Arbeit ist. Somit ist die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß § 6 Abs. 1 lit. a KDG erfüllt und eine Einverständniserklärung nicht erforderlich.

Für die Nutzung von Videokonferenzsystemen regten wir die Einholung einer Einwilligungserklärung / Einverständniserklärung aufgrund der Übertragung von Bild und Ton sowie der damit verbundenen Einblicke in das private Wohnumfeld an (siehe Tätigkeitsbericht 2020 KDSA Ost, S. 61 ff).

5.3.3 Schulhilfekonferenz im Klassenverteiler

In einem weiteren Fall tauschte die Schulleitung mit einem Lehrenden Informationen über eine geplante Schulhilfekonferenz per E-Mail aus. Dabei wurde jedoch anstatt der persönlichen E-Mailadresse des Lehrenden versehentlich der E-Mail Verteiler der gesamten Klasse genutzt. Die Information, dass für ein Kind eine Schulhilfekonferenz einberufen wird, ist sensibel und schützenswert, da diese für gewöhnlich in besonders schwierigen und konfliktreichen Situationen erfolgt.

Da dieses Versehen dennoch zeitnah aufgefallen ist, wurde umgehend die E-Mailfunktion der Klasse deaktiviert. Damit sollte ausgeschlossen werden, dass diese Information von allen Kindern bzw. deren Eltern gelesen und somit offengelegt wird. Im Folgenden wurden von dem Dienstleister die alten Zugangsdaten der E-Mailaccounts gelöscht und neue Zugangsdaten an die Eltern ausgegeben. Jedoch war die Löschung der alten E-Mailaccounts unvollständig und in Folge dessen war es möglich sich mit den alten Zugangsdaten weiterhin einzuloggen. Erst als dieses aufgefallen ist, wurde eine endgültige Löschung der alten E-Mailaccounts in die Wege geleitet.

Unsere Dienststelle hat die Schule sowie den Schulträger dahingehend sensibilisiert, sich für derartige Aufträge als Verantwortliche und Auftrag-

geber in Zukunft ein entsprechendes Protokoll für Arbeiten an der beauftragten Datenverarbeitung aushändigen lassen. Nur damit kommt die Verantwortliche ihrer Rechenschaftspflicht nach und kann die beauftragten Arbeiten überprüfen oder reklamieren.

Im Weiteren wurden selbstverständlich auch die Schulleitung und die Lehrenden sensibilisiert, sorgsam und achtsam mit E-Mailadressen und Verteilern umzugehen sowie ganz genau zu prüfen, an wen eine E-Mail gesendet und wem geantwortet wird.

Fazit: Sorglose E-Mailweiterleitungen und Beantwortungen bergen Gefahren! Für neue „Anlässe" sind stets neue E-Mails zu erstellen. Vorsicht ist ebenfalls beim automatischen einfügen der Kontakte geboten. Ähnlich lautende E-Mailadressen können so ungewollt in den E-Mail Verteiler aufgenommen werden.

5.3.4 Jahrbücher

Ein ehemaliger Schüler hat sich bereits vor längerer Zeit darüber beschwert, dass ein Jahrbuch auf der Webseite der Schule offen einsehbar ist. Dieses Jahrbuch konnte heruntergeladen und weiterverbreitet werden. Weder die Gesichter noch die Namen waren unkenntlich gemacht. Eine Einwilligungserklärung des ehemaligen Schülers lag dafür nicht vor.

In Folge dieser Beschwerde wurde das Jahrbuch von der Webseite entfernt. Alles war gut, oder doch nicht?
Nach einiger Zeit tauchte das Jahrbuch erneut auf der Webseite der Schule auf. Der Name und das Foto des Petenten waren ersichtlich. Was war passiert?

Ein aktives Hochladen durch die Schule hat nicht stattgefunden. Vermutet wird daher, dass nach einem technischen Fehler auf der Webseite und dem Versuch diese wiederherzustellen, die Datei (Jahrbuch) erneut mit hochgeladen wurde.
Auch hier hat unsere Dienststelle dahingehend sensibilisiert Aufträge oder Wartungsarbeiten an der Datenverarbeitung zu protokollieren, um der Rechenschaftspflicht nachzukommen, die beauftragten Arbeiten überprüfen und Änderungen nachvollziehen zu können.

Im Weiteren haben wir angeregt, grundsätzlich zu überdenken, ob Jahrbücher mit Fotos und weiteren personenbezogenen Daten online veröffentlicht werden sollten. Medien (Fotos, Videos, Informationen) können im Internet beliebig vervielfältigt, geteilt und weitergegeben werden. Der Ersteller dieser Medien (Verantwortlicher) ist nur schwer in der Lage dies rückgängig zu machen und eine Verbreitung zu stoppen.
Zudem ist unabhängig davon, ob Betroffene Einwilligungserklärungen zur Veröffentlichung von Medien erteilen oder nicht, ein datenschutzkonformes Handeln in einem derartigen Fall immer schwer und zeitaufwendig, da sich an Schulen eine Menge Einwilligungserklärungen ansammeln können, die im Fall einer Veröffentlichung überprüft werden müssen.

5.3.5 Aus gesundheitlichen Gründen nicht im Dienst

In einer Bildungsstätte wurde den Eltern eines dort betreuten Kindes per E-Mail mitgeteilt, dass ein Pädagoge aus gesundheitlichen Gründen bereits mehrere Wochen nicht im Dienst ist und es daher zur Verzögerung bei der Beantwortung ihrer Anfrage gekommen ist.

Die Mitteilung über den Gesundheitszustand enthält ein personenbezogenes Datum besonderer Kategorie (§ 4 Nr. 2 KDG). Das Mitteilen dieser Information per E-Mail an die Eltern stellt eine Verarbeitung im Sinne des § 4 Nr. 3 KDG durch Offenlegen dar.

Auch wenn den Eltern des betreuten Kindes möglicherweise bekannt gewesen ist, dass der betroffene Pädagoge seit längerem erkrankt ist, rechtfertigt dies nicht die vorgenommene Offenlegung der Gesundheitsdaten. Da es sich dabei um personenbezogene Daten besonderer Kategorie handelt, ist eine Verarbeitung generell unzulässig.

Das Erwähnen der Abwesenheit dieses Kollegen oder der Hinweis auf einen bestehenden Personalmangel hätte genügt, um die Verzögerung zu begründen.

In diesem Fall wurde durch die Datenschutzaufsicht eine förmliche Beanstandung gegenüber dem Verantwortlichen ausgesprochen, um diesen zur Einhaltung des KDG anzuhalten.

Fazit: Zu beobachten ist, dass krankheitsbedingte Abwesenheit häufig angegeben wird, wenn es zu Verzögerungen oder Versäumnissen kommt. Doch Vorsicht, sobald sich Rückschlüsse auf Personen ziehen lassen, handelt es sich unbefugte Offenlegung personenbezogener Daten besonderer Kategorie, die die Verletzung von Rechten und Freiheiten der betroffenen Personen zur Folge haben können.

6 Datenschutz im Beschäftigungsverhältnis

6.1 Schutzkonzept und erweitertes Führungszeugnis

Wann darf der Arbeitgeber die Vorlage eines erweiterten Führungszeugnisses gem. §§ 30 a, 32 V Bundeszentralregistergesetz (BZRG) verlangen? Diese Frage wurde in der letzten Zeit häufiger an unsere Dienststelle herangetragen. Ursächlich dafür ist das Bestreben einiger (katholischer) Einrichtungen von allen Mitarbeitenden unabhängig von deren Einsatz das erweiterte Führungszeugnis abzufordern, um den Schutz vor sexualisierter Gewalt gerecht zu werden. Mitarbeitende, die in der Arbeit mit Kindern, Jugendlichen sowie schutz- und hilfebedürftigen Erwachsenen eingesetzt werden, sind dazu gesetzlich verpflichtet.

In unserem letzten Tätigkeitsbericht 2021 haben wir unter Punkt 2.3 ausführlich dargelegt, in welchen Fällen die Vorlage verlangt werden darf.

Die Absicht, dass die Pflicht zur Vorlage eines erweiterten Führungszeugnisses auch technische Mitarbeitende und Verwaltungsmitarbeiter betreffen soll, wenn diese aufgrund örtlicher Gegebenheiten Einzelkontakt zu Schutzbefohlenen haben können oder im Laufe ihrer Tätigkeit schutzwürdigen Personen begegnen können (vorsorgliche Vorlage), geht aus einigen institutionellen Schutzkonzepten und/oder Präventionsordnungen der Einrichtungen hervor.

Demnach wären dann auch Mitarbeitende der Buchhaltung oder IT-Abteilung zur Vorlage verpflichtet sowie auch der Hausmeister eines Ordinariates. Auch die in einer Schuldnerberatung tätigen Beschäftigten, könnten

daher zur Vorlage verpflichtet werden, da Klienten gelegentlich ihre Kinder zur Beratung mitbringen, diese jedoch selbst beaufsichtigen.

Die bloße Möglichkeit, die Technische- oder Verwaltungsmitarbeitende haben, mit den Kindern Kontakt aufzunehmen reicht jedoch nicht aus, diese zur Vorlage eines erweiterten Führungszeugnisses zu verpflichten. Werden erweiterte Führungszeugnisse von allen Mitarbeitenden abverlangt, besteht die Gefahr, dass der Arbeitgeber aufgrund der Sonderregelungen der §§ 30a BZRG, 72a SGB VIII Informationen über den Mitarbeitenden erhält, die über den Schutzzweck dieser Vorschrift hinausgehen. Durch diese Vorschrift darf jedoch nicht - über das durch den Gesetzeszweck bedingte Maß hinaus - in das Persönlichkeitsrecht des Mitarbeiters eingegriffen werden.

Unsere Aufsicht ist der Ansicht, dass nur für Personal, welches regelmäßig die Beaufsichtigung, Betreuung etc. von Schutzbefohlenen im Sinne der entsprechenden Regelungen des SGB und den weiteren Gesetzen durchführt, eine gesetzliche Grundlage zur Vorlage eines erweiterten Führungszeugnisses vorliegt.

6.2 Anwendbarkeit des KDG im Beschäftigungskontext

Entscheidung des Interdiözesanen Datenschutzgerichtes (IDSG) 19/2021 vom 25.04.2022.

Ein Betroffener zeigte der kirchlichen Datenschutzaufsicht eine Datenschutzverletzung an. Dabei wurde folgendes dargestellt: Der Betroffene schloss nach Beendigung seines Ausbildungsverhältnisses bei einem Bistum einen Arbeitsvertrag mit einer katholischen gGmbH. Er behauptet, der Geschäftsführer dieser gGmbH habe ihm in einem Gespräch mitgeteilt, ein Abteilungsleiter des Bistums habe ihm, dem Geschäftsführer, telefonisch geraten, er solle darauf achten, wen er sich ins Haus hole, denn der Betroffene habe dem Abteilungsleiter mit seinem Anwalt gedroht.

Die Datenschutzaufsicht sah darin eine Datenschutzverletzung in Form einer unzulässigen Weitergabe von personenbezogenen Daten, sofern man

den Vortrag des Betroffenen als zutreffend unterstelle. Die Aufsicht lehnte eine Sanktionierung des Verantwortlichen jedoch ab, weil die Darstellungen des Betroffenen nicht unumstößlich beweisbar seien.

Dagegen wendete sich der Betroffene mit einer Klage an das IDSG.

In seiner o. g. Entscheidung sieht das IDSG eine Anwendbarkeit des KDG nicht gegeben, da es im geschilderten Fall ausschließlich um eine Gesprächssituation gegangen sei. Der sachliche Anwendungsbereich wäre gem. § 2 Abs. 1 KDG nur eröffnet, wenn die personenbezogenen Daten in einem Dateisystem im Sinne von § 4 Ziffer 8 KDG gespeichert sind oder gespeichert werden sollen. Das Gericht sieht nur dann eine Ausnahme gegeben, wenn von dem Gespräch eine Niederschrift gefertigt worden wäre oder zumindest beabsichtigt gewesen sei, eine solche zu fertigen.

Vorliegend handelt es sich um eine Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis. Der Betroffene als Person, deren Beschäftigungsverhältnis beendet ist, gilt gem. § 4 Nr. 24 lit. i) KDG weiterhin als Beschäftigter i. S. d. KDG. § 53 Abs. 3 KDG legt ausschließlich für den Bereich des Beschäftigtendatenschutzes fest, dass diese Norm bei jeglicher Verarbeitung personenbezogener Daten anzuwenden ist, unabhängig davon wie diese Daten verarbeitet worden sind. Damit unterfallen dem Anwendungsbereich des Beschäftigtendatenschutzes nahezu alle Verarbeitungen, die mit Informationen über den Beschäftigten zusammenhängen. Durch § 53 Abs. 3 KDG wird der sachliche Anwendungsbereich nach § 2 Abs. 1 KDG für den Bereich eines Beschäftigungsverhältnisses erweitert und ist auch dann eröffnet, wenn die Verarbeitung der personenbezogenen Daten nicht in einem Dateisystem gespeichert sind oder werden sollen. Das KDG gilt deshalb auch bei Befragungen von Beschäftigten gem. § 4 Nr. 24 KDG, sowie auch bei rein tatsächlichen Beobachtungen durch Wach- oder Sicherheitspersonal. Ebenso bei einem Anruf beim früheren Arbeitgeber.

Der sachliche Anwendungsbereich des KDG ist nach unserer Ansicht mithin eröffnet.

Ein früherer Arbeitgeber, der bereitwillig Auskünfte über ehemalige Beschäftigte erteilt, handelt ohne Rechtsgrundlage und damit unzulässig.

Insoweit ist die Feststellung der Datenschutzaufsicht richtig, wenn sie in dem Verhalten des Abteilungsleiters einen Datenschutzverstoß sieht. Entgegen der gerichtlichen Entscheidung ist der Anwendungsbereich des KDG eröffnet und es wäre im Rahmen des Amtsermittlungsgrundsatzes zu prüfen gewesen, ob die Behauptungen des Betroffenen zutreffen. Sollte sich dies dabei als zutreffend herausstellen, wäre eine Beanstandung gegenüber dem betroffenen Bistum folgerichtig gewesen.

6.3 Nebentätigkeitsgenehmigung und Datenschutz

Die Pflichten von Beschäftigten ergeben sich aus dem Inhalt des Arbeitsvertrages. Beschäftigte haben die darin bestimmte und geschuldete Arbeitsleistung in dem festgelegten Umfang und an dem vertraglich vereinbarten Ort persönlich zu erbringen.

Außerhalb dieser arbeitsvertraglichen Pflichten sind Beschäftigte jedoch in der Verwendung ihrer Arbeitskraft frei. Das ergibt sich für eine berufliche (entgeltliche) Tätigkeit außerhalb des Hauptarbeitsverhältnisses aus der in Art. 12 Abs. 1 S. 1 GG geregelten Berufsfreiheit und für nicht berufliche (ehrenamtliche) Tätigkeiten aus Art. 2 Abs. 1 GG, der die freie Entfaltung der Persönlichkeit schützt.

Arbeitnehmer haben damit einen grundgesetzlich geschützten Anspruch auf Ausübung einer Nebentätigkeit. Im Umkehrschluss ist deshalb eine Klausel, die Arbeitnehmern jede entgeltliche oder unentgeltliche Nebentätigkeit untersagt, unwirksam.

Nach den einschlägigen Regelungen in den kirchlichen Dienstvertragsordnungen und „Tarif"-verträgen ist die Ausübung einer Nebentätigkeit ausdrücklich zulässig (z. B. § 5 Abs. 2 AVR; § 3 Abs. 3 DVO; § 19 KODA NW). Es besteht aber die Verpflichtung, die Arbeitgeberin über deren Aufnahme zu unterrichten (§ 5 Abs. 2 AVR) bzw. ist diese anzuzeigen (§ 3 Abs. 3 DVO; § 19 KAVO NW). Beschäftigte sind nicht verpflichtet, eine Zustimmung oder Genehmigung einzuholen. Vielmehr kann die Arbeitgeberin nach diesen Regelungen eine Nebentätigkeit nur untersagen oder mit Auflagen versehen, wenn die Nebentätigkeit geeignet ist, die arbeitsvertraglichen Haupt-

pflichten oder die berechtigten Interessen der Arbeitgeberin zu beeinträchtigen.

Das bedeutet, dass Arbeitnehmer nur solche Nebentätigkeiten zu unterlassen haben, die zur Beeinträchtigung des Hauptarbeitsverhältnisses führen oder entgegenstehende berechtigte Interessen der Arbeitgeberin berühren.

Eine Beeinträchtigung des Hauptarbeitsverhältnisses besteht in jedem Fall dann, wenn die Nebentätigkeit während des Hauptarbeitsverhältnisses, ggf. auch mit den Arbeitsmitteln der Arbeitgeberin ausgeübt werden soll. Darüber hinaus aber auch dann, wenn Beschäftigte wegen des Nebenarbeitsverhältnisses unausgeruht zum Hauptarbeitsverhältnis erscheinen und sich dies in mangelnder Leistung oder Konzentration objektiv auswirkt.

Berechtigte Interessen der Arbeitgeberin sind berührt, wenn eine Tätigkeit bei einem potentiellen Mitbewerber der Arbeitgeberin oder im gleichen Markt ausgeführt werden. Aber auch dann, wenn durch eine Nebentätigkeit der Ruf der Arbeitgeberin oder das Empfinden ihrer Kunden betroffen werden.

Weiterhin sind auch die Vorschriften des Arbeitszeitgesetzes einzuhalten. Adressat des öffentlich-rechtlichen Arbeitszeitschutzes ist die Arbeitgeberin. Sie hat die Einhaltung der dort bestimmten Höchstarbeitszeiten zu überwachen. Nach § 2 Absatz 1 Nr. 1, 2. Hs. ArbZG sind die Arbeitszeiten bei mehreren Arbeitgebern zusammenzurechnen. Soll eine Nebentätigkeit in einem zweiten Arbeitsverhältnis ausgeübt werden, darf die Arbeitgeberin ihre Zustimmung verweigern, wenn durch die Ausübung beider Tätigkeiten die gesetzliche Höchstarbeitszeit überschritten wird. Dabei ist zu berücksichtigen, dass Arbeitnehmer im Sinne des Arbeitszeitgesetzes nur Arbeiter und Angestellte sowie die zu ihrer Berufsbildung Beschäftigten (§ 2 Abs. 2 ArbZG) sind. Für Arbeitnehmer, die neben ihrer Haupttätigkeit freiberuflich bzw. selbständig tätig sind, gelten die arbeitszeitrechtlichen Regelungen nicht.

Aus den Darlegungen zu den arbeitsvertraglichen Pflichten der Arbeitsvertragsparteien ergibt sich die datenschutzrechtliche Begrenzung des Umfanges der vorzulegenden personenbezogenen Daten.

Die Vertragspartei, für die die Nebentätigkeit ausgeübt werden soll, ist der Arbeitgeberin zu benennen, wenn die Möglichkeit besteht, dass sich die Hauptarbeitgeberin zu dieser Vertragspartei in einem Konkurrenzverhältnis befinden kann.

Mitzuteilen ist auch, welche Tätigkeit in der Nebentätigkeit ausgeübt werden soll, damit die Arbeitgeberin prüfen kann, ob dadurch ihr Ruf oder das Empfinden ihrer Kunden gestört werden könnte.

Der zeitliche Umfang der Nebentätigkeit ist zu benennen, wenn es sich bei beiden Tätigkeiten um ein Arbeitsverhältnis im Sinne des Arbeitszeitgesetzes handelt. Die Arbeitgeberin muss dann prüfen können, ob die Summe der Arbeitszeiten aus beiden Arbeitsverhältnissen die vom Arbeitszeitgesetz festgelegte Höchstarbeitszeit überschreitet.

Wird die Nebentätigkeit im Rahmen einer selbständigen Tätigkeit ausgeübt, ist eine entsprechende Darlegung nicht erforderlich. Eine diesbezügliche Forderung der Arbeitgeberin wäre also unzulässig.

Ebenfalls nicht erforderlich ist es, die für die Nebentätigkeit vereinbarte Entgelthöhe mitzuteilen, da die Zustimmung der Arbeitgeberin nicht davon abhängig gemacht werden kann.

6.4 Abbildungen von Beschäftigten – immer wieder ein Problem

Wiederholt haben wir darauf hingewiesen, dass Veröffentlichungen, bei denen Beschäftigte abgebildet werden, eine Verarbeitung personenbezogener Daten darstellt. Für solche Darstellungen ist regelmäßig eine Einwilligung von Mitarbeitenden erforderlich, die vor der Veröffentlichung einzuholen ist.

Die Einwilligung ist jeweils für die konkrete Darstellung einzuholen und dabei ist darüber aufzuklären, in welchen Medien die Veröffentlichung erfolgen soll. Wenn Verantwortliche gegen diese Verpflichtungen verstoßen, kann dies neben einer Sanktion durch die Datenschutzaufsicht auch

zu einem Schadensersatzanspruch der betroffenen Beschäftigten führen. Einen solchen Fall hatte das LAG Schleswig-Holstein[30] zu entscheiden.

In einem 36-sekündigen Werbevideo eines Pflegedienstes war eine Mitarbeiterin ab Sekunde 11 zu sehen, wie sie in ein Dienstfahrzeug einsteigt und dann in Portraitgröße als sie im Fahrzeug sitzt. Nach Beendigung des Arbeitsverhältnisses hat die Mitarbeiterin den Arbeitgeber aufgefordert, das Video nicht weiter zu verwenden. Darüber hinaus hat sie ein Schmerzensgeld gefordert, weil ihre Persönlichkeitsrechte durch die Aufnahmen beeinträchtigt worden seien.

Der Arbeitgeber hatte es versäumt, vorab eine schriftliche Einwilligungserklärung der Mitarbeiterin einzuholen, aus der hervorgeht, dass sie mit der Verarbeitung einverstanden ist.

Das Gericht stellt dazu fest:

> *„Durch den geltend gemachten Verstoß der Beklagten gegen die Bestimmungen der DS-GVO ist der Klägerin ein immaterieller Schaden entstanden. Der Rechtsanspruch auf immateriellen Schadensersatz nach Art. 82 Abs. 1 DS-GVO erfordert über die Verletzung der DS-GVO hinaus nicht zusätzlich, dass die verletzte Person einen (weiteren) von ihr erlittenen immateriellen Schaden darlegt. Bereits die Verletzung der DS-GVO selbst führt zu einem auszugleichenden immateriellen Schaden."*

Im vorliegenden Fall hielten die Richter einen Schmerzensgeldanspruch der Klägerin in Höhe von 2.000 € für gerechtfertigt.

Interessant ist in diesem Fall, dass das Gericht keine Ausführungen zur Erheblichkeit des Verstoßes gemacht hat. Der Schmerzensgeldanspruch der Klägerin sei auch gerechtfertigt, obwohl die Klägerin nicht in ihrem Intimbereich betroffen sei und sogar sehenden Auges an der Erstellung des Videos mitgewirkt habe. Darüber hinaus halten die Richter die Höhe des Schmerzensgeldanspruches für gerechtfertigt, weil eine Entschädigung wegen eines Verstoßes gegen die DS-GVO über eine symbolhafte Summe hinausgehen muss. Zu diesem Problemkreis verweisen wir auch auf unsere Ausführungen zur Entscheidung des ArbG Neuruppin unter Punkt 1.2.7 in diesem Bericht.

30 LAG Schleswig-Holstein, Beschluss vom 01.06.2022 - 6 Ta 49/22

6.5 Kündigung von Menschen mit Behinderung während der Probezeit

Regelmäßig wird für den Beginn eines Arbeitsverhältnisses eine Probezeit vereinbart. Diese beträgt häufig sechs Monate. Dieser zeitliche Umfang ist der Tatsache geschuldet, dass erst dann die Regelungen des Kündigungsschutzgesetzes greifen. Für Menschen mit Behinderung besteht gem. § 168 SGB IX ein besonderer Kündigungsschutz, weil eine Kündigung der vorherigen Zustimmung des Integrationsamtes bedarf. Allerdings gilt auch dieser besondere Kündigungsschutz nach § 173 Abs. 1 Nr. 1 SGB IX erst, wenn das Arbeitsverhältnis zum Zeitpunkt des Zugangs der Kündigungserklärung ohne Unterbrechung bereits länger als sechs Monate bestanden hat.

Arbeitgeberinnen sind nach diesen gesetzlichen Vorgaben also weitgehend frei, in diesem Zeitraum ein bestehendes Arbeitsverhältnis zu beenden, soweit nicht offensichtliche Willkür oder Diskriminierung der Grund sind. Speziell mit der Regelung den besonderen Kündigungsschutz für Menschen mit Behinderung auch erst nach einer Beschäftigungszeit von einem halben Jahr wirksam werden zu lassen, wollte der Gesetzgeber erreichen, dass dieser Personenkreis nicht dadurch benachteiligt wird, weil Arbeitgeber in dem verstärkten Kündigungsschutz eine Einschränkung ihrer Entscheidungsfreiheit sehen.

Eine Entscheidung des Europäischen Gerichtshofs[31] stellt nun aber klar, dass eine Kündigung von Menschen mit Behinderung auch in der Probezeit nur eingeschränkt möglich ist. Aufgrund von Art. 5 der europäischen Gleichbehandlungsrahmenrichtlinie (Richtlinie 2000/78/EG), die die Diskriminierung von Menschen mit Behinderung im Arbeitsverhältnis untersagt, ist der Arbeitgeber verpflichtet, „angemessene Vorkehrungen für Menschen mit Behinderungen" zu treffen. In seinem Urteil stellt der EuGH fest, dass dieser Begriff impliziert, dass Beschäftigte, die aufgrund einer Behinderung für ungeeignet erklärt wurden, die wesentlichen Funktionen der bisherigen Stelle zu erfüllen, auf einer anderen Stelle einzusetzen sind, für die sie die notwendige Kompetenz, Fähigkeit und Verfügbarkeit aufweisen. Dies gilt ausdrücklich auch für die Probezeit[32].

31 EuGH, Urteil vom 10.02.2022 - C-485/20 HR Rail
32 EuGH, Pressemitteilung Nr. 26/22 vom 10.02.2022

Es liegt die Befürchtung nahe, dass diese Entscheidung Menschen mit Behinderung „Steine statt Brot“ gibt. Werden Menschen mit Behinderung nunmehr in der Probezeit stärker vor Kündigung geschützt als alle anderen, könnten sich Arbeitgeber veranlasst sehen, nur Menschen ohne Behinderung einzustellen.

Dieser Befürchtung kann jedoch mit konsequenter Einhaltung des Datenschutzes begegnet werden. Es gibt keine gesetzliche Grundlage, die Bewerbende dazu verpflichtet, gegenüber einem potentiellen Arbeitgeber anzugeben, ob sie einen Schwerbehindertenausweis besitzen. Die Schwerbehinderteneigenschaft stellt ein personenbezogenes Datum besonderer Kategorie gem. § 4 Nr. 2 KDG (Art. 9 Abs. 1 DS-GVO) dar. Die Verarbeitung besonderer Kategorien personenbezogener Daten ist gem. § 11 Abs. 1 KDG (Art. 9 Abs. 1 DS-GVO) verboten. Ein Ausnahmetatbestand im Sinne des jeweiligen Abs. 2 der genannten Vorschriften ist nicht gegeben. Darüber hinaus ist die Verarbeitung dieses Datums auch gem. § 53 KDG (§ 26 BDSG) nicht für die Begründung des Arbeitsverhältnisses erforderlich.

Fazit: Bewerbende sind also nicht verpflichtet, Auskunft darüber zu geben, ob sie als Schwerbehinderte anerkannt sind. Arbeitgeber sind nicht berechtigt Bewerbende tätigkeitsneutral nach einer Schwerbehinderung zu fragen.

Davon zu unterscheiden ist die Frage nach solchen gesundheitlichen Einschränkungen, die die Übernahme der arbeitsvertraglich geschuldeten Tätigkeit dauerhaft unmöglich machen. Diese Frage ist aber unabhängig davon, ob eine anerkannte Schwerbehinderung vorliegt, da für den Arbeitgeber nur von Interesse ist, ob der Bewerber die ausgeschriebene Tätigkeit übernehmen kann oder nicht. Das hängt aber nicht vom Besitz eines Schwerbehindertenausweises ab.

6.6 Datenschutz nur solange es keine Arbeit macht?

Entfernung einer Abmahnung aus der Personalakte nach Beendigung des Arbeitsverhältnisses

Entscheidet sich eine Arbeitgeberin zum Ausspruch einer Abmahnung, verfolgt sie dabei zwei Ziele. Zum einen wird damit eine Pflichtverletzung

Beschäftigter gerügt. In einer hinreichend deutlichen Art und Weise werden Mitarbeitende damit aufgefordert, ihre arbeitsvertraglichen Pflichten einzuhalten (Rügefunktion). Zum anderen ist damit die Androhung arbeitsrechtlicher Konsequenzen für den Fall verbunden, dass sich die Pflichtverletzung wiederholt (Warnfunktion).

Mit einer Abmahnung werden personenbezogene Daten verarbeitet. Dies ist rechtmäßig, wenn und solange damit eine der Bedingungen des § 6 Abs. 1 KDG erfüllt ist bzw. wenn dies gem. § 53 KDG für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.

Nach einer Entscheidung des LAG Sachsen-Anhalt[33] ist das dann nicht mehr der Fall, wenn das Arbeitsverhältnis beendet ist. Denn nach der Beendigung eines Arbeitsverhältnisses kann weder die Rüge- noch die Warnfunktion einer Abmahnung eine Wirkung entfalten, weshalb die Erforderlichkeit zur weiteren Verarbeitung (Speicherung) nicht mehr gegeben ist.

Anders hat jetzt das LAG Niedersachsen[34] entschieden.

Die Richter stellen zunächst fest, dass der Anspruch auf Löschung dann und soweit nicht besteht, sofern gesetzliche Aufbewahrungsfristen dem entgegenstehen. Solche können nach den Ausführungen des Gerichts insbesondere steuer- oder sozialversicherungsrechtlicher Art sein. Gleichzeitig referiert das Gericht die in der Literatur vertretene Meinung, personenbezogene Daten seien nach Beendigung des Arbeitsverhältnisses zu löschen, soweit Aufbewahrungsfristen nicht bestünden. Auch das Urteil des LAG Sachsen-Anhalt wird in diesem Zusammenhang zitiert. Für seine Rechtsauffassung führt das Gericht dann aber lediglich Praktikabilitätsgründe an: „in der Konsequenz würde dies bedeuten, dass der Arbeitgeber nach Beendigung eines jeden Arbeitsverhältnisses den vorhandenen Datenbestand des ausscheidenden Arbeitnehmers danach sortieren müsse, ob Aufbewahrungsfristen bestehen oder nicht." Dabei übersieht das Gericht, dass es keinen Rechtsgrundsatz gibt, der die Verarbeitung personenbezogener Daten erlaubt, nur weil ihre pflichtgemäße Löschung mit Arbeit verbunden ist.

Im Gegenteil verlangt Art. 12 Abs. 3 DS-GVO (§ 14 Abs. 3 KDG) die unverzügliche Erledigung eines Löschungsantrages, spätestens innerhalb eines

33 LAG Sachsen-Anhalt, Urteil vom 23.11.2018 – 5 Sa 7/17
34 LAG Niedersachsen, Urteil vom 04.05.2021 – 11 Sa 1180/20

Monats und gewährt für den Fall einer hohen Komplexität oder einer großen Anzahl von entsprechenden Anträgen eine Fristverlängerung von weiteren zwei Monaten.

Das Urteil des LAG Niedersachsen entbehrt somit einer rechtlichen Grundlage, der Auffassung des Gerichts ist deshalb und unter Zugrundelegung der in der Literatur vertretenen Ansicht und dem Urteil des LAG Sachsen-Anhalt nicht zu folgen.

7 Technischer Datenschutz

7.1 Unterschied zwischen Authentisierung, Authentifizierung und Autorisierung

Inzwischen sollte der Grundsatz für alle Beschäftigte hinlänglich bekannt sein, dass nicht jeder auf alle personenbezogene Daten Zugriff haben sollte. Geltende Datenschutzbestimmungen verlangen von Unternehmen, Einrichtungen etc. diese Vorgabe strikt einzuhalten. Aus diesem Grund sind IT-Systeme mit Zugangskontrollen und Berechtigungsmechanismen ausgestattet: Bei einem Zugriff auf Daten (egal welcher Art) müssen die Personen zuerst nachweisen, dass sie zum Zugriff auf genau diese Daten berechtigt sind.

Solch eine Überprüfung wird gerne als Authentisierung, Authentifizierung oder Autorisierung bezeichnet. Häufig wird davon ausgegangen, dass alle drei Begriffe dieselbe Bedeutung haben. Da die drei „AAA-Begriffe“ ähnlich „klingen“, wird oftmals darunter die dieselbe Bedeutung verstanden. Doch dem ist nicht so, denn tatsächlich gibt es gravierende Unterschiede.

Zur Veranschaulichung ein vereinfachtes Beispiel:

Ein Zugangs-/Zugriffs-Prozess auf die Daten lässt sich vereinfacht in drei Schritten (**A-A-A**) abbilden. Dabei stehen **A**uthentisierung, **A**uthentifizierung und **A**utorisierung für jeweils einen dieser Schritte.

Zum Anfang ist standardmäßig alles auf Rot: [**A-A-A**].

1. **Authentisierung:** Authentisierung bezeichnet das Nachweisen einer Identität. Eine Person oder ein Service (z.B. ein Gerät, Token,

Dienst) möchte aus seiner Perspektive eine Anmeldung an einem IT-System durchführen. Dafür benutzt es eine/seine Identität. Eine Authentisierung kann in Form von Benutzerkennung erfolgen, oder aber auch in jeder anderen Form, wie z.B. per Chipkarte oder anhand biometrischer Merkmale, z. B. ein Fingerabdruck. Damit ist allerdings noch kein Zugang gewährt.

Zur Veranschaulichung: Jemand steht vor der Haustür und klingelt! [**A-A-A**]

2. Authentifizierung: Authentifizierung bezeichnet die Prüfung des Identitätsnachweises auf seine Authentizität (Echtheit, authentisch). Im Rahmen der Authentifizierung werden die von der Identität (z.B. von einer Person) gemachten Angaben überprüft. Dafür werden in der Regel Identitäten aus einer Datenbasis (dem Wissen) abgeglichen und im Erfolgsfall als „bekannt" bestätigt.

Zur Veranschaulichung: Ein Blick aus dem Fenster – „oh der Postbote Max Postman ist es" – die Identität ist bereits „bekannt"! Diese Identität (er) ist berechtigt einen Schlüssel zu erhalten [**A-A-A**]. Er erhält Schlüssel Nummer 9.

3. Autorisierung: Die Autorisierung ist eine Berechtigung, d.h. eine explizite Zulassung oder Sperrung auf etwas, die sich auf die authentifizierte Identität (z.B. der Postbote Max Postman) bezieht. Sie definiert welche bereits bestätigte Identität welche Dienste und welche System-Ressourcen nutzen darf. Damit werden der Identität (z.B. Max Postman) im Rahmen eines Rollen- und Berechtigungskonzepts Berechtigungen eingeräumt oder verwehrt. Die Berechtigungen entscheiden darüber, in welchem Umfang das System dann nutzbar ist und beispielsweise auf welche Daten zugegriffen werden darf.

Zur Veranschaulichung: Der jetzt identifizierte und auch authentifizierte Max Postman (Identität) kann mit dem Schlüssel Nummer 9 eine Tür öffnen, bei der er auch Zugang zur Paketablage mit der Nummer 9 erhält und ein Paket abholt oder einlagert (speichert). [**A-A-A**]. Mit dem Schlüssel Nummer 9 hat er keine Möglichkeit weitere Türen oder Paketablagen zu öffnen.

Einige mögen eine solch präzise Unterscheidung als Spitzfindigkeit erachten. Doch gerade jetzt in der Digitalisierung und einer Zunahme von Cyberattacken ist sie mehr als nur notwendig. Dies trifft besonders für sensible Dokumentationen zu, wie z.B. Bewerber- und/oder Personaldaten, Gesundheitsdaten, interne sensible Infrastruktur-Unterlagen. Dort ist es wichtig, die Begriffe auseinanderzuhalten und korrekt in Rollen- und Berechtigungs-Prozessen zu verwenden.

7.2 Microsoft 365 und Windows

7.2.1 Einsatz von Microsoft 365 - noch immer nicht ausreichend

Die Dokumentation der Datentransfers von Microsoft 365 reicht noch immer nicht aus, um einen rechtmäßigen Einsatz nachzuweisen.

Microsoft konnte die deutschen Datenschutzbehörden nicht davon überzeugen, dass der Einsatz von Microsoft 365 in Behörden, Schulen oder Unternehmen rechtskonform gestaltet werden kann.

Der Bundesdatenschutzbeauftragte Ulrich Kelber erklärte am 24. November 2022 zum Abschluss der Datenschutzkonferenz von Bund und Ländern (DSK) auf einer Pressekonferenz, dass weiterhin unklar sei, welche Daten erhoben, übertragen und für eigene Zwecke verarbeitet würden.

Es gäbe weiterhin Mängel in der Transparenz und der Prüfung, ob die Datenverarbeitung zu eigenen Zwecken rechtmäßig sei. Kelber sieht daher weiteren „Verbesserungsbedarf".

Die Arbeitsgruppe DSK Microsoft Onlinedienste hatte auf Basis von Microsoft-Unterlagen einen als vertraulich eingestuften Bericht erstellt. Die DSK hat dazu inzwischen eine Zusammenfassung veröffentlicht[35].

Auf Grundlage des Beschlusses kam die DSK u. a. zu folgender Festlegung:

35 https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

> *„Die DSK stellt unter Bezugnahme auf die Zusammenfassung des Berichtes fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022" nicht geführt werden kann".*
> *„Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden."*

Kelber führt aus, die der DSK vorliegenden Unterlagen hatten nicht ausgereicht, „um die Rechtmäßigkeit des Einsatzes von Microsoft 365 belegen zu können".

7.2.2 BSI – Telemetrie-Komponente in Windows

Das BSI hat im Projekt „SiSyPHuS Win10: Analyse der Telemetriekomponenten[36]" die technischen Analysen von Windows 10 aktualisiert und u.a. die Deaktivierung der Telemetrie erneut betrachtet. Das BSI gibt damit aktualisierte Empfehlungen zur Deaktivierung der Telemetrie sowie eine Liste aktueller Telemetrie-Endpunkte für Windows. Zudem hat das BSI mit dem Telemetrie Monitoring Framework (TMFW) eine technische Lösung zur Überwachung der analysierten Telemetrie-Komponente erarbeitet.

Für Benutzer, die Microsoft-Produkte und/oder -Dienste nutzen, während Sie mit Ihrem Microsoft-Konto angemeldet sind, bietet Microsoft selbst ein Datenschutz-Dashboard[37] an, mit dem sich Benutzer sich anzeigen lassen können, welche Daten gesammelt wurden. Dort können u.a. auch Daten manuell gelöscht werden.

An dieser Stelle sei erwähnt, dass sich eine **Telemetrie-Datenerfassung nicht nur auf Microsoft** bezieht, sie betrifft auch zahlreiche Software anderer Hersteller, etwa Google mit Android.

36 https://www.bsi.bund.de/dok/11713512
37 https://account.microsoft.com/privacy

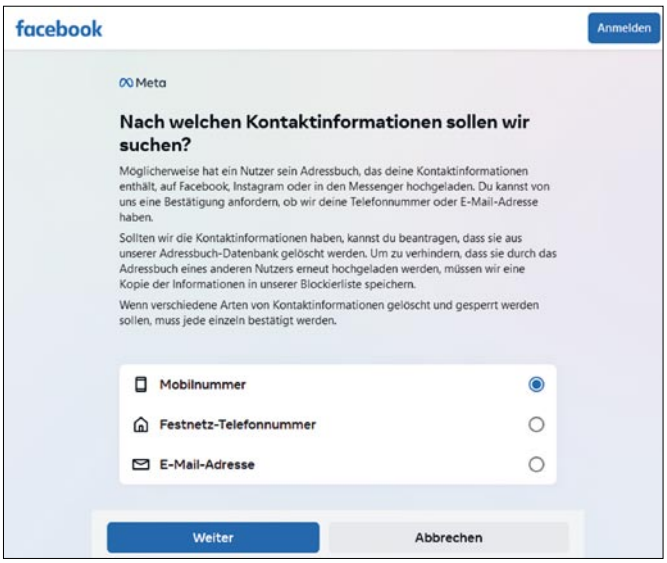
7.3 Aus den sozialen Medien

7.3.1 Ich bin nicht bei WhatsApp, Instagram - oder doch?

Meta (WhatsApp, Instagram, Facebook) macht in den AGBs kein Geheimnis daraus, dass z.B. der Messenger-Dienst alle Kontakt-Adressdaten vom Smartphone überträgt. Demzufolge werden u.a. Kontaktinformationen von Personen zu Meta übermittelt, die kein Benutzerkonto haben und den Dienst auch nicht nutzen.

Durch diese Datenverarbeitung entstehen quasi „Schattenprofile“, durch die u.a. Kontakt-Querverbindungen ausgewertet werden könnten.

Meta kennt mich also durch „Andere“, auch wenn ich mir nie einen Benutzer-Account anlege.

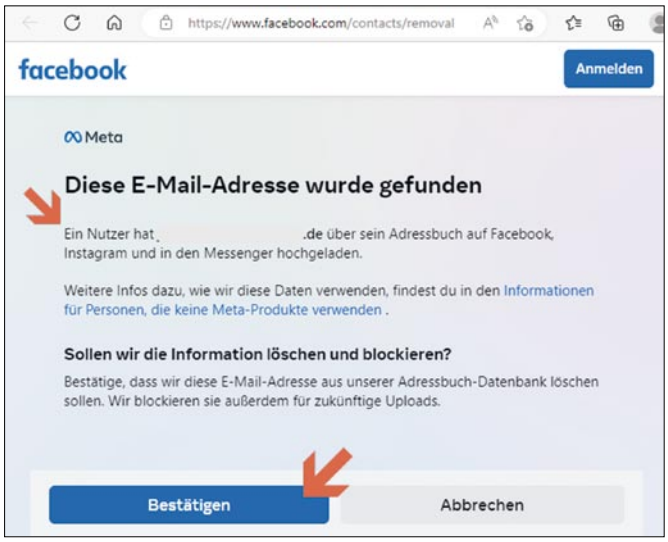


Ob mich Meta kennt, kann man leicht selbst überprüfen und das geht so:

Meta stellt ein Webformular zur Verfügung, welches die Möglichkeit bietet, selbst zu überprüfen, ob die eigenen Kontaktinformationen gespeichert sind.

Möglicherweise hat ein Nutzer sein Adressbuch, das deine Kontaktinformationen enthält, **auf Facebook, Instagram oder in den Messenger hochgeladen.** Man kann von Meta eine Bestätigung anfordern, ob die eigene Telefonnummer oder E-Mail-Adresse dort gespeichert ist.

Link zum Zeitpunkt des Berichts:
https://www.facebook.com/
contacts/removal



7.3.2 Meta hat Apps identifiziert, die Facebook Zugangsdaten ausspionieren

Auf der Website von Meta heißt es: „ … *Wir haben in diesem Jahr mehr als 400 bösartige Android- und iOS-Apps identifiziert, die auf Personen im Internet abzielen, um ihre Facebook-Anmeldeinformationen zu stehlen. Unsere Sicherheitsforscher haben in diesem Jahr mehr als 400 schädliche Android- und iOS-Apps gefunden, die darauf ausgelegt waren, Facebook-Anmeldeinformationen zu stehlen und die Konten von Personen zu kompromittieren…*"

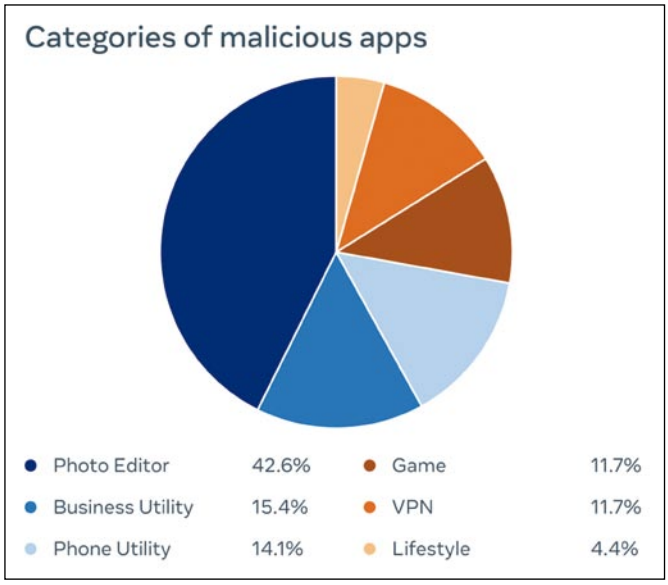


Bild: Meta (protecting-people-from-malicious-account-compromise-apps)

Die analysierten Apps wurden im Google Play Store und im App Store von Apple gelistet und als Bildbearbeitungsprogramme, Spiele, VPN-Dienste, Business-Apps und andere Dienstprogramme getarnt, um Personen dazu zu verleiten, sie herunterzuladen.

Wenn eine Person eine dieser Apps installiert hat, wird sie vor dem Start der versprochenen Funktionen aufgefordert, sich mit den Facebook-Zugangsdaten anzumelden. Die dort eingetragenen Anmeldedaten (Benutzernamen und Passwort) sind danach der App und somit u.a. dem App-Betreiber/Entwickler zur weiteren Verarbeitung/Nutzung bekannt.

Empfehlung: Anwender sollten prüfen, ob sie ggf. eine gelistete App installiert haben und es kann zudem nicht schaden, proaktiv sein Passwort zu ändern[38].

7.4 Website - Vorbeugen vor Abmahnung

7.4.1 Abmahnwelle im Fall Google-Fonts

Im letzten Quartal des Berichtszeitraums erhielten viele Betriebe und Einrichtungen Abmahnschreiben mit einer Geldforderung aufgrund der Einbindung von Google-Fonts auf deren Webseiten. In den meisten Fällen kamen diese Schreiben von Rechtsanwaltskanzleien, die sich auf Abmahnungen im großen Stil spezialisiert haben.

Wie kam es dazu?

Das Landgericht München hat mit Urteil vom 20.01.2022 die Betreiberin einer Website für den Einsatz von Google Fonts neben Unterlassung zu einem Schadensersatz in Höhe von 100 Euro verurteilt, da der Webseitenbetreiber Google-Fonts und damit verbunden die IP-Adresse an Google übermittelt hat. Für die Übermittlung an Google gab es keine Einwilligung seitens des Nutzers.

Laut einem Urteil des BGH[39] stellt die IP-Adresse ein personenbezogenes Datum dar, welches durch die Weitergabe an Google unerlaubt verarbeitet wird und somit eine Verletzung des allgemeinen Persönlichkeitsrechts darstellt, so die Begründung in den Abmahnungen.

Dabei ist Google-Fonts nur ein Beispiel von vielen. In der Regel existieren noch mehr Dienste, die regelmäßig in Webseiten eingebunden werden (z.B. Karten, Captcha-Dienste). Übermitteln diese Dienste im Hintergrund

38 https://about.fb.com/news/2022/10/protecting-people-from-malicious-account-compromise-apps
39 BGH, Urteil vom 16.05.2017 - VI ZR 135/13

Daten an Drittanbieter (z.B. Google, Meta, YouTube), so muss vorher eine gültige Einwilligung vorliegen. Bei der Nutzung von Webseiten geschieht dies in aller Regel mit Hilfe eines sogenannten „Consent-Banners", der die entsprechenden Informationen enthält.

Nachdem im Herbst 2022 zahlreiche Abmahnungen bei deutschen Webseitenbetreibern eingegangen waren, da sie für ihre Schriftarten Google Fonts in die Webseite eingebunden hatten, musste das Amtsgericht Berlin-Charlottenburg[40] im Rahmen einer negativen Feststellungsklage über die Begründetheit des Schadensersatzanspruchs der Abmahnung entscheiden.

Das AG Berlin-Charlottenburg entschied, dass dem Abmahner kein Schadensersatzanspruch aus der Verwendung von Google-Fonts durch einen Webseitenbetreiber zusteht. Im Falle der dynamischen Einbindung von Google-Fonts komme zwar ein Datenschutzverstoß in Betracht, sofern die Übertragung der IP-Adresse des Seitenbesuchers ohne vorherige Einwilligung erfolgt. Ein Schadensersatzanspruch steht dem "Verletzten" aber nicht zu – weder *„aus § 823 BGB noch aus der DS-GVO oder unter einem anderen rechtlichen Gesichtspunkt"*. Zudem hält das Gericht die Masche der Abmahnenden dann für rechtsmissbräuchlich, wenn sich der vermeintlich Geschädigte eine Einnahmequelle durch das massenhafte Versenden von „Abmahnungen" schafft. Vorliegend wurden derartige Umstände in großem Umfang geltend gemacht, weshalb ein Rechtsmissbrauch nach Ansicht des Gerichts durchaus vorliegen könnte.

Generelle Empfehlung: Unternehmen und auch Privatpersonen sollten überprüfen, welche Webdienste sie auf ihren Internetseiten eingebunden haben, für die eine Einwilligung benötigt wird. Grundsätzlich können Webdienste auch immer lokal auf dem eigenen Server gespeichert und von dort geladen werden. Alternativen können Dienste, z. B. auch Schriftarten (Webfonts) genutzt werden, die keine Cookies setzen oder IP-Adressen im Hintergrund weiterleiten. Sollte eine dynamische Einbindung der Schriften technisch notwendig sein, muss ein zusätzliches „Consent-Tool" eingesetzt werden, mit dem die Einwilligung der Seitenbesucher vor dem Aufbau der Seite eingeholt wird.

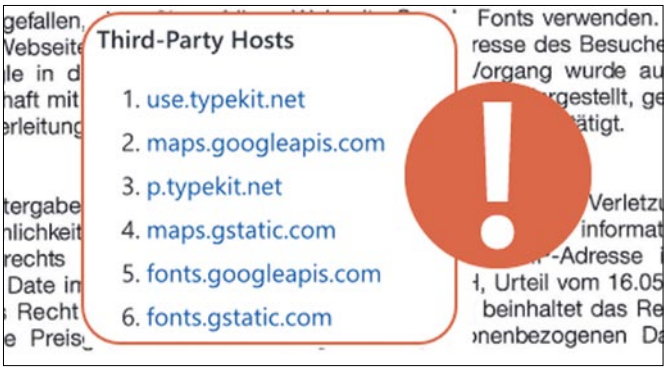
40 AG Charlottenburg, Urteil vom 20.12.2022 - 217 C 64/22

7.4.2 Website Überprüfungen und Selbstcheck

In unseren TB 2021 hatten wir darüber informiert, dass unsere Website Überprüfungen fortgesetzt und ggf. ausgeweitet werden. Aus Anlass des Inkrafttretens des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) im Dezember 2021, lag der Fokus im aktuellen Berichtsjahr auf folgenden Überprüfungen:

1. Querverbindungen zur Drittanbietern (Drittanbieter-Hosts), darunter u.a. auch die Einbindung von Schriftarten (Fonts)
2. Setzen von Cookies

In Anlehnung an die Ergebnisse der anlasslosen wie auch anlassbezogenen Überprüfungen haben wir uns zur Sensibilisierung dazu entschlossen, eine Online-Veranstaltung durchzuführen (1 Jahr TTDSG und Websites mit Fonts und Co). Im Rahmen dieser Veranstaltung ging es u.a. um eingebundene „Webfonts" (Schriftarten) und darum wie ein Verantwortlicher oder ein Datenschutzbeauftragter (bDSB) einen Test mit den vorhandenen Mitteln eines Webbrowsers selbst durchführen kann. Denn auch im Hinblick auf die Erstellung einer Datenschutzinformation ist es wichtig zu wissen, wie die Website aufgebaut ist, welche zusätzlichen Komponenten integriert sind und was sich ggf. im Hintergrund abspielt.



Durch die positive Resonanz und dem Interesse an dieser Veranstaltung wiederholen wir im aktuellen Geschäftsjahr (2023) die Veranstaltungsreihe. Termine zu unseren Veranstaltungen und Video-Sprechstunden veröffentlichen wir auf unserer Website unter www.kdsa-ost.de/termine.

7.5 Schöne neue HR-Welt: Robot Recruiting und die rechtlichen Grenzen

Digitalisierung bedeutet nicht nur Remote-Work und Videokonferenz – auch in der Personalabteilung verändert sich gerade vieles. Eine wichtige Neuerung ist das sogenannte Robot-Recruiting, bei dem künstliche Intelligenz den Menschen im Recruiting-Prozess unterstützt.

Für den Begriff der künstlichen Intelligenz (KI) findet sich bislang noch keine allgemeingültige Definition. Oft wird sie mit maschinellem Lernen oder Big Data Analytics gleichgesetzt. Im juristischen Sprachgebrauch wird der Begriff künstliche Intelligenz daher häufig verwendet, um Algorithmen zu beschreiben.

Algorithmen, die in der Lage sind, aus der Analyse von Daten zu „lernen", können sich weiterentwickeln, sich neuen Situationen anpassen und selbstständig Korrelationen herstellen. Das bedeutet, man kann ein solches System etwa mit den Daten bereits eingestellter Bewerber „füttern" und so herausfinden lassen, welche Eigenschaften sie auszeichnen. Die so gewonnenen Erkenntnisse lassen sich gezielt bei zukünftigen Bewerberprozessen verwenden. Diese automatisierte Durchführung eines Bewerberverfahrens nennt sich „Robot Recruiting".

Robot Recruiting wird bislang der sogenannten „schwachen künstlichen Intelligenz" zugerechnet. Das bedeutet, dass die Systeme auf die Lösung konkreter Anwendungsprobleme auf Basis von Methoden aus der Mathematik und Informatik fokussiert sind. Dem gegenüber besitzen „starke" KI-Systeme die gleichen intellektuellen Fähigkeiten wie ein Mensch und können diesen darin sogar übertreffen. Abzugrenzen vom Begriff Robot Recruiting ist das Recruiting 4.0: Hier wird der Prozess der Personalbeschaffung durch die Verwendung von digitalen Plattformen und Medien unterstützt.

Rechtliche Grenzen von Robot Recruiting

Fraglich ist, inwieweit das Robot-Recruiting in Deutschland derzeit zulässig ist. Die rechtlichen Grenzen richten sich derzeit insbesondere nach dem

Bundesdatenschutzgesetz (BDSG) und der Datenschutzgrundverordnung (DS-GVO).

Nach dem BDSG dürfen personenbezogene Daten im Rahmen eines Arbeitsverhältnisses nicht in jedem Fall erhoben und verarbeitet werden (§ 26 BDSG). Vielmehr muss die Datenverarbeitung für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich sein. Die Begründung verlangt eine umfangreiche Abwägung der widerstreitenden Interessen und Rechtsgüter im Einzelfall. Die Rechtsprechung vertritt hierbei einen sehr restriktiven Ansatz.

Das BDSG macht allerdings eine Einschränkung, wonach eine Datenverarbeitung jedenfalls möglich ist, wenn und soweit eine freiwillige Einwilligung der Bewerberin oder des Bewerbers vorliegt. Die Freiwilligkeit der Einwilligung ist jedoch im Rahmen eines Bewerbungsprozesses in der Regel abzulehnen, denn Freiwilligkeit kann nur angenommen werden, sofern der Bewerber in der Lage ist, die Einwilligung zu verweigern, ohne einen Nachteil zu erleiden. Bei einer Ablehnung des Bewerbungsprozesses muss er jedoch befürchten, gar nicht erst in Betracht gezogen zu werden.

Die DS-GVO untersagt es, eine Person, die von einer Datenverarbeitung betroffen ist, einer ausschließlich auf einem automatisierten Prozess beruhenden Einzelentscheidung zu unterwerfen (sogenanntes „Profiling“, Art. 22 DS-GVO / § 24 KDG). Genauer: Diese Regelung schützt im Bereich des Personalwesens den Bewerber davor, von einer Entscheidung betroffen zu sein, die aus einem automatisierten Datenverarbeitungsprozess entspringt, ohne dass ein Mensch substanziell steuernd dazwischengetreten ist. Mithin muss sich der Einsatz von künstlicher Intelligenz im Bewerbungsverfahren darauf beschränken, eine Vorauswahl unter Bewerbern zu treffen. Auch hier existiert ein Ausnahmetatbestand für die Einwilligung des Bewerbers, doch auch hier kann in der Regel nicht von einer Freiwilligkeit ausgegangen werden.

Nach der DS-GVO / dem KDG ist der Bewerber außerdem bei Erhebung von personenbezogenen Daten zu informieren (Art. 13 DS-GVO / § 15 KDG) und erhält einen Auskunftsanspruch (Art. 15 DS-GVO / § 17 KDG) – er kann also Auskunft darüber verlangen, ob und welche personenbezogenen Daten erhoben und verarbeitet wurden

Zwischen Objektivität und „maschineller Diskriminierung“

Intelligente Softwarekonzepte eröffnen neue Möglichkeiten im Recruiting. Bereits vor dem Bewerbungsgespräch kann ein automatisierter Algorithmus eine Vorauswahl treffen. Das spart Zeit, denn automatisierte Systeme sind in der Lage, große Datenmengen präziser und schneller zu durchsuchen als der Mensch.

Grundsätzlich sind die intelligenten Systeme zudem in der Lage, eine Entscheidung rein objektiv zu fällen, also sie ausschließlich auf Tatsachen aufzubauen. Künstliche Intelligenz lässt sich nicht von (eigenen) Vorurteilen oder Stimmungen beeinflussen und kann so dabei helfen, Benachteiligungen aus den im Allgemeinen Gleichbehandlungsgesetz genannten Gründen zu verhindern.

Dennoch ist Vorsicht geboten, denn auch bei automatisierten Bewerbungsprozessen ist Diskriminierungspotenzial in Form von sogenannter stellvertretender Diskriminierung (Proxy Discrimination) gegeben. Dazu kann es etwa kommen, wenn eine Gruppe im Datensatz der Vergangenheit überrepräsentiert war und so vom selbstlernenden System auch in Zukunft bevorzugt wird. Einfach ausgedrückt: Wurden bislang hauptsächlich weiße Männer eingestellt, so kann das System aus dem Datensatz lernen, dass weiße Männer bevorzugt eingestellt werden sollen.

Ein weiteres Risiko: Die Leistungsfähigkeit von selbstlernenden Systemen wird zunehmend dazu führen, dass ihr Output von außen immer schwerer nachzuvollziehen ist. Hier muss wieder der Mensch eingreifen und untersuchen, wie das Ergebnis des Datenverarbeitungsprozesses zustande gekommen ist. Das kann mit einem erheblichen Aufwand verbunden sein.

7.6 Keine Daten – kein Datenschutzvorfall

Nicht ohne Grund wurde das Wort **„Datenschutzvorfall“** genannt und nicht **„Datenschutzrelevant“**, denn **keine Daten** kann auch bedeuten, dass Daten zerstört sind und darauf kein Zugriff mehr möglich ist. Für diesen Fall sollten technische und organisatorische Maßnahmen getroffen worden sein, um die Daten wiederherstellen zu können. Daten, auch ohne Personenbezug, z.B. betriebswirtschaftliche Daten, die verarbeitet werden, sollten ständig verfügbar sein.

„Keine Daten“ könnte u.a. auch bedeuten, dass auf Grund eines Datenverlustes (Diebstahl, Daten zerstört und unbrauchbar, kein Zugriff, …) es keine Daten mehr gibt oder der Zugriff auf benötigte Informationen nicht mehr möglich ist. Wenn sich nun aber gerade in diesen Datenbeständen personenbezogene und wirtschaftlich wichtige Daten befinden, sind diese Daten nicht mehr verfügbar. Dies ist u.U. nicht nur ein wirtschaftlicher Schaden, sondern kann auch eine datenschutzrelevante und ggf. eine meldepflichtige Datenpanne darstellen, die sich als eine Datenschutzverletzung nach KDG (DS-GVO) erweisen kann.

7.6.1 Unlesbare Daten - nicht datenschutzrelevant

Häufig wird angenommen, dass der Verlust unlesbarer Daten keinen Datenschutzverstoß darstellt. Dem ist nicht so, denn auch unlesbare und/oder verschlüsselte Daten sind Daten. Das bedeutet, dass verschlüsselte Daten mit „Personenbezug“ auch personenbezogene Daten im rechtlichen Sinne sein können, die den geltenden Datenschutzbestimmungen unterfallen. Sofern festgestellt werden sollte, dass eine Entschlüsselung und damit verbunden eine Offenlegung dieser Daten unwahrscheinlich oder unmöglich erscheint, läge darin kein Datenschutzvorfall.

Bei den Maßnahmen zur Verschlüsselung ist selbstverständlich der entsprechende „Stand der Technik“ zu berücksichtigen.

7.6.2 Schutz durch Datenverschlüsselung

Zum Schutz personenbezogener und/oder sicherheitsrelevanter Daten ist die Datenverschlüsselung eine technische Maßnahme (§ 6 KDG-DVO). Damit können Einrichtungen, Betriebe, etc. die Wahrscheinlichkeit einer Datenpanne und somit auch eines Verstoßes gegen geltende Datenschutzbestimmungen verringern. Ein weiterer Vorteil für den Verantwortlichen oder den Auftragsverarbeiter ist, dass bei einem Verlust der Daten durch die Verschlüsselung keine Gefahr für die Rechte und Freiheiten natürlicher Personen besteht.

Es gibt verschiedene Möglichkeiten Daten durch Verschlüsselung vor unberechtigter Offenlegung/Kenntnisnahme zu schützen, z. B. durch Hardware-Verschlüsselung bei Festplatten, verschlüsselte USB-Sticks oder mit Hilfe von Software.

Im TB für die Jahre 2020 unter Punkt 7.2 und 2021 unter Punkt 7.5.1 haben wir Möglichkeiten der Verschlüsselung aufgezeigt. Bei der Auswahl der Verschlüsselung ist entscheidend welches Medium (z. B. E-Mail, Festplatte etc.) und welche Bereiche (kompletter Datenträger oder für Teilbereiche) zu schützen sind.

Nicht zu vernachlässigen ist, wie und wo die Daten und ggf. erforderliche Sicherheits-Schlüssel zusätzlich gesichert (Backup/Recovery) werden sollen.

Bei den aktuell zur Verfügung stehenden Möglichkeiten und technischen Mitteln, kann es keine plausible Ausrede geben, weshalb sicherheitsrelevante, wie auch personenbezogen Daten, beim Datentransport nicht verschlüsselt werden (z.B. Datentransport im Rahmen von Home-Office, Notebook, etc.)!

7.6.3 Einfach und wirkungsvoll mit Windowsmitteln

Anwender haben mit Windows 10 ab der Version Professional bereits ein Programm namens „Bitlocker[41]“ und z.B. „BitLocker To Go“ zur Verschlüsselung lokaler und externer Datenträger an Bord und benötigen keine zusätzlichen Hilfsmittel.

Schritt für Schritt zum verschlüsselten USB-Stick

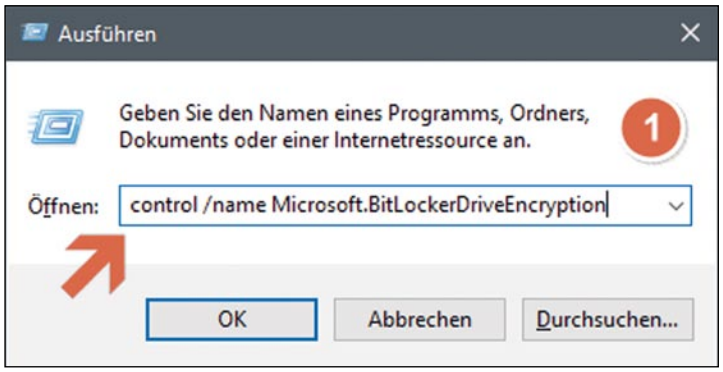
Als erstes verbindet man einen Datenträger, der nur noch verschlüsselte Daten enthalten soll, mit dem USB-Anschluss des Computers. Das kann ein USB-Stick sein oder aber auch eine externe Festplatte. In einem nächsten Schritt kann der Windows-BitLocker, der sich unterschiedlich starten lässt (je nach Windows-Kenntnisse), gestartet werden.

Windows-Taste gedrückt halten und dann das „r“ betätigen (Befehl: Ausführen), es erscheint der „Ausführen“

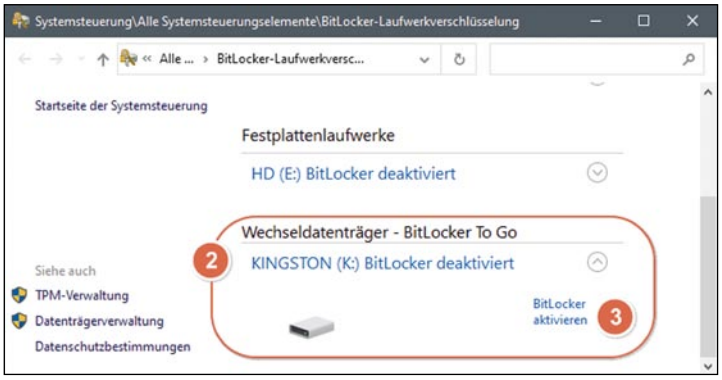
41 https://learn.microsoft.com/de-de/windows/security/information-protection/bitlocker/bitlocker-overview

Dialog. Hier kopieren Sie den folgenden Befehl in das „Öffnen" Eingabefeld und bestätigen mit Enter **[1].**

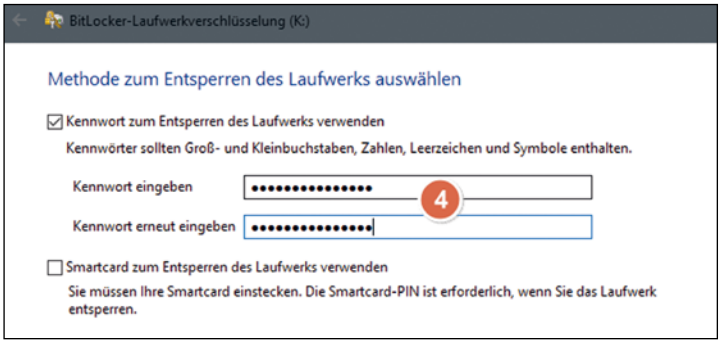
control /name Microsoft.BitLockerDriveEncryption



Eine weitere Möglichkeit besteht über die Windows-Einstellungen. Dort trägt man einfach „Bitlocker" in das Feld „Einstellung suche" ein **[1]**.

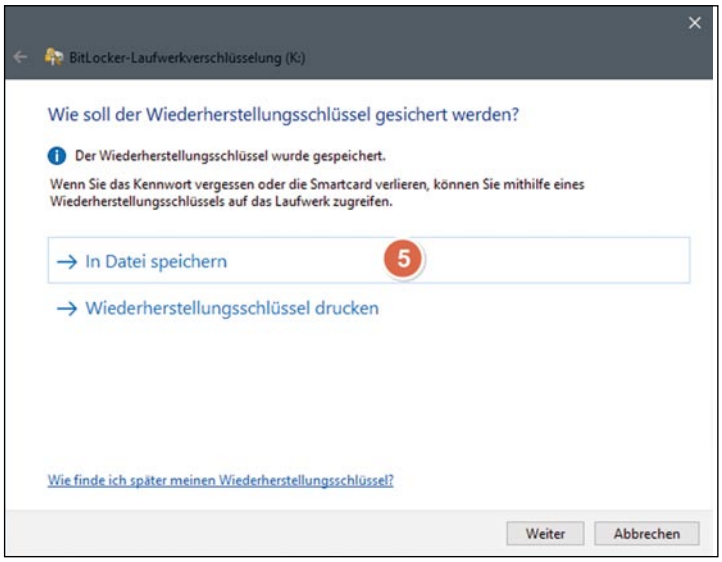


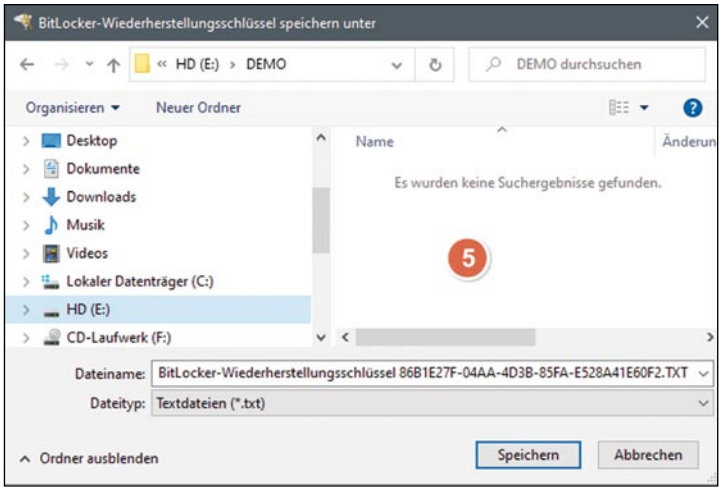
Sobald das Programm gestartet ist, wählt man den entsprechenden Datenträger zur Verschlüsselung aus. Am Beispiel wäre es das Laufwerk K **[2]** und bestätigt BitLocker aktivieren **[3]**.



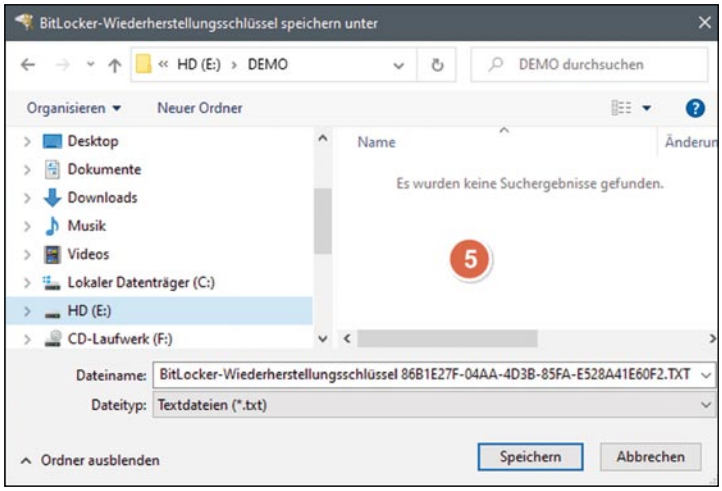
Im nächsten Dialog müssen wir ein Kennwort eintragen **[4]**. Immer wenn wir den Datenträger an einen PC anschließen und verwenden möchten, müssen wir mit Hilfe des hier hinterlegten Kennworts, das verschlüsselte Laufwerk öffnen.

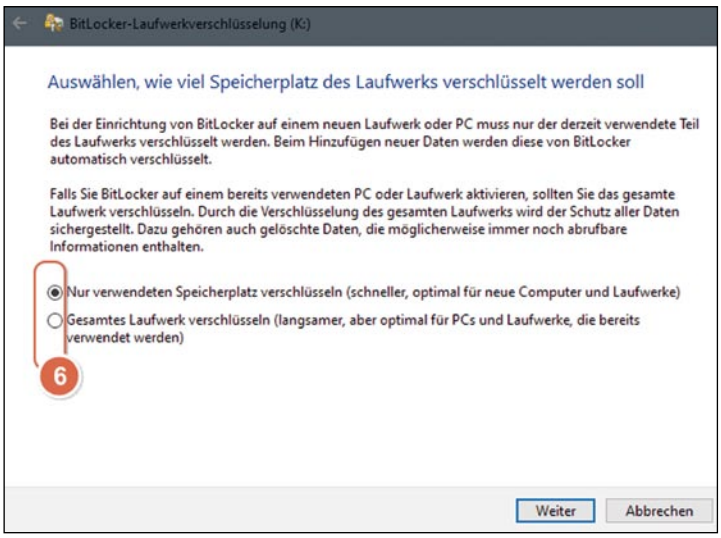
Der nächste Dialog erfordert die Angabe, wo der Wiederherstellungsschlüssel gespeichert werden sollte **[5]**. Mit diesem Schlüssel kann man im Bedarfsfall auf die Daten zugreifen. Aus diesem Grund sollten solche Sicherheits-Schlüssel zusätzlich an einem dafür eingerichteten zentralen und sicheren Ort gesichert werden (wie oben erwähnt). Zusätzlich ist ein Ausdruck möglich. Die Optionen zur Sicherung und zum Kennwortändern können auch später wiederholt durchgeführt werden, allerdings nur wenn das Medium entsperrt (geöffnet) ist.

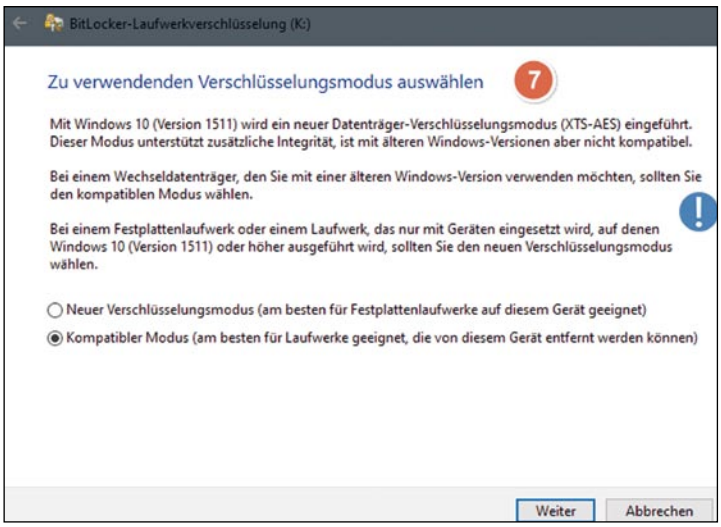


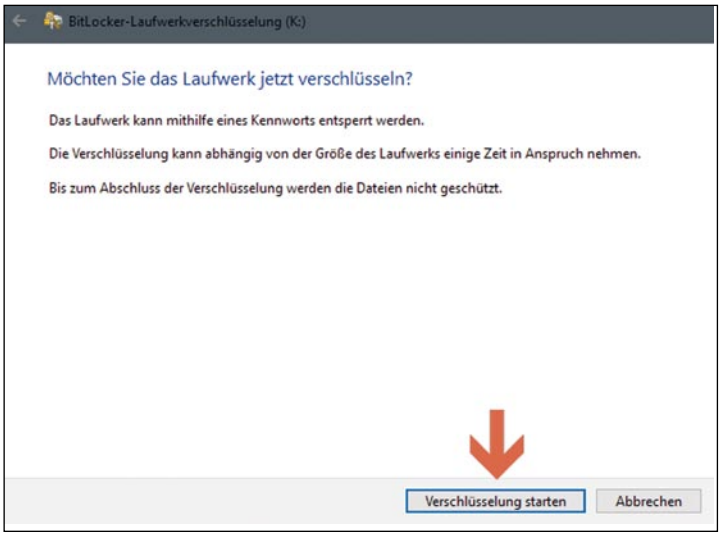


Bevor das Laufwerk endgültig verschlüsselt wird, stehen zwei Optionen zu Auswahl.









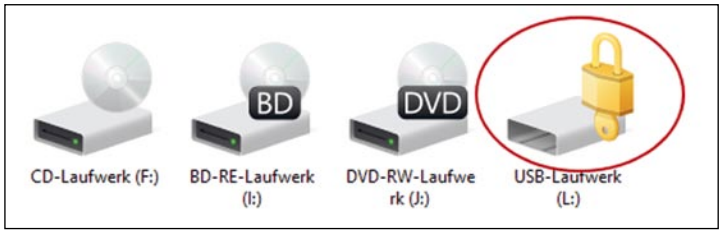
Falls es sich um einen bereits gebrauchten Datenträger handelt, sollte man sich für die zweite Option (Gesamtes Laufwerk) entscheiden, auch wenn der Vorgang länger dauert. So ist man auf jeden Fall auf der sicheren Seite **[6]**.

Tipp: Option „Gesamtes Laufwerk“ wählen, auch wenn diese Option mehr Zeit in Anspruch nimmt, ist man damit auf der sichersten Seite.
Jetzt nur noch den Verschlüsselungsmodus wählen **[7]** und die Verschlüsselung kann endgültig gestartet werden.

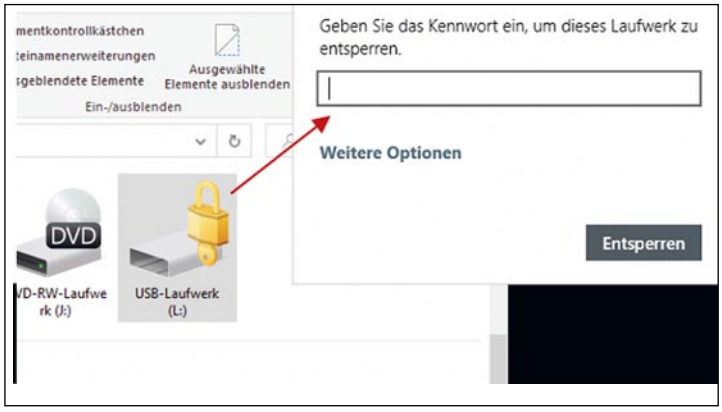
Je nach Größe des Datenträgers benötigt der Vorgang eine gewisse Zeit, die nicht unterbrochen werden sollte.

Bitte beachten! Falls sich wichtige Daten vor einer Verschlüsselung auf dem Datenträger befinden, sollte unbedingt eine Sicherheitskopie erstellt werden, denn leider kann auch beim Verschlüsselungsvorgang etwas schief gehen oder aber der Strom fällt während der Laufzeit aus.

Nachdem das Laufwerk erfolgreich verschlüsselt wurde, steht es zur Verfügung. Zum Test kann das Laufwerk vom USB-Anschluss entfernt und erneut angesteckt werden.



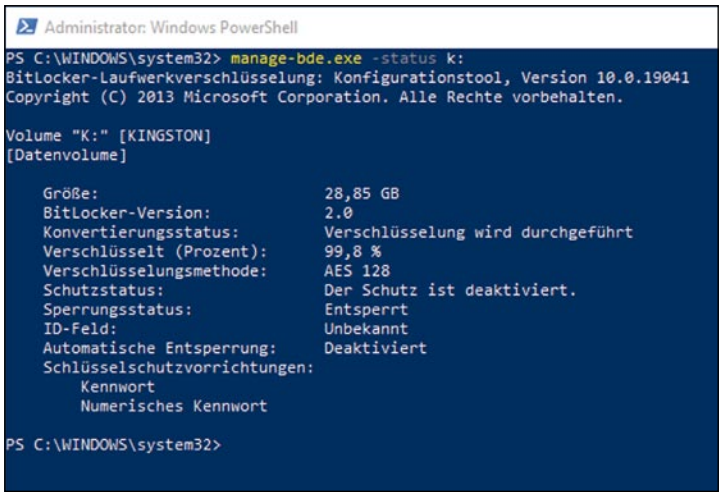
In der Laufwerk-Übersicht erscheint das verschlüsselte Laufwerk mit einem Schloss gekennzeichnet und kann mit dem entsprechenden Kennwort zur Verwendung entsperrt/geöffnet werden.



Hinweis für Fortgeschrittene und Administratoren

Mit der Windows-PowerShell kann der Status und die Verschlüsselungsmethode angezeigt und u.a. zur Dokumentation verwendet werden

PowerShell als Administrator ausführen,
Befehl:
manage-bde.exe -status k:

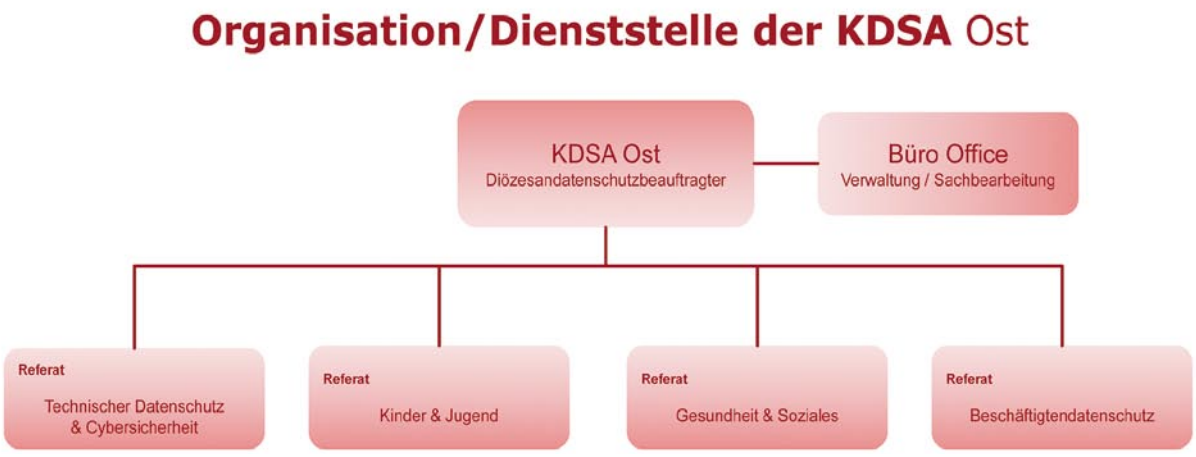


Die Kirchliche Datenschutzaufsicht Ost

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.

Öffentlichkeitsarbeit

Die Aufklärung und Sensibilisierung zum Schutz persönlicher Daten ist eine wichtige Aufgabe, damit frühzeitig erkannt wird, um was es beim Datenschutz geht. Durch die zunehmende Digitalisierung steigt die Gefahr der Verschmelzung von personenbezogenen Daten mit betrieblichen Daten bis hin zur Untrennbarkeit. Lösch- oder Änderungsbegehren hinsichtlich einzelner persönlicher Daten wird damit erschwert und die Gefahr, das persönliche Daten an unbefugte Dritte gelangen, steigt. Das ist z.B. bei den sich häufenden Cyber-Attacken der Fall, bei denen Daten an die Öffentlichkeit geraten, die genau genommen nach den geltenden Datenschutzbestimmungen (sobald der Zweck der Verarbeitung und ggf. die Aufbewahrungsfristen entfallen sind) nicht vorhanden sein dürften.

Um verstärkt Akzeptanz auf den Datenschutz im rechtlichen Sinne zu schaffen, führen wir zusätzlich zu aktuellen Themen auf unserer Website unter www.kdsa-ost.de öffentlichen Video-Sprechstunden und gemeinsame Diskussionsrunden zu Fragen rund um das Thema Datenschutz und Informationssicherheit durch.

Ein weiteres erfolgreich angenommen Angebot sind unsere fach- und anlassbezogenen Online-Veranstaltungen.

Mit unserem jährlichen Tätigkeitsbericht, den wir als Druckausgabe und Online bereitstellen, tragen wir u.a. dazu bei, dass Datenschutz und Informationsfreiheit im täglichen Leben und der damit verbundenen digitalen Welt Beachtung finden.

Anhang

Microsoft Versionsinformationen

Microsoft Windows 10 und Exchange (Stand der Technik)

Windows 10 – Lebenszyklus und Supportende

Version	Latest revision date	Latest Build	End of servicing: Home, Pro, Pro Education and Pro for Workstations	End of servicing: Enterprise, Education and IoT Enterprise
22H2	2023-02-21	19045.2673	2024-05-14	2025-05-13
21H2	2023-02-21	19044.2673	2023-06-13	2024-06-11
20H2	2023-02-21	19042.2673	End of servicing	2023-05-09

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

Exchange Server – Buildnummern (Stand der Technik 2022)

Exchange Server 2019 CU12 Nov22SU 8. November 2022
15.2.1118.20 15.02.1118.020

Exchange Server 2016 CU23 Nov22SU 8. November 2022
15.1.2507.16 15.01.2507.016

Exchange Server 2013 CU23 Nov22SU 8. November 2022

15.0.1497.44 15.00.1497.044

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

Abkürzungen

AG	Amtsgericht
ArbG	Arbeitsgericht
ArbZG	Arbeitszeitgesetz
AU	Arbeitsunfähigkeit
AVR	Richtlinien für Arbeitsverträge in den Einrichtungen des Deutschen Caritasverbandes
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationssicherheit
BGB	Bürgerliches Gesetzbuch
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit und Information
BT.-Drs	Bundestag-Drucksache
BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
DDSB	Diözesandatenschutzbeauftragten
DSK	Datenschutzkonferenz
DS-GVO	Datenschutz-Grundverordnung
DVG	Digitale-Versorgung-Gesetz
DVO	Kirchliche Dienstvertragsordnung
eGK	elektronische Gesundheitskarte
ePA	elektronische Patientenakte
EU	Europäische Union

EuGH	Europäischer Gerichtshof
GG	Grundgesetz
GrCH	Grundrechtecharta
HTML	Hypertext Markup Language (Auszeichnungs-sprache für Webseiten)
http	Hypertext Transfer Protokoll (unverschlüsselt)
https	Hypertext Transfer Protokoll Secure (verschlüsselt)
HK-SozDatenschutzR	Handkommentar Sozialdatenschutzrecht
IDSG	Interdiözesane Datenschutzgericht
IfSG	Infektionsschutzgesetz
LAG	Landesarbeitsgericht
LG	Landgericht
LPK	Lehr- und Praxiskommentar
KDG	Kirchliches Datenschutzgesetz
KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
KKG	Gesetzes zur Kooperation und Information im Kinderschutz
KODA NW	Kommission zur Ordnung diözesanen Arbeitsvertrags-rechts der (Erz-) Bistümer in Nordrhein-Westfalen
MAV	Mitarbeitervertretung
NJW	Neue Juristische Wochenzeitung
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PDSG	Patientendaten-Schutz-Gesetz
PStG	Personenstandsgesetz

RiLi	Richtlinie
RFID	radio-frequency identification
SGB	Sozialgesetzbuch
SMTP	E-Mail-Übertragungsprotokoll
SSL	Secure Socket Layer (TLS)
StGB	Strafgesetzbuch
TLS	Transport Layer Security
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
VDD	Verbandes der Diözesen Deutschlands
VPN	Virtual Private Network
VG	Verwaltungsgericht
VwVfG	Verwaltungsverfahrensgesetz

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