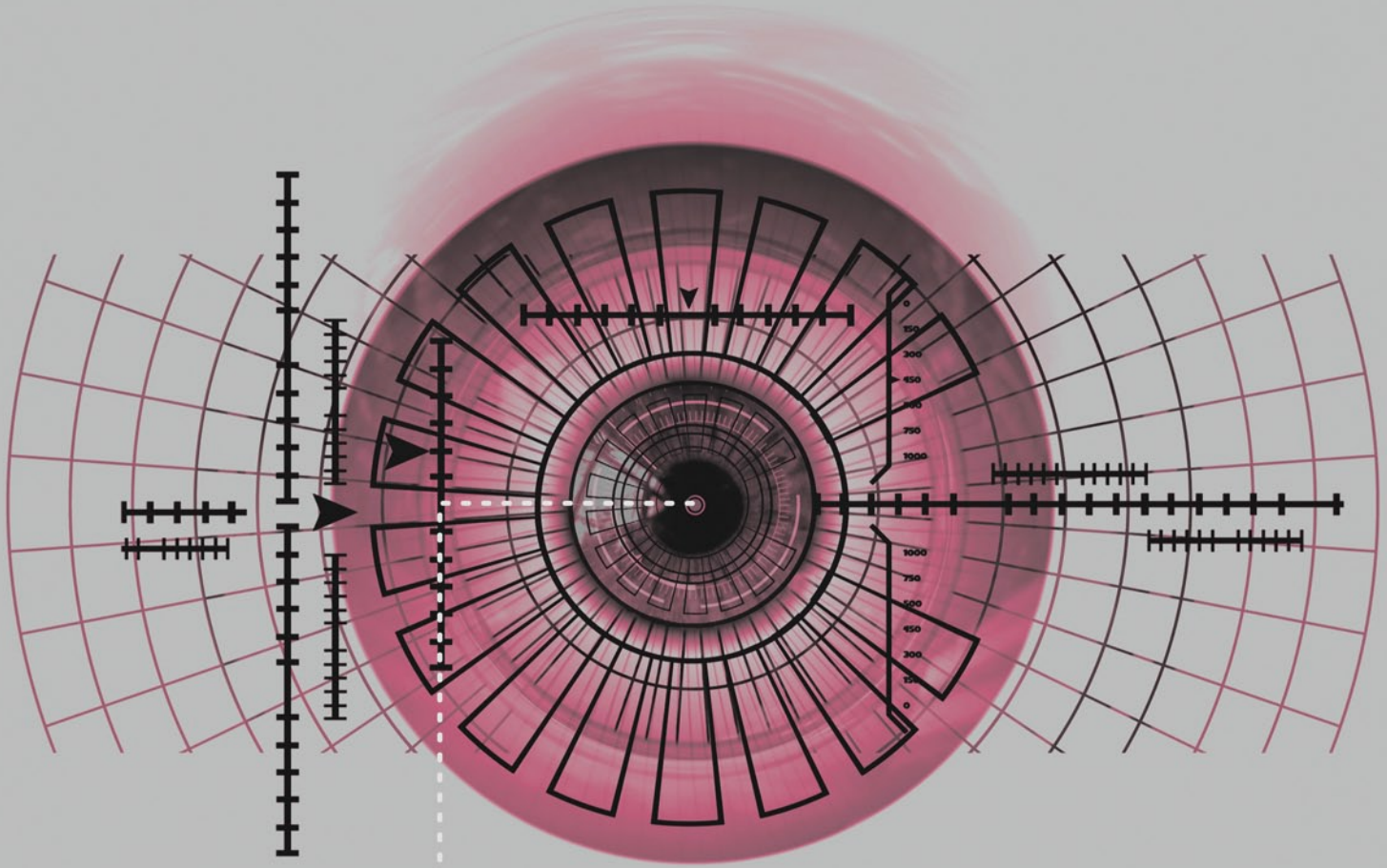


Tätigkeitsbericht 2020

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

„Ein observierter Mensch ist nicht frei"

Juli Zeh

5. Tätigkeitsbericht des Diözesandatenschutzbeauftragten

für

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

Berichtszeitraum 01.01.2020 bis 31.12.2020

Inhaltsverzeichnis

Vorwort

Jede Einrichtung oder Dienststelle die gehalten ist, einen Bericht über das letzte Jahr zu verfassen, wird auf die besonderen Umstände, die durch die Corona-Pandemie bedingt waren, hinzuweisen. Auch die Arbeit unserer Dienststelle war maßgeblich von dieser Situation geprägt.

Die Pandemie, ihr Ausmaß und die Folgen waren für alle Beteiligten neu. Die damit verbundenen Herausforderungen haben allen Verantwortlichen hohe Belastungen auferlegt.

Jedoch sind Grundsätze gerade in Krisen wichtige Eckpfeiler an denen sich Problemlösungen orientieren können. Wer in solchen Situationen diese Stützen ignoriert, wird nach einer Pandemieeindämmung ein anderes System vorfinden.

Datenschutz schützt das Persönlichkeitsrecht. Das Bundesverfassungsgericht hat ein Recht auf informationelle Selbstbestimmung als Grundrecht, welches sich aus den Artikeln 1 und 2 des Grundgesetzes ergibt, anerkannt. Insoweit ist es einmal mehr erschreckend, wie schnell Regierung und Politiker bereit sind, Grundrechte für reine Praktikabilitätserwägungen zu opfern.

Zum Teil gibt man sich gar nicht erst die Mühe darzustellen, dass Datenschutz ein Grundrecht ist, sondern stellt dieses als Luxus dar, den man sich in Krisensituationen nicht leisten kann. Der Öffentlichkeit wird unterdessen erklärt es handele sich um die Abwägung zwischen Datenschutz und Volksgesundheit.

Hier wird an eine Tradition angeknüpft, die aus der Terrorbekämpfung bereits hinlänglich bekannt ist. Es wird ein Problem aufgezeigt, dessen einzige Lösung vermeintlich in der Einschränkung des grundgesetzlich garantierten Datenschutzes besteht. Unabhängig davon, dass sich solche Einschränkungen häufig als überflüssig bzw. nicht nützlich erweisen oder sich zumindest durch eine Änderung der äußeren Umstände inzwischen überholt haben, bleiben die Einschränkungen bestehen.

Belastbare Gründe, warum der Datenschutz die Pandemiebekämpfung angeblich behindert, sind zu keiner Zeit vorgetragen worden. Im Gegenteil, Bürger*innen sind immer bereit Einrichtungen, denen sie vertrauen, perso-

nenbezogene Daten zu offenbaren. So genießen Ärzte und Krankenkassen das Vertrauen von 87 % der Bürger*innen. Das Vertrauen in staatliche Institutionen ist mit 71 % demgegenüber deutlich geringer.[1]

Wenn staatliche Stellen personenbezogene Daten, die im Zusammenhang mit der Pandemiebekämpfung erhoben worden sind zweckwidrig weitergeben, ist darin ein Datenschutzverstoß zu sehen. Vor allem aber sinkt das Vertrauen der Bürger*innen. Ohne dieses Vertrauen aber ist eine effiziente Pandemiebekämpfung nicht möglich. Es ist nicht erforderlich datenschutzrechtliche Regelungen aufzugeben, sondern bestehenden Datenschutzgesetze einzuhalten.

Es erscheint wichtig, Datenschutz den Menschen näher zu bringen. Die Verantwortungsträger müssen dafür deutlich machen, dass Datenschutz ein Grundrecht jedes Einzelnen ist und nicht in erster Linie ein lästiges Hindernis bei der Durchsetzung von Interessen gleich welcher Art.

Wer in einer zunehmend digitalisierten Welt Datenschutz immer weiter reduzieren will, will Grundrechte einschränken und wird das Vertrauen der Bürger*innen verlieren und damit zu einer Destabilisierung des Gemeinwesens beitragen.

1 Postbank Digitalstudie 2020

1 Entwicklung des Datenschutzes

1.1 Entwicklung des Datenschutzes in der Bundesrepublik

1.1.1 Datenschutz gerät in Pandemiezeiten durch staatliche Stellen unter Druck

Die Entwicklung des Datenschutzes war zunächst geprägt von der Pandemiebekämpfung. Zur Eindämmung der Pandemie war und ist es sinnvoll, auch IT-Lösungen dafür zu suchen.

Mit der Entwicklung und Einführung der Corona-Warn-App ist es gelungen, ein System an den Start zu bringen, welches den Datenschutz gewährleistet. Das Herunterladen und das Nutzen der App ist freiwillig und die gesammelten Daten werden dezentral auf den einzelnen Smartphones gespeichert. Die Corona-Warn-App wurde in Deutschland mehr als 25 Millionen Mal heruntergeladen und hat nur deshalb eine so hohe Akzeptanz in der Bevölkerung gefunden, weil die Menschen sich darauf verlassen können, dass ihre Daten nicht zu unvorhersehbaren Zwecken missbraucht werden. Zudem kann sie datenschutzgerecht fortentwickelt werden.

Nachteilig ist bislang, dass die Eigentümer von Android-Geräten gezwungen sind, die Standortfunktion freizugeben. Mit dieser Freigabe können alle anderen Apps, die auf dem Gerät installiert -meistens vorinstalliert- sind, ebenfalls auf die Standortdaten des Nutzers zugreifen. Zwar weist die Corona-Warn-App bei ihrer Installation auf diesen Umstand hin, eröffnet aber keine andere Möglichkeit.

Wenn Nutzer der App positiv auf das Coronavirus getestet worden sind, müssen sie diese Tatsache selber in die App eintragen. Nur dann kann die App ihren Zweck erfüllen, die anderen Nutzer über einen Kontakt mit positiv getesteten zu informieren und diese dadurch anzuregen, sich ebenfalls einem Test zu unterziehen. Bislang geben aber nur 60 % der teilnehmenden Nutzer selber ein positives Testergebnis ein.[2]

2 https://www.spiegel.de/netzwelt/netzpolitik/corona-warn-app-weniger-datenschutz-hilft-auch-nicht-gegen-covid-19-

Fraglich ist, inwieweit dieses unbefriedigende Ergebnis eine Folge staatlichen Handelns ist. Obwohl die Stigmatisierung von Infizierten ein weltweites Problem darstellt,[3] verletzten staatliche Behörden datenschutzrechtliche Vorschriften und tragen so zu einer Stigmatisierung bei. So wurden in einigen Bundesländern[4] die Gesundheitsämter angewiesen, die unter Quarantäne stehenden Personen an die Polizei zu melden. In einigen Landkreisen[5] wurden die Namen infizierter Personen auch an Feuerwehren und Rettungsdienste weitergegeben. Für eine solche Datenverarbeitung fehlt jede Rechtsgrundlage. Wenn Folge einer freiwilligen Mitteilung gesellschaftliche Stigmatisierung ist, wird Systemen wie der Corona-Warn-App mittelfristig kein Erfolg beschieden sein.

Der zunehmende Druck staatlicher Stellen auf den Datenschutz wird dazu führen, dass sich noch mehr Menschen dem System entziehen. Wenn dann der Datenschutz weiter eingeschränkt wird, führt dies in eine Abwärtsspirale.

Ein Beispiel für diese Entwicklung sind die Listen, die Restaurants und andere Veranstalter führen müssen/mussten, um die Kontaktdaten ihrer Kunden zu erheben. Dies soll dem Zweck der behördlichen Nachverfolgbarkeit von Infektionsketten dienen.

Die personenbezogenen Daten, die jemand beim Gaststättenaufenthalt angegeben hat, geben in der Regel Aufschluss über seine Freizeitgestaltung. An Orten der Kommunikation, des Austauschs und der Freizeitgestaltung ist die Privatsphäre im Rahmen des Rechts auf informationelle Selbstbestimmung besonders schutzwürdig. Vielfach stellte sich heraus, dass das Vertrauen in dieses Verfahren bei den betroffenen Bürgern gering ist. So konnten erforderliche Nachverfolgungen nicht durchgeführt werden, weil die Betroffenen falsche Kontaktdaten oder Phantasienamen angegeben haben. Der an sich sinnvolle Zweck der Pandemiebekämpfung konnte deshalb nicht erreicht werden.

Allerdings haben auch hier staatliche Stellen dazu beigetragen, das Misstrauen der Bürger zu schüren. Wiederholt wurden durch die Polizei zum

3 https://unicef.at/fileadmin/media/Infos_und_Medien/Info-Material/Ernaehrung_und_Gesundheit/Soziale-Stigmatisierung-Coronavirus.pdf
4 Belegt für Sachsen-Anhalt, Niedersachsen, Mecklenburg-Vorpommern
5 z.B. Salzlandkreis / Sachsen-Anhalt

Zweck der Verfolgung von Straftaten die Listen verwendet, die einen anderen Zweck erfüllen sollten.

1.1.2 EuGH kippt Privacy Shield Abkommen

Die §§ 40 und 41 KDG (Art. 44 ff. DS-GVO) regeln unter welchen Voraussetzungen eine Datenübermittlung in ein Drittland außerhalb der Europäischen Union zulässig ist. Zwischen den USA und der Europäischen Union war eine Übermittlung zunächst auf der Grundlage des Safe-Harbour Abkommens möglich. Dieses Abkommen wurde vom Europäischen Gerichtshof (EuGH)[6] für nicht vereinbar mit den europäischen Datenschutzstandards erklärt. In der Folgezeit wurde mit dem Privacy Shield Abkommen eine neue Rechtsgrundlage für einen Datenaustausch zwischen Europa und den USA geschaffen.

Am 16.07.2020 hat der EuGH in einem weiteren Urteil[7] entschieden, dass auch das Privacy Shield Abkommen nicht dem Schutzniveau entspricht, welches dem in der Union durch die DS-GVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist.

Die Datenschutzaufsichten sind nach dem Urteil des EuGH verpflichtet, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie im Licht der Umstände dieser Übermittlung der Auffassung sind, dass die Standarddatenschutzklauseln in diesem Land nicht eingehalten werden oder nicht eingehalten werden können. Eine Übertragung von personenbezogenen Daten in ein Drittland allein mit dem Hinweis auf das Privacy Shield Abkommen ist deshalb unzulässig.

Verantwortliche sollten also alle Datenempfänger, die ihren Sitz in den USA haben, daraufhin überprüfen, ob diese geeignete Garantien i. S. d. §§ 40, 41 KDG haben. Unternehmen, die den Datentransfer bislang ausschließlich auf das Privacy Shield Abkommen stützten, sind auszuschließen. Da kirchliche Einrichtungen selten in der Lage sein werden, mit Datenempfängern im Drittland kurzfristig die passenden Standarddatenschutzklauseln abzuschließen, werden sich die Einrichtungen perspektivisch von diesen Dien-

6 EuGH Urteil vom 06.10.2015 - C-362/14
7 EuGH Urteil vom 16.07.2020 - C-311/18

sten trennen müssen. Eine Übergangsfrist legt der EuGH in seinem Urteil nicht fest.

1.1.3 Neue Privilegien für Geimpfte? - aus datenschutzrechtlicher Sicht

In der Öffentlichkeit ist eine Diskussion darüber entbrannt, ob es für Personen, die gegen Covid-19 geimpft wurden, Lockerungen von den Corona-Beschränkungen geben sollte. Der Ethikrat der Bundesrepublik hat dazu eine Entscheidung getroffen, in der er sich zur derzeitigen Situation gegen eine Privilegierung Geimpfter ausspricht.

Der entscheidende Punkt in der Diskussion ist die Frage, ob es sich um Privilegien handelt oder um das Recht, Grundrechte wieder ausüben zu dürfen. Durch die Corona Verordnungen werden die Menschen vielfältig in der Ausübung ihrer Grundrechte eingeschränkt. Kontaktverbote, Einschränkung des Bewegungsradius und die Pflicht zum Tragen einer Mund-Nasen-Bedeckung schränken die persönliche, grundgesetzlich gewährte Freiheit ein. Im Vordergrund der Diskussion stehen aber nicht diese Einschränkungen, sondern es wird darüber diskutiert, ob Geimpfte das Recht haben sollen, Restaurants, Clubs, Kinos, Konzerte und andere Kulturveranstaltungen wieder besuchen zu können.

Ein Grundrecht auf Besuch eines Restaurants oder eines Konzertes gibt es nicht.

Das Grundrecht aus Artikel 2 Grundgesetz gewährt das Recht auf freie Entfaltung der Persönlichkeit. Dieses Recht besteht aber nur im Rahmen der tatsächlichen Möglichkeiten. Die Corona Verordnungen verbieten niemandem Restaurants oder Konzerte zu besuchen. Die Möglichkeit dies zu tun besteht aber nicht, weil diese Einrichtungen aufgrund der Corona Verordnungen geschlossen sind. Adressat der Grundrechtseinschränkungen sind also nicht alle Bürger*innen, sondern die Gewerbetreibenden, die ihre Leistungen derzeit nicht anbieten dürfen. Ein Recht des Einzelnen gegen den Staat auf Öffnung bestimmter Einrichtungen gibt es nicht und schon gar nicht leitet sich ein solcher Anspruch aus dem Grundgesetz ab. Hier muss also zunächst deutlich differenziert werden, welche Corona Beschrän-

kungen für Geimpfte aufgehoben werden müssen, um ihnen ihre volle Grundrechtsausübung wieder zu ermöglichen.

Im Wesentlichen einheitlich ist die Bewertung, eine Diskussion darüber sei solange überflüssig, wie nicht geklärt sei, ob Geimpfte nicht weiterhin Überträger des Virus sein können. Wenn auch Geimpfte noch Überträger des Virus sein können, verbietet sich eine Abfrage des Impfstatus, weil mit einer solchen Frage ein rechtlich billigenswerter Zweck nicht verfolgt werden kann. Wenn Geimpfte und Ungeimpfte in gleicher Weise ansteckend sein können, hilft die Information über den Impfstatus nichts.

Abgesehen davon, dass die Diskussion derzeit also verfrüht ist, ist ein Ausblick auf die Zeit nach einer entsprechenden Klärung geboten. Bei allen weiteren Überlegungen wird hier immer vorausgesetzt, dass wissenschaftlich erwiesen ist, dass eine Verbreitung des Virus durch Ansteckung bei Geimpften nicht erfolgen kann.

Auch unter dieser Annahme ist zu unterscheiden:

Darf es eine unterschiedliche Behandlung in der Zeit geben, in der noch nicht genug Impfstoff für alle Impfwilligen vorhanden ist?

Darf es staatlich vorgeschrieben werden, dass Gaststätten- und Kulturbetriebe im Rahmen eines Hygienekonzeptes nur solche Kunden einlassen, die über eine Impfung verfügen?

Aus datenschutzrechtlicher Sicht ist dazu zunächst folgendes festzustellen:

Die Frage nach dem Impfstatus ist ein personenbezogenes Datum gem. Art. 4 Nr. 1 DS-GVO. Weil mit der Abfrage nach dem Impfstatus Informationen über den Gesundheitsstatus verbunden sind, handelt es sich auch um ein Gesundheitsdatum gem. Art. 4 Nr. 15 DS-GVO. Somit ist mit der Abfrage ein personenbezogenes Datum besonderer Kategorie gem. Art. 9 Abs. 1 DS-GVO betroffen. Die Verarbeitung solcher Daten ist gem. Art. 9 Abs. 1 DS-GVO untersagt.

Eine Ausnahme davon lässt die DS-GVO nur dann zu, wenn einer der Ausnahmetatbestände des Art. 9 Abs. 2 DS-GVO gegeben ist.

Während der Ethikrat das Befolgen von Regelungen wie Maske-Tragen oder Abstand-Halten auch für Geimpften für zumutbar hält, gibt es für Andere[8] verfassungsrechtlich keine Legitimation mehr, die Betroffenen in ihren Grundrechten weiter zu beschränken. Hier ist der letzteren Ansicht der Vorzug zu geben. Denn ein sicherer Eingriff in die Grundrechte Einzelner kann nicht damit begründet werden, dass andernfalls vermutlich die allgemeine Akzeptanz der Maßnahmen zu sinken droht (so aber der Ethikrat).

Nach derzeitigem Kenntnisstand geht von dem Virus zumindest solange eine Gefahr für die Volksgesundheit aus, wie eine Herdenimmunität durch eine Impfung noch nicht erreicht ist. Bis dieser Zustand erreicht ist, stellen Ungeimpfte ein potentielles Risiko zumindest für andere Ungeimpfte dar. Weiterhin wird dadurch das staatliche Gesundheitssystem gefährdet, wenn sich Ungeimpfte unkontrolliert anstecken, erkranken und in Krankenhäusern behandelt werden müssen.

Der funktionsfähige Erhalt des Gesundheitssystems stellt ein erhebliches öffentliches Interesse i. S. v. Art. 9 Abs. 2 lit. g) DS-GVO dar, welches es rechtfertigt solche Daten zu verarbeiten, um die Allgemeinheit zu schützen.

Wenn es aber Menschen gibt, von denen im Hinblick auf die Übertragung des Virus keine Gefahr ausgeht, besteht kein Grund, Gewerbetreibenden zu verbieten, solche Personen zu bedienen.

Die Gewerbetreibenden müssten dann aber die Sicherheit haben, dass durch ihre Kunden sie selbst und ihr Personal nicht gefährdet werden. Dies ist nur zu erreichen, indem man den Impfstatus erfragt bzw. sich bestätigen lässt. Die Verpflichtung des Arbeitgebers, Arbeitnehmern einen gefährdungsfreien Arbeitsplatz zur Verfügung zu stellen, ergibt sich aus dem Arbeitsschutzgesetz (§ 3 ArbSchG). Die Frage nach dem Impfstatus wäre also zulässig, mit der Folge, dass Ungeimpften der Zutritt oder die Teilnahme verboten werden könnte. Das dies von weiten Teilen der ungeimpften Bevölkerung als ungerecht empfunden werden wird, weil diese schlicht keine Möglichkeit hatten sich impfen zu lassen und ihnen deshalb die volle Teilhabe am öffentlichen Leben vorenthalten wird, ist eine von der Politik zu klärende Frage, die keinen Einfluss auf die rechtliche Bewertung hat.

8 Rupert Scholz und Alexander Ehlers. https://www.aerztezeitung.de/Politik/Diskussion-um-Privilegien-fuer-Geimpfte-415960.html vom 30.12.2020

Die Öffnung von Gaststätten- und Kulturbetrieben unter der Auflage den Impfstatus der Kunden zu verarbeiten ist also zweckmäßig.

Gleichwohl kann der Verordnungsgeber von einer solchen Auflage als Voraussetzung für eine Öffnung absehen. Dies kann politische Gründe haben oder nach einer Abwägung verschiedener Rechtsgüter erfolgen.

In diesem Fall darf es aber dem Gewerbetreibenden nicht verwehrt werden zum Schutz seines Personals und seiner selbst die Vorlage des Impfausweises zur Bedingung für die Inanspruchnahme seiner Dienste zu machen, weil er nur so sicherstellen kann, eine ansonsten bestehende Gefährdung abzuwenden.

Anders ist aber zu entscheiden, wenn es für alle Impfwilligen ein Impfangebot gegeben hat und eine Herdenimmunität eingetreten ist.[9] In diesen Fällen ist davon auszugehen, dass die dann immer noch Ungeimpften eine Impfung aus persönlichen Gründen ablehnen und bereit sind, sich daraus möglicher Weise ergebende Konsequenzen zu tragen.

Wenn alle Bürger*innen die Möglichkeit hatten sich impfen zu lassen, trifft dies auch auf die Betreiber von Gaststätten und Kulturbetrieben und ihr Personal zu. Ein weiterer Schutz ist dann nicht mehr erforderlich. In einem solchen Fall ist kein rechtlich nachvollziehbarer Zweck gegeben, der die Frage nach einem Impfausweis rechtfertigen könnte. Wenn alle die es wollen durch Impfung geschützt sind, geht für sie von einem Ungeimpften keine Gefahr mehr aus. Staatliches Recht dürfte dann keine Rechtsgrundlage für eine Abfrage bieten. Wenn es für eine Datenverarbeitung keinen rechtlich anerkannten Zweck gibt, ist eine solche Datenverarbeitung nicht erforderlich und damit zunächst unzulässig.

Etwas anderes könnte dann gelten, wenn sich ein Recht zur Verarbeitung personenbezogener Daten besonderer Kategorie aus einer Einwilligung Betroffener ableiten ließe. Wesentliche Voraussetzung für eine Einwilligung ist aber ihre Freiwilligkeit. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss gem. Art. 7 Abs. 4 DS-GVO berücksichtigt werden, ob die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung von der Verarbeitung personenbezogener Daten abhängig gemacht wurde, die für

9 Die Feststellung eines solchen Zustandes müsste von einer staatlichen Stelle festgestellt werden

die Erfüllung des Vertrages nicht notwendig sind. Zur Leistungserbringung ist unter den dann gegebenen Umständen für die Betreiber von Gaststätten und Kulturbetrieben die Kenntnis des Impfstatus nicht erforderlich. Die Leistungserbringung kann in diesen Fällen keinen Zweck darstellen, für den die Erhebung von Gesundheitsdaten erforderlich ist. Somit wäre eine entsprechende Datenverarbeitung unzulässig. Eine trotzdem erfolgte Abfrage des Impfstatus würde unrechtmäßig in die Grundrechte der Betroffenen eingreifen.

Zusammenfassung:

1. Solange nicht geklärt ist, ob Geimpfte das Virus trotz der Impfung an Dritte weitergeben können, ist eine Diskussion um die Aufhebung von Beschränkungen, die auch für diese Personen gelten, verfrüht.

2. Wenn wissenschaftlich gesichert ist, dass eine Ansteckungsgefahr für Dritte von geimpften Personen nicht mehr ausgeht, jedoch eine Herdenimmunität noch nicht erreicht ist, weil eine Durchimpfung der Bevölkerung aufgrund unzureichender Impfmöglichkeiten noch nicht gegeben ist, erscheint es rechtlich geboten für Geimpfte die bestehenden Beschränkungen aufzuheben. In diesen Fällen darf die Erbringung von Dienstleistungen an den Nachweis einer Impfung geknüpft werden.

3. Wenn eine Durchimpfung der Bevölkerung stattgefunden hat und eine Herdenimmunität eingetreten ist, darf die Erbringung von Dienstleistungen oder der Abschluss von Verträgen nicht mehr vom Nachweis der Impfung abhängig gemacht werden.

1.1.4 Regelungen zur Bestandsdatenauskunft sind verfassungswidrig

Ein weiteres grundlegendes Urteil ist durch das Bundesverfassungsgericht (BVerfG) am 27.05.2020 ergangen.[10] Darin wird festgestellt, dass § 113 des Telekommunikationsgesetzes (TKG) die Inhaber von Telefon- und Internetanschlüssen in ihren Grundrechten auf informationelle Selbstbestimmung sowie auf Wahrung des Telekommunikationsgeheimnisses (Art. 10 Abs. 1 GG) verletzt. Die in der Vorschrift geregelte sog. „manuelle Bestandsdaten-

10 BVerfG Beschluss vom 27.05.2020 - 1BvR 1873/13; 1BvR 2618/13

auskunft" ermöglicht es Sicherheitsbehörden von Telekommunikationsunternehmen Auskunft insbesondere über den Anschlussinhaber eines Telefonanschlusses oder einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse zu erlangen. Diese Stammdaten bilden im Regelfall den Kern eines oder mehrerer Datensätze, da sie grundsätzliche Informationen über Einzelpersonen enthalten. Dazu gehören z. B. der Name oder die Adresse einer Person sowie weitere statische Daten, welche sich auf den konkreten Erhebungszweck beziehen.

Die Erteilung einer Auskunft über Bestandsdaten ist grundsätzlich verfassungsrechtlich zulässig. Übermittlungs- und Abrufregelungen müssen aber die Verwendungszwecke der Daten hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen. Der entscheidende Senat hat ausdrücklich wiederholend festgestellt, dass eine Auskunft über Zugangsdaten nur dann erteilt werden darf, wenn die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Unzulässig ist es demnach, unabhängig von solchen Zweckbestimmungen einen Datenvorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt.

Bereits in unserem 2. Tätigkeitsbericht[11] hatten wir auf die Gefahren hingewiesen, die von einer allgemeinen Vorratsdatenspeicherung für Einrichtungen von Kirche und Caritas ausgehen.

Das Bundesverfassungsgericht hat sich mit dieser Entscheidung einmal mehr klar für einen effektiven Datenschutz ausgesprochen und deutlich gemacht, dass durch diesen Persönlichkeitsrechte geschützt werden und deshalb Eingriffe besonderer gesetzgeberischer Sorgfalt bedürfen.

1.1.5 Registermodernisierungsgesetz

Unter dieser Bezeichnung plante die Bundesregierung die Einführung einer zentralen Personenkennziffer.

Schon bei der Einführung der Steuer-ID im Jahr 2007 hatte es Kritik gegeben, dass diese später als einheitliche Personenkennziffer genutzt werden

11 2.TB 2017, S. 11

könnte. Seinerzeit widersprach die Bundesregierung einer solchen Vermutung. Doch genau das soll jetzt geschehen. Die Steuer-ID soll als einheitliche Personenkennzahl zu nutzen sein.

Mit dem Gesetz würde es technisch möglich mehr als 50 unterschiedliche staatliche Datenbanken und Register miteinander zu verknüpfen. Dadurch kann man ein recht genaues Bild über die Lebensumstände eines Menschen erhalten. Durch Zusammenführung der Daten aus unterschiedlichen Registern, die durch die Verwendung einer einheitlichen Identifikationsnummer sehr viel einfacher wird, wächst das Risiko einer missbräuchlichen Verwertung. Damit würden viele Sicherheitsmaßnahmen obsolet.

Bereits 2019 hatte die Datenschutzkonferenz davor gewarnt, dass die Schaffung solcher einheitlichen und verwaltungsübergreifenden Personenkennziffer gefährlich sein könne. Personenbezogene Daten, die in großem Umfang vorliegen, können leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden. Auch das Bundesverfassungsgericht hatte wiederholt entschieden, dass eine universelle Personenkennziffer nicht mit dem Grundgesetz zu vereinbaren ist, weil die Gefahr zu groß sei, die von der damit verbundenen Möglichkeit der individuellen Verhaltensaufzeichnung und Profilbildung einhergehe.

Die Bundesregierung präferiert die Einführung der einheitlichen Personenkennziffer, da diese wesentliche Voraussetzung für die nutzerfreundliche Digitalisierung von Verwaltungsleistungen sei, damit Daten und Nachweise elektronisch übermittelt werden können. Das ist zunächst sicher richtig, jedoch bedarf es dazu einer einheitlichen Personenkennziffer nicht. Am Beispiel von Österreich ist zu sehen, wie eine Alternative aussehen kann, die datenschutzrechtlich weniger gefährlich ist. Dort wird seit Jahren ein System erfolgreich eingesetzt, bei dem einzelne Behörden so genannte „bereichsspezifische“ Nummern vergeben, während sie auf die eigentliche Personenkennziffer keinen Zugriff haben.

Der wissenschaftliche Dienst des Bundestages hat das Gesetz, mit dem die Einführung der einheitlichen Personalkennziffer umgesetzt werden soll, als zumindest verfassungsrechtlich problematisch eingestuft.[12] Die Daten-

12 WD 3 - 3000 - 196/20

schutzkonferenz hält es für verfassungswidrig.[13] Es ist also davon auszugehen, dass auch dieses Gesetz zumindest durch das Bundesverfassungsgericht geprüft wird.

Unabhängig dieser Einwendungen hat der Bundesrat dieses Gesetz in seiner Sitzung am 28.01.2021 beschlossen.

1.2 Entwicklung in den kirchlichen Einrichtungen

1.2.1 Patienten Datenschutzgesetz (PatDSG)

Im Gegensatz zu bislang teilweise bestehenden Ordnungen, die die Fragen des Patientendatenschutzes regelten, ist die neue Regelung ausdrücklich als Gesetz gestaltet worden. Es steht damit auf einer Stufe mit dem Kirchlichen Datenschutzgesetz (KDG) und ist eine besondere Rechtsvorschrift im Sinne von § 2 Abs. 2 KDG.

Die vollständige amtliche Bezeichnung des Gesetzes lautet: „Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens“. Aus dem Inhalt des Gesetzes geht der durch die Überschrift intendierte Zweck nur bedingt hervor.

Lt. Präambel des Gesetzes ist die Seelsorge so zu gestalten, dass das Persönlichkeitsrecht auf Schutz der Patientendaten gewahrt wird. Dass bei Seelsorge die Persönlichkeitsrechte zu beachten sind, sollte eine Selbstverständlichkeit sein, deren explizite Erwähnung in einem Gesetzestext nicht erforderlich ist. Die weite Begriffsdefinition von „Patientendaten“ in diesem Gesetz ist datenschutzrechtlich fraglich.

Wesentlicher Inhalt des Gesetzes ist es, Krankenhausseelsorge in drei Kategorien einzuteilen und diesen unterschiedliche Rechte zuzuweisen.

Zunächst ist nicht definiert und völlig offen, was mit einer „konzeptionell implementierten Seelsorge“ gemeint ist. Nach § 3 Abs. 1 PatDSG muss es lediglich „fundiert“ sein. Welchen Umfang das Konzept haben muss und welche Inhalte zwingend erforderlich sind, ist nicht festgelegt. Dafür wer-

13 DSK Entschließung vom 26.08.2020

den dem in diesem Rahmen tätigen Seelsorger erhebliche Rechte an der Verarbeitung personenbezogener Daten besonderer Kategorie eingeräumt.

Im Falle einer nicht konzeptionell implementierten Seelsorge dürfen einer mit Seelsorgeauftrag ausgestatteten Person auch ohne Einwilligung der Betroffenen personenbezogene Daten einschließlich Aufenthaltsort und Aufnahmedatum bekannt gegeben werden, wenn Betroffene ihre Religion/Konfession mitgeteilt haben. Die Mitteilung über die Zugehörigkeit zu einer Religion/Konfession bedeutet keine Einwilligung im Hinblick auf eine Seelsorge. Die im Gesetz an dieser Stelle vorgesehene Reglung, wonach eine Seelsorge zu unterbleiben hat, wenn der Patient dies ausdrücklich nicht wünscht, stellt eine mit dem Datenschutzrecht nicht vereinbare „Opt-Out-Regelung" dar. In Bezug auf die Verarbeitung personenbezogener Daten muss niemand erklären, dass und warum er etwas nicht will, sondern es bedarf immer einer freiwilligen und informierten Einwilligung für die Verarbeitung personenbezogener Daten.

Der Gesetzgeber scheint dies gesehen zu haben, da für die Seelsorge durch die Kirchengemeinde eine solche Regelung vorgesehen ist. Es ist nicht nachvollziehbar, warum es eine unterschiedliche Behandlung der in § 4 und § 5 PatDSG genannten Fälle geben soll.

Im Rahmen des Gesetzgebungsverfahrens haben sich die Datenschutzaufsichten wiederholt kritisch zu diesem Gesetz geäußert.

1.2.2 Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG)

Zum Jahresende ist von der Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) auch das datenschutzbezogene Verwaltungsverfahrensgesetz beschlossen worden. Die Verabschiedung eines solchen Gesetzes war notwendig geworden, da die Datenschutzaufsichten durch das Kirchliche Datenschutzgesetz (KDG) berechtigt sind, regelnd in die Verarbeitung personenbezogener Daten durch kirchliche Stellen einzugreifen. Für diese Form der Tätigkeit bietet das kanonische Recht keine hinreichende formelle Rechtsgrundlage für die Datenschutzaufsichten. Die Rechtsakte, die die Datenschutzaufsichten erlassen, sind aber nicht nur von

kirchlichen Stellen, sondern ggf. auch von staatlichen Gerichten zu überprüfen. Deshalb benötigen die Datenschutzaufsichten eine formelle Rechtsgrundlage für ihr Tätigwerden.

Nach dem neuen Gesetz (KDS-VwVfG) sind jetzt für den Erlass von Bußgeldbescheiden die Regelungen des Ordnungswidrigkeitengesetzes (OWiG) anzuwenden. Für verfahrensrechtliche Grundsätze wird nicht allgemein auf das staatliche Verwaltungsverfahrensgesetzt (VwVfG) verwiesen. Vielmehr wird aus diesem und dem Codex Juris Canonici (CIC) ein auf kirchliche Bedürfnisse zugeschnittenes Verfahrensrecht geschaffen. Dabei ist festzustellen, dass dies ausschließlich für kirchliche Datenschutzaufsichten anwendbar ist und nicht für andere Bereiche kirchlicher Verwaltung gilt. Da kirchlichen Datenschutzaufsichten bislang keine Zwangsmittel zur Durchsetzung ihrer Forderungen zur Verfügung standen, musste eine Regelung geschaffen werden, um der Forderung des Art. 91 Abs. 2 DS-GVO zu entsprechen. Die Datenschutzaufsicht soll nach dem neuen Gesetz zur Durchsetzung ihrer Forderungen auf kirchliche Zuwendungsgeber der bußgeldbelasteten Einrichtung zurückgreifen können, wenn diese keine Zahlung leistet. Ähnlich wie bei einem Vollstreckungs- und Überweisungsbeschluss können die Datenschutzaufsichten kirchliche Dienststellen anweisen, einer Einrichtung zustehende Zuschüsse an die Datenschutzaufsicht auszuzahlen.

Auch in dieser Hinsicht war dieses Gesetz erforderlich, um einen Einklang mit den Regelungen der DS-GVO näher zu kommen.

2 Datenschutzaufsicht

2.1 Prüfrechte der Datenschutzaufsicht

Eine Kooperation zwischen Verantwortlichen und der Datenschutzaufsicht verläuft häufig unbefriedigend. Dabei sind die Regelungen des KDG zu einer diesbezüglichen Zusammenarbeit eindeutiger als die der DS-GVO.

Art. 31 DS-GVO spricht davon, dass Verantwortliche auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten. Durch diese Formulierung wird der Verantwortliche nicht eindeutig zur

Zusammenarbeit verpflichtet. Gleichzeitig wird eine Zusammenarbeit aber auch nicht in das Belieben des Verantwortlichen gestellt. Eine Rechtsverbindlichkeit wird auch nicht durch die Interpretation des im Text verwendeten Indikativ: „arbeiten … zusammen" herbeigeführt.

Demgegenüber stellt § 44 Abs. 2 lit. a) und lit. b) KDG eine wesentlich eindeutigere Vorschrift dar: „Die … kirchlichen Stellen sind verpflichtet, im Rahmen ihrer Zuständigkeit lit. a) den Anweisungen der Datenschutzaufsicht Folge zu leisten, lit. b) die Datenschutzaufsicht bei Erfüllung ihrer Aufgaben zu unterstützen."

Die Eindeutigkeit bezieht sich auf mehrere Punkte. Zunächst ist durch den verwendeten Imperativ „sind verpflichtet" klar, dass es sich hierbei um eine Rechtspflicht des Verantwortlichen handelt. Weiterhin sind die „Anweisungen" nicht näher spezifiziert. Demnach kann die Datenschutzaufsicht festlegen, welche Anweisungen sie im Rahmen ihrer Überwachungspflicht gem. § 44 Abs. 1 KDG aussprechen kann. Die Vorschrift fordert, anders als Art. 58 Abs. 1 lit a) DS-GVO, nicht, dass diese Anweisungen „erforderlich" zur Aufgabenerfüllung der Datenschutzaufsicht sind. Die Aufsicht ist deshalb nicht verpflichtet, die hohen Anforderungen an die Erforderlichkeit darzulegen, da es ausreicht, wenn die Anweisungen zur Aufgabenerfüllung hilfreich bzw. nützlich sind. Schließlich ist die Datenschutzaufsicht bei der Erfüllung ihrer Aufgaben unabhängig davon zu unterstützen, ob eine diesbezügliche Anfrage vorliegt. Die Vorschrift verpflichtet also Verantwortliche auch zu proaktivem Handeln.

Beispielhaft („insbesondere") werden in § 44 Abs. 2 lit. b) KDG einzelne Verpflichtungen des Verantwortlichen benannt. Der Aufsicht ist danach Auskunft zu ihren Fragen zu gewähren. Auch hier ist durch den abermals verwendeten Imperativ „ist zu gewähren" kein Interpretationsspielraum gegeben. Die Aufsicht legt also fest, welche Fragen sie im Rahmen ihrer Aufgabenerfüllung für zweckdienlich hält.

Weiterhin ist der Datenschutzaufsicht Einsicht in Unterlagen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Neben der Einsicht in die personenbezogenen Daten selber, die beispielhaft erwähnt werden („namentlich"), ist der Einblick auch in solche

Unterlagen zu gewähren, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen, wie z. B. Datenverarbeitungsprogramme.

§ 44 Abs. 2 lit c) KDG legt weiterhin fest, dass die Datenschutzaufsicht Datenschutzuntersuchungen vornehmen kann. Eine Einschränkung im Hinblick auf eine solche Untersuchung enthält die Vorschrift nicht. Es steht also im freien Ermessen der Datenschutzaufsicht in welchem Umfang eine Datenschutzuntersuchung durchgeführt wird. Insbesondere ist die Aufsicht nicht darauf beschränkt, sich im Zusammenhang mit Datenschutzbeschwerden auf den Beschwerdegegenstand zu beschränken. Vielmehr ist es sinnvoll und zweckmäßig anlässlich einer Beschwerde zu prüfen, wie es zu einem Datenschutzvorfall kommen konnte. Dabei sind regelmäßig auch die technisch-organisatorischen Maßnahmen bzw. entsprechende Verzeichnisse der Verarbeitungstätigkeiten und allgemeine Arbeitsanweisungen in die Überprüfung mit einzubeziehen.

Im Hinblick auf die Verzeichnisse der Verarbeitungstätigkeiten legt § 31 Abs. 4 KDG fest, dass diese der Datenschutzaufsicht auf deren Anfrage zur Verfügung zu stellen sind. Aufgrund dieser Formulierung geht die Pflicht des Verantwortlichen also über ein „einsehen lassen“ hinaus. Der Datenschutzaufsicht sind auf deren Verlangen die Verzeichnisse physisch zugänglich zu machen, ggf. also in Kopie zu übersenden.

2.2 Umfang der Beratungspflicht durch die Datenschutzaufsicht

Häufig kommt es zu Unstimmigkeiten über die Beratungspflicht der Datenschutzaufsicht. Dies mag darin begründet sein, dass die Bezeichnung im KDG als „Diözesandatenschutzbeauftragter“ sich nicht deutlich vom betrieblichen Datenschutzbeauftragten abhebt. Dies wird auch in einigen Datenschutzhinweisen von Einrichtungen deutlich, die als „Datenschutzbeauftragten“ schlicht die Kontaktdaten der Datenschutzaufsicht angeben (und in diesen Fällen regelmäßig nicht wissen, dass sie selbst zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet sind). In den staatlichen Datenschutzgesetzen ist die Unterschiedlichkeit durch die Bezeichnungen „Datenschutzbeauftragter“ und „Aufsicht“ deutlicher hervorgehoben.

Es ist nicht Aufgabe der Datenschutzaufsicht Verantwortliche primär zu beraten. § 44 Abs. 3 lit. b) KDG spricht im Hinblick auf eine Beratung ausdrücklich nicht von Verantwortlichen. Soweit an dieser Stelle von Beratung gesprochen wird, geht es um eine politische Beratung[14] i. S. einer sachverständigen Beteiligung bei Gesetzesvorhaben u. ä.

Weiterhin spricht das Gesetz in § 35 Abs. 3 KDG davon, dass sich Verantwortliche eine Stellungnahme der Datenschutzaufsicht vorlegen lassen können, wenn sie nach Anhörung des betrieblichen Datenschutzbeauftragten zu der Ansicht gelangen, ohne Hinzuziehung der Aufsicht sei eine Datenschutzfolgenabschätzung nicht möglich.

Auch eine generelle Beratungspflicht der Aufsicht gegenüber den betrieblichen Datenschutzbeauftragten sieht das Gesetz nicht vor. Soweit § 38 S. 3 lit. e) KDG den betrieblichen Datenschutzbeauftragten auffordert, mit der Datenschutzaufsicht zusammenzuarbeiten, begründet dies dessen Verpflichtung, die Datenschutzaufsicht bei ihren Aufgaben zu unterstützen.

Gem. § 38 S. 2 KDG kann sich der betriebliche Datenschutzbeauftragte an die Datenschutzaufsicht wenden, wenn er beim Hinwirken auf die Einhaltung des Gesetzes oder anderer datenschutzrechtlicher Fragen Zweifel hat. Zweifelsfälle im Sinne dieser Vorschrift setzen aber konkrete Fragen zu einzelnen Problemen voraus. Das darf nicht zu einer Aufgabenübertragung an die Aufsicht oder zu unsubstantiierten Pauschalanfragen an diese führen.

Ebenso wenig darf die Aufsicht aufgrund des § 38 S. 3 lit e) KDG die betrieblichen Datenschutzbeauftragten als „Hilfsaufsichten" rekrutieren. Diese Vorschrift führt nicht zu einem Weisungsrecht der Aufsicht gegenüber den betrieblichen Datenschutzaufsichten.

Die Vereinnahmung in der einen als auch in der anderen Richtung würde die klare funktionale Trennung der beiden Aufgabenbereiche bzw. Organe entgegen der gesetzlichen Intention auflösen.

Ungeachtet dieser Grundsätze ist unsere Dienststelle um eine kooperative Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten im Rahmen regelmäßiger Erfahrungsaustausche bemüht. Anlässlich dieser Treffen stellt die Aufsicht ihre Rechtsauffassung zu bestimmten Themen oder

14 Hense, in: Sydow, Kirchliches Datenschutzrecht, 1. Aufl. 2020, § 44 Rn. 13

Problemen vor. Die betrieblichen Datenschutzbeauftragten können dazu ihre praktischen Erfahrungen einbringen. Zudem können sie eine rechtliche Bewertung zu den in der Praxis auftauchenden datenschutzrechtlichen Problemen von der Aufsicht erfragen. Im Ergebnis soll auf diese Weise ein rechtskonformer und praxisgeeigneter Datenschutz gewährleistet werden.

2.3 Anforderungen an die Beschwerde bei der Datenschutzaufsicht gem. § 48 KDG

Jede betroffene Person hat das Recht gemäß § 48 KDG eine Beschwerde bei der Datenschutzaufsicht gem. § 42 KDG einzureichen, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen das KDG verstößt. Der Beschwerdeführer hat nicht nur ein Recht auf Beantwortung und Bescheidung seiner Beschwerde, sondern einen darüberhinausgehenden Anspruch auf fehlerfreie Ermessensausübung und im Falle einer Ermessensreduzierung auf Null einen Anspruch auf ein konkretes Einschreiten der Datenschutzaufsicht.[15] Eine Beschwerde kann formlos eingereicht werden, da § 48 KDG keine ausdrücklichen Formerfordernisse regelt. Inhaltlich dürfen an die Beschwerde keine strengen Anforderungen gestellt werden, damit das Beschwerderecht grundsätzlich einfach und unbürokratisch ausgeübt werden kann.[16] Die Beschwerde muss aber alle Informationen enthalten, die erforderlich sind, damit die Datenschutzaufsicht den Sachverhalt erfassen und gegebenenfalls weiter aufklären und etwaige Datenschutzrechtsverstöße prüfen kann. Die Beschwerde muss daher Angaben über die betroffene Person und den Verantwortlichen aufweisen und zumindest ansatzweise zum Ausdruck bringen, welcher Verstoß gegen datenschutzrechtliche Vorschriften gerügt wird.[17] Schließlich kann der Beschwerdeführer keine Ermittlungen ins Blaue hinein durch die Datenschutzaufsicht beantragen.[18] Dabei kann von der betroffenen Person zwar keine juristische Bewertung erwartet werden, allerdings muss die Behauptung eines Rechtsverstoßes substantiiert -zumindest in Grundzügen- Angaben über den tatsächlichen Verstoß aufweisen.[19]

15 VG Mainz, 16.01.2020 - 1 K 129/19
16 Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 77 Rn. 10
17 Mundil, in: Wolff/Brink, BeckOK, Art. 77 Rn. 7
18 VG Mainz, 22.07.2020 -1 K 473/19.MZ
19 Mundil, in: Wolff/Brink, BeckOK, Art. 77 Rn. 7; VG Mainz 22.07.2020 -1 K 473/19 MZ

Wird vom Betroffenen eine nicht hinreichend konkretisierte Beschwerde eingereicht, muss die Datenschutzaufsicht den Beschwerdeführer darauf hinweisen und auf eine Konkretisierung der Beschwerde hinwirken.[20] Wurden Tatsachen vorgetragen, die eine Rechtsverletzung hinreichend wahrscheinlich erscheinen lassen, so wird die Datenschutzaufsicht diesem Vorbringen auch von Amts wegen nachgehen.

2.4 Meldepflicht contra Selbstbelastungsfreiheit

Gem. § 33 Abs. 1 KDG hat der Verantwortliche der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten zu melden, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten einer natürlichen Person darstellt. Eine solche Meldung hat regelmäßig innerhalb von 72 Stunden nach Feststellung der Verletzung zu erfolgen.

Mit dieser Regelung verpflichtet das Gesetz den Verantwortlichen zur Selbstbelastung. Der Verantwortliche sieht sich aufgrund dieser Regelung gegebenenfalls in der Zwicklage, den Datenschutzverstoß ordnungsgemäß zu melden und sich somit einer Sanktion auszusetzen oder einen neuerlichen Verstoß zu begehen, indem er eine Meldung unterlässt und auf Nichtentdeckung hofft.

Es stellt sich deshalb die Frage, ob eine solche Selbstbelastung eine Sanktionierung nach § 51 KDG ausschließt.

Für den staatlichen Bereich legen die §§ 42 Abs. 4 und 43 Abs. 4 BDSG fest, dass die Meldung eines Datenschutzverstoßes nicht oder nur mit Zustimmung des Meldenden in einem Straf- oder Ordnungswidrigkeitenverfahren verwendet werden darf. Eine solche Vorschrift ist im KDG nicht etabliert. Fraglich ist deshalb, ob sich eine solche Rechtsfolge trotz Fehlens einer entsprechenden Vorschrift aus verfassungsrechtlichen Grundsätzen ergibt, die zum Ausschluss eines Bußgeldes führen.

Eine zwangsweise herbeigeführte Selbstbezichtigung ist verfassungsrechtlich nur dann zulässig, wenn sie mit einem strafrechtlichen Verwertungsverbot einhergeht.[21] Der Zwiespalt, in den ein solcher Zwang den Einzelnen

20 Nemitz in Ehmann/Selmayr DS-GVO Art. 77, Rn 8
21 BVerfG Beschluss v. 15.10.2004 - 2 BvR 1316/04; BVerfGE 56, 37 <50 f.

führt, muss vor allem aus Gründen der Menschenwürde vermieden werden.[22] Die Würde des Menschen würde verletzt, wenn dessen erzwungene Aussage als Mittel gegen ihn selbst verwendet werden dürfte.[23]

Verfassungsrechtlich können sich jedoch grundsätzlich nur natürliche Personen auf die Grundrechte berufen. Für juristische Personen gilt dies gem. Art. 19 Abs. 3 GG nur dann, wenn die entsprechenden Grundrechte dem Wesen nach auch auf die juristische Person anwendbar sind. Bei dem Sanktionsverbot aufgrund einer Selbstanzeige geht es um den Schutz der Würde der natürlichen Person. Diese kann dem Wesen nach nicht auf juristische Personen anwendbar sein. Eine Geltung dieses Grundrechts für juristische Personen scheidet deshalb aus.

Das BDSG unterscheidet in den §§ 40 Abs. 4 S. 2, 42 Abs. 4 und 43 Abs. 4 aber nicht nach natürlichen und juristischen Personen, sondern stellt den Meldepflichtigen von Verfolgung frei. Meldepflichtig gem. Art. 33 Abs. 1 DS-GVO ist der Verantwortliche gem. Art. 4 Nr. 7 DS-GVO. Diese Vorschrift erweitert also die verfassungsmäßig gebotene Regelung auch auf juristische Personen.

Da das BDSG im kirchlichen Bereich keine Anwendung findet, ist eine Erweiterung des verfassungsmäßigen Schutzes bei Selbstbelastung auch auf juristische Personen nicht geboten.

2.5 Können Betroffene von Aufsichtsbehörden eine Geldbuße gegen den Verantwortlichen erzwingen?

Betroffene Personen haben grundsätzlich ein Recht auf Beschwerde bei einer Datenschutz-Aufsichtsbehörde. Das Verwaltungsgericht Ansbach musste sich mit der Frage beschäftigen, ob ein Betroffener einen eigenen Anspruch darauf hat, dass die Aufsichtsbehörde eine Datenschutzverletzung mit einer Geldbuße sanktioniert.[24]

Der Betroffene war der Ansicht, dass Datenschutzverstöße vorlagen, die mit einem Bußgeld zu ahnden sind. Das VG Ansbach war dagegen der Auf-

22 vgl. BVerfGE 56, 37 <42, 49>) BVR 26.2.97- 1 BVR 2172/96
23 BVerfGE 56, 37, 41
24 Verwaltungsgericht Ansbach, Urteil vom 16.03.2020, Az. AN 14 K 19.00464

fassung, dass keine oder keine wesentliche Datenschutzverletzung vorlag. Ungeachtet dessen nahm das Gericht jedoch auch zu der Frage Stellung, ob und inwieweit die Aufsichtsbehörde für den Fall einer Datenschutzverletzung zur Verhängung eines Bußgeldes gegenüber dem Arbeitgeber verpflichtet gewesen wäre.

Insofern führte das Gericht aus, dass die Datenschutz-Aufsichtsbehörde nach Art. 58 Abs. 2 Datenschutz-Grundverordnung (DS-GVO) eine Reihe sogenannter Abhilfebefugnisse habe, zu denen auch die Verhängung einer Geldbuße nach Art. 83 DS-GVO zähle. Die Ausübung und die Auswahl dieser Befugnisse stünde jedoch im Ermessen der Aufsichtsbehörde (sogenanntes "Opportunitätsprinzip" gem. § 47 Abs. 1 OWiG). Dies folge, so das Gericht, aus der Analyse des Wortlautes des Art. 83 Abs. 2 S. 2 DS-GVO sowie aus den Erwägungsgründen 148 und 150 zur DS-GVO.

Ein Anspruch eines Beschwerdeführers auf Verhängung einer Geldbuße käme nur in Betracht, wenn sich das Entschließungsermessen der Aufsichtsbehörde "auf Null" reduzieren würde. Dies könne nur angenommen werden, wenn die Verhängung einer Geldbuße die einzig mögliche Abhilfemaßnahme sei, die "zur Schaffung rechtmäßiger Zustände führe". In diesen Fällen hält das VG Ansbach – ohne letztlich abschließend darüber zu entscheiden – einen Anspruch einer betroffenen Person auf aufsichtsbehördliches Einschreiten prinzipiell für denkbar und begründet dies mit Art. 78 Abs. 1 DS-GVO, wonach jede Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde habe.

Das Gericht hat in dem der Entscheidung zugrundeliegenden Fall eine Ermessensreduzierung "auf Null" verneint. Der Betroffene hat damit keinen Anspruch darauf, dass die Aufsichtsbehörde Datenschutzverstöße mit der Festsetzung einer Geldbuße gegen den Verantwortlichen sanktioniert.

Das VG Ansbach hat mithin sehr hohe Anforderungen an einen Anspruch einer betroffenen Person auf Sanktionen der Aufsichtsbehörde gegenüber einem Verantwortlichen im Sinne der DS-GVO gestellt. Die Aufsichtsbehörde kann, nach der Auffassung des Gerichts, auch bei Vorliegen einer Datenschutzverletzung stets prüfen, ob eine Geldbuße oder eine andere Abhil-

femaßnahme (z.B. eine Verwarnung oder eine Anweisung in Bezug auf die konkrete Datenverarbeitung) angemessen ist.

Das Beschwerderecht eines Betroffenen bleibt also ein „scharfes Schwert" für den Verantwortlichen.

3 Datenschutz allgemein

3.1 Versendung personenbezogener Daten

3.1.1 Versendung personenbezogener Daten per Fax

Mehrfach haben wir darauf hingewiesen, dass bei der Versendung personenbezogener Daten per Fax besondere Sicherheitsvorkehrungen zu treffen sind.

Nunmehr hat das Oberverwaltungsgericht (OVG) Lüneburg[25] festgestellt, dass bei der Übermittlung personenbezogener Daten durch eine Einrichtung das Grundrecht auf informationelle Selbstbestimmung der Betroffenen durch Sicherheitsvorkehrungen zu gewährleisten ist.

Bei der Versendung von Telefaxen ist eine Verschlüsselung regelmäßig nicht möglich. Deshalb besteht an der Empfangsstelle grundsätzlich kein Hindernis für die Wahrnehmung der Daten. Das OVG verlangt personenbezogene Daten besonderer Kategorie (§ 4 Nr. 2 KDG) ausschließlich per Post zu versenden oder einen Boten einzusetzen. Dieser Auffassung schließt sich unsere Dienststelle an.

Aber auch bei der Versendung personenbezogener Daten (§ 4 Nr. 1 KDG) sind besondere organisatorische Maßnahmen zu treffen. Diese sind schriftlich festzulegen und Mitarbeitenden, die für eine Fax-Versendung infrage kommen, zuvor schriftlich bekannt zu machen. Das Fehlen solcher organisatorischen Maßnahmen führt zu einer Beanstandung durch die Datenschutzaufsicht. Wenn das Fehlen solcher Maßnahmen ursächlich für einen Datenschutzverstoß wird, weil ein Mitarbeiter die objektiv erforderliche Sorgfalt nicht eingehalten hat, wird dies immer mit einem Bußgeld geahndet werden.

25 Beschluss vom 22.07.2020 – 11 LA 104/19

3.1.2 Versendung personenbezogener Daten per E-Mail

Uns wurde ein Fall angezeigt, in dem personenbezogene Daten verschlüsselt per E-Mail versandt worden sind. Der Schlüssel zum Öffnen der E-Mail wurde in einer separaten E-Mail an denselben Empfänger versandt.

Wiederholt wurde darauf hingewiesen, dass personenbezogene Daten nur dann per E-Mail versendet werden dürfen, wenn die Versendung verschlüsselt stattfindet. Dazu ist es ausreichend, aber auch erforderlich, die Mitteilung, die die personenbezogenen Daten enthält, gegen eine direkte Öffnung zu schützen. Für die Öffnung der personenbezogenen Daten benötigt der Empfänger ein Passwort. Dieses Passwort muss im Sinne eines Zwei-Faktoren-Verfahrens auf einem anderen Weg als per Mail an den Empfänger gesendet werden.

Ein Zwei-Faktor-Verfahren liegt dann nicht vor, wenn die verschlüsselte Datei und das Passwort über denselben Kanal (E-Mail) versendet werden. Der Versand von personenbezogenen Daten per E-Mail gewährleistet keine ausreichende Sicherheit. Der häufig herangezogene Vergleich einer E-Mail mit einer Information auf einer Postkarte ist durchaus zutreffend. Deshalb ist die Verschlüsselung der Daten erforderlich. Wenn jedoch das Passwort über denselben unsicheren Übertragungsweg versendet wird, erhöht sich die Datensicherheit bestenfalls geringfügig. Auf jeden Fall stellt dies keine organisatorische Maßnahme zum Schutz für Rechte und Freiheiten der betroffenen Person gem. § 26 Abs. 1 KDG dar. Ein solches Verfahren wäre vergleichbar mit dem Abschließen einer Tür und dem gleichzeitigen Danebenhängen des Schlüssels.

Um eine datenschutzkonforme Versendung zu gewährleisten, hat die Übersendung des Passworts auf einem anderen Weg zu erfolgen. Dabei wird eine Zusendung des Schlüssels per Briefpost naturgemäß ausscheiden, da andernfalls die Versendung der personenbezogenen Daten per E-Mail sinnlos gewesen wäre. Auf jeden Fall ist es aber zumutbar und möglich das Passwort mit Hilfe telefonischer Übermittlung entweder fernmündlich oder per Short Message Service (SMS) weiter zu geben. Weiterhin besteht die Möglichkeit, gerade bei Kommunikationspartnern, die häufiger korrespondieren, ein festes Passwort zu vereinbaren, welches ggf. turnusmäßig gewechselt wird.

Der Verantwortliche wurde aufgefordert, das für die Versendung von personenbezogenen Daten bestehende Verfahrensverzeichnis diesbezüglich zu ergänzen.

3.2 Double Opt-In - Opt-Out Verfahren

Gem. § 7 Abs. 2 S. 3 UWG ist die Zusendung von Werbe-E-Mails nur nach vorheriger ausdrücklicher Zustimmung des Empfängers erlaubt. D. h. der Empfänger muss selbst erklärt haben, dass er mit der Zusendung von Werbung einverstanden ist. Dies entspricht einem Opt-In-Verfahren. Es reicht nicht aus, dass der Empfänger die Möglichkeit hatte, der Zusendung von Werbung im Sinne eines Opt-Out-Verfahrens zu widersprechen.

Problematisch war nun, dass auch Dritte eine Zusendung von Werbung oder Newsletters an eine E-Mail-Adresse veranlassen konnten, die gar nicht die ihre war. Mit dem Double-Opt-In-Verfahren soll das ausgeschlossen werden. Bei diesem Verfahren stimmt der Empfänger der Zusendung von Werbung oder Newslettern zunächst zu und bekommt eine E-Mail zugesandt, mit der er aufgefordert wird, sein ursprüngliches Einverständnis noch einmal zu bestätigen. Auf diese Weise wird abgeprüft, ob der Zustimmende auch Inhaber der E-Mail-Adresse ist. Erst wenn das Einverständnis noch einmal erklärt wird, erhält der Nutzer die Werbung oder Newsletter. Dieses Verfahren ist als Nachweis der Zustimmung von den Gerichten anerkannt.[26]

Bislang ist dieses Verfahren immer unter dem Gesichtspunkt des Wettbewerbsrechtes betrachtet worden. Am Anfang des Berichtszeitraumes wurde aber ein Beschluss der österreichischen Datenschutzaufsichtsbehörde veröffentlicht[27], der die Problematik aus datenschutzrechtlicher Sicht beleuchtet.

Unstreitig handelt es sich bei der E-Mail-Adresse einer natürlichen Person um ein personenbezogenes Datum. § 26 KDG verpflichtet Verantwortliche, dafür zu sorgen, dass Datensicherungsmaßnahmen angewandt bzw. eingesetzt werden, die Betroffene vor unrechtmäßiger Verarbeitung ihre personenbezogenen Daten schützen. Mit technisch-organisatorischen

26 OLG Düsseldorf, 17.03.2016 I – 15 U 64/15; OLG Celle, 15.05.2014 - 13 U 15/14
27 GZ: DSB-D130.073/0008-DSB/2019 vom 09.10.2019

Maßnahmen sind alle Maßnahmen gemeint, die darauf hinwirken, dass die Verarbeitung von Daten datenschutzgerecht und sicher erfolgt.[28] Dabei sind der Stand der Technik, die Implementierungskosten und der mit der Einführung verbundene Aufwand zu berücksichtigen.

Zur Verifizierung der Berechtigung einer bei Anmeldung zu einem Newsletter o. ä. verwendeten E-Mail-Adresse ist das Double-Opt-In-Verfahren Stand der Technik. Auch die damit verbundenen Kosten und der zur Einrichtung erforderliche Aufwand sind gering.

Damit ist der Ansicht der österreichischen Datenschutzaufsichtsbehörde darin zu folgen, die Implementierung eines Double-Opt-In-Verfahrens als verpflichtend für eine datenschutzkonforme Verarbeitung personenbezogener Daten zu fordern. Soweit bei Überprüfungen diesbezügliche Versäumnisse der Verantwortlichen festgestellt werden, stellen diese einen Datenschutzverstoß dar.

3.3 Eindeutiger Kündigungsschutz für den betrieblichen Datenschutzbeauftragten

§ 37 KDG regelt die Rechtsstellung des betrieblichen Datenschutzbeauftragten. In Abs. 4 ist die Unzulässigkeit einer ordentlichen Kündigung des Arbeitsverhältnisses mit dem betrieblichen Datenschutzbeauftragten festgeschrieben. Nur eine Kündigung aus wichtigem Grund, also eine außerordentliche Kündigung, ist zulässig. Das gilt unabhängig davon, ob die Kündigung mit der Erfüllung der Aufgaben als betrieblicher Datenschutzbeauftragter in Verbindung steht. Die Regelung geht über einen bloßen Abberufungs- und Benachteiligungsschutz hinaus. Der Kündigungsschutz wirkt auch nach Beendigung der Bestellung noch ein Jahr fort. Da das KDG keine näheren Einschränkungen festschreibt, gilt dieser Kündigungsschutz in jedem Fall. Es werden damit auch solche betrieblichen Datenschutzbeauftragten dem Kündigungsschutz unterstellt, die sich noch in der Probezeit befinden.[29] Ebenso gilt der Kündigungsschutz für vom Verantwortlichen freiwillig ernannte betriebliche Datenschutzbeauftragte, da eine Regelung wie sie § 38 Abs. 2 BDSG trifft, fehlt.

28 Herrlein, in: Sydow Kirchliches Datenschutzrecht, 1. Aufl. 2020, § 26 Rn. 7; Paal/Pauly DS-GVO 3. Aufl. 2021, Art. 32 Rn. 28
29 Franzen, in: Erfurter Kommentar zum Arbeitsrecht, 20. Aufl. 2020, § 38 BDSG Rn. 10

Während die DS-GVO nur einen Abberufungs- und Benachteiligungsschutz fordert, findet sich in § 38 Abs. 2 i. V. m. § 6 Abs. 4 BDSG eine dem kirchlichen Datenschutzrecht vergleichbare Regelung. Das Bundesarbeitsgericht (BAG) hat diesbezüglich aber die Frage aufgeworfen und dem Europäischen Gerichtshof (EuGH) zur Klärung vorgelegt, ob diese nationale Norm mit den Regeln der DS-GVO vereinbar ist.[30] Dies könnte aus Sicht des BAG dann der Fall sein, wenn wegen der schon durch die Richtlinie 95/46/EG bewirkten Vollharmonisierung entsprechend der Rechtsprechung des EuGH auch verschärfende nationale Regelungen unzulässig sind.

Die Entscheidung des EuGH in dieser Sache hat auf das kirchliche Datenschutzrecht keine direkte Auswirkung. Zwar müssen gem. Art 91 DS-GVO die kirchlichen Datenschutzregelungen mit der DS-GVO „im Einklang" stehen, aber sie müssen nicht wortgleich übereinstimmen [31], sondern Kern- und Wesensinhalt der DS-GVO rezipieren.[32] Die grundsätzlichen Wertungen der DS-GVO bestehen an dieser Stelle darin, den betrieblichen Datenschutzbeauftragten vor Benachteiligung zu schützen und die konsequente Normumsetzung zu sichern. Diesen Wertungen wird das KDG gerecht. Unabhängig von der Frage, ob die DS-GVO eine Vollharmonisierung fordert oder Mindeststandards festlegt, kann die kirchliche Regelung also von Art. 91 DS-GVO im o. g. Umfang abweichen.

3.4 Schadensersatz gem. § 50 Abs. 1 KDG

Immer wieder wurde in Veröffentlichungen in den letzten Jahren auf das Risiko der Verhängung hoher Bußgelder durch die Datenschutzaufsichten im Zusammenhang mit Datenschutzverstößen hingewiesen. Weit weniger Beachtung fand in der öffentlichen Diskussion die o. g. Vorschrift, nach der Betroffenen einen Anspruch auf Ersatz des materiellen oder immateriellen Schadens gegen die kirchliche Stelle zusteht, wenn ein Verantwortlicher oder Auftragsverarbeiter gegen das KDG verstößt.

Für die Geltendmachung eines solchen Schadensersatzanspruches sind nicht die kirchlichen Datenschutzgerichte, sondern die staatlichen Zivil-

30 BAG 30.06.2020 – 2 AZR 225/20 (A)
31 Hense; in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 9,1 Rn. 20
32 Jacob, in: Eßer/Kramer/v. Lewinski, DSGVO/BDSG, 7. Auflage 2020, Art. 91, Rn. 13

gerichte anzurufen.[33] Zwar erlaubt Art. 91 DS-GVO den Religionsgemeinschaften die bei ihnen bestehenden Datenschutzgesetze weiterhin anzuwenden, wenn sie diese mit der DS-GVO in Einklang bringen, so dass im kirchlichen Bereich nicht die DS-GVO gilt, sondern die kirchlichen Datenschutzgesetze, aber das gilt eben ausdrücklich nur für diese datenschutzrechtlichen Regelungen. Schadensersatzansprüche sind davon nicht umfasst und deshalb ausschließlich nach staatlichem Recht zu beurteilen.

Gem. § 50 Abs. 3 KDG kehrt sich im Falle eines Datenschutzverstoßes die Beweislast um. D. h. Verantwortliche oder Auftragsverarbeiter sind von einer Haftung nur dann befreit, wenn sie nachweisen können, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind.

Hat die kirchliche Datenschutzaufsicht festgestellt, dass eine Datenschutzverletzung objektiv vorliegt, ist diese Feststellung im Verfahren vor den Zivilgerichten bindend (§ 47 Abs. 2 KDG).

Schadensersatzansprüche sind individuelle Ansprüche Betroffener. Diese bestehen daher unabhängig davon, ob durch die kirchliche Datenschutzaufsicht bereits eine Geldbuße verhängt worden ist.

Nach § 51 Abs. 6 KDG können gegen kirchliche Stellen, die öffentlich-rechtlich verfasst sind, keine Geldbußen verhängt werden. Das schließt aber nicht aus, dass diese Stellen von Betroffenen auf Schadenersatz in Anspruch genommen werden können.

Der Begriff des Schadens ist weit auszulegen, damit Betroffene einen wirksamen Ersatz bekommen.[34] Dabei sind im Gegensatz zur Vorgängervorschrift nunmehr auch ausdrücklich Nichtvermögensschäden, also immaterielle Schäden, auszugleichen. Darunter fallen z. B. Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung oder andere gesellschaftliche Nachteile.[35] Wann ein immaterieller Schaden vorliegt, ist derzeit aber nicht abschließend entschieden. Nach einer weiten Auslegung kann ein Betroffener für jede Verletzung der DS-GVO durch Verarbeitung seiner perso-

33 LAG Nürnberg, 29.05.2020 - 8 Ta 36/20
34 Erwägungsgrund 146 zur DS-GVO
35 Erwägungsgrund 75 zur DS-GVO

nenbezogenen Daten auch ein angemessenes Schmerzensgeld verlangen. Insbesondere bei der Zugänglichmachung von Daten einer betroffenen Person für Dritte ohne ihr Einverständnis wird ein Schadensersatzanspruch auch einen immateriellen Schaden abzudecken haben, der diese öffentliche „Bloßstellung" kompensiert.[36] Der immaterielle Schaden läge nach dieser Vorschrift allein in der unrechtmäßigen Verarbeitung.[37]

Die bislang in Deutschland dazu ergangenen Gerichtsentscheidungen sind nicht einheitlich. Das LG Darmstadt hat einem Betroffenen einen Schadensersatz in Höhe von 1.000 € zugesprochen, weil der Verantwortliche seine Bewerberdaten an einen unberechtigten Dritten versandt hat.[38]
Das Arbeitsgericht Düsseldorf hat einem Arbeitnehmer einen Schadensersatzanspruch für einen immateriellen Schaden in Höhe von 5.000 € für einen verspäteten und unvollständigen Auskunftsanspruch zugesprochen. Nach Ansicht des Gerichts liegt ein immaterieller Schaden auch dann vor, wenn der Betroffene um seine Rechte und Freiheiten gebracht oder daran gehindert wird, die ihn betreffenden personenbezogenen Daten zu kontrollieren.[39] Andere Gerichte tendieren eher zu einer einschränkenden Auslegung.[40] Danach soll nicht bereits jede individuell empfundene Unannehmlichkeit oder jeder Bagatellverstoß einen Schadenersatzanspruch begründen.[41] Einer Verpflichtung zum Ausgleich eines immateriellen Schadens müsste vielmehr eine tatsächliche, brennbare Persönlichkeitsrechtsverletzung gegenüberstehen.[42]

Schadenersatzansprüche entziehen sich der Bewertung durch die Datenschutzaufsicht. Wir halten es aber für wichtig, an dieser Stelle auf weitere, insbesondere finanzielle Risiken hinzuweisen, denen Verantwortliche im Zusammenhang mit Datenschutzverstößen ausgesetzt sind.

3.5 Mit Auskunftsersuchen richtig umgehen!

Geht in einer kirchlichen Stelle ein Auskunftsersuchen ein, ist ignorieren die schlechteste aller Lösungen. Das Gesetz fordert, dass der Verantwortliche

36 Nemitz in Ehmann/Selmayr, Datenschutz-Grundverordnung 2. Auflage 2018 Rn. 13
37 Wybitul NJW 2019, 3265 (3266)
38 LG Darmstadt, Urteil vom 26.05.2020 - 13 O 244/19 Rn. 76
39 ArbG Düsseldorf 05.03.2020 9 Ca 6557/18 (nicht rechtskräftig Nachinstanz LAG Düsseldorf Az.: 14 Sa 29420)
40 OLG Dresden 11.06.2019 – 4 U 760/19; LG Karlsruhe 02.08.2019 – 8 O 26/19
41 OLG Dresden a.a.O.
42 LG Karlsruhe a.a.O.

in jedem Fall eine Antwort erteilen muss und zwar unverzüglich, also ohne schuldhaftes Zögern, spätestens aber innerhalb eines Monats nach Eingang des Antrags auf Auskunftserteilung (§ 14 Abs. 3 S. 1 KDG).

Abzuwarten und zu versuchen, das Ganze auszusitzen, ist keine Option, denn die Nichterfüllung der Auskunftspflicht kann mit der Verhängung einer Geldbuße geahndet werden. Eine Fristverlängerung ist nur in besonderen Ausnahmefällen möglich (§ 14 Abs. 3 S. 2 KDG). Ein solcher Ausnahmefall liegt nicht schon vor, wenn bestimmte Mitarbeiter krank oder im Urlaub sind. Auch eine routinemäßige Verlängerung scheidet aus, vielmehr ist auf den Einzelfall, d.h. der Komplexität des Auskunftsersuchens und auf den sich hieraus ergebende Arbeitsaufwand abzustellen. Der Betroffene muss jedoch über den Grund der Verzögerung ebenfalls innerhalb der Monatsfrist informiert werden. Der Verantwortliche darf gem. § 14 Abs. 3 S. 2 KDG die Auskunftsfrist um weitere zwei Monate verlängern.

Wird die Monatsfrist durch den Verantwortlichen versäumt, tritt Verzug ohne Mahnung gem. § 286 BGB i.V.m. § 14 Abs. 3 S. 2 KDG ein, da sich die Leistung nach dem Kalender berechnen lässt. Nimmt sich der Betroffene daher nach Ablauf der Frist einen Anwalt zur vorgerichtlichen Geltendmachung des Auskunftsanspruches, kann er die hierfür angefallenen Rechtsanwaltskosten als Verzugsschaden geltend machen. Dies neben der Möglichkeit Schadensersatz für immaterielle Schäden geltend zu machen.

Bei einer eingehenden Anfrage sind fünf zentrale Fragen zu klären.

- Werden überhaupt Daten des Anfragenden verarbeitet?
- Kann die Auskunft vielleicht verweigert werden?
- Welche Inhalte müssen mitgeteilt werden?
- In welcher Form muss die Auskunft erfolgen?
- Ist der Anfragende berechtigt?

1. Werden Daten des Anfragenden verarbeitet?

Zunächst muss geklärt werden, ob im konkret angefragten Fall überhaupt eine Verarbeitung von personenbezogenen Daten über die betroffene

Person stattfindet. Grundvoraussetzung dafür ist, dass der Verantwortliche einen Überblick darüber hat, wo er welche Daten verarbeitet.

a) Negativauskunft

Liegen keine Daten über den Anfragenden vor, muss der Verantwortliche ihm auch dies mitteilen. Das ergibt sich aus § 17 Abs. 1 erster Halbsatz KDG.

Bei einer solchen sogenannten Negativauskunft sind einige weitere Punkte zu beachten, da die Anfrage selbst personenbezogene Daten, wie den Namen des Absenders und seine Anschrift enthält. Der Verantwortliche muss diese Daten zwangsläufig verarbeiten, um eine Antwort erteilen zu können.

Beachtet werden muss, dass die allgemeinen Datenschutz-Grundsätze anzuwenden und insbesondere die allgemeinen Datenschutz-Informationen zur Verfügung zu stellen sind.

Die Hinweise zum Datenschutz müssen die üblichen Angaben nach § 14 KDG (Art. 13 DS-GVO) enthalten. Dazu gehört u.a. eine Angabe, wie lange das Unternehmen oder die Behörde Auskunftsersuchen und deren Beantwortung aufbewahrt.

Es ist sinnvoll, die Auskunftserteilung und auch Negativauskünfte für eine gewisse Zeit zu speichern. Dies ergibt sich aus der Rechenschaftspflicht gemäß § 5 Abs. 2 KDG. Denn nur so kann im Streitfall nachgewiesen werden, dass der Datenschutz eingehalten wird.

Beispielformulierung für eine Negativauskunft

Sehr geehrte/r Frau/Herr ...,

wir haben keine personenbezogenen Daten zu Ihrer Person gespeichert. Davon ausgenommen sind diejenigen Daten, die Sie uns selber in Ihrer Bitte um Auskunft mitgeteilt haben.
Unsere Hinweise zum Datenschutz finden Sie ... (z.B. nachfolgend, auf der Rückseite, in angehängter Datei, auf der Internetseite www.xyz.de/datenschutz).

Speicherfrist für Negativauskünfte

Eine unbefristete Speicherung ist, wie sonst auch, generell nicht zulässig. Als Richtwert lässt sich auf die Verjährungsvorschriften zurückgreifen, da

das KDG keine Regelung trifft. Nach Ablauf der Verjährungsfrist kann ein Betroffener keine Ansprüche mehr aus einer Nicht- oder Falscherteilung einer Auskunft geltend machen.

In analoger Anwendung von § 31 Abs. 2 Nr. 1 Ordnungswidrigkeitengesetz (OWiG) ergibt sich eine Verjährungsfrist von 3 Jahren.

Negativauskunft sollten somit drei Jahre nach der Auskunftserteilung aufbewahrt und danach gelöscht werden.

b) Datenverarbeitung erfolgt

Werden Daten der betroffenen Person verarbeitet, muss der Verantwortliche nun prüfen, ob er die Auskunft erteilen muss.

2. Auskunftsverweigerung

In der Regel wird ein Verantwortlicher die Auskunft erteilen müssen. Ausnahmen gibt es nur bei offenkundig unbegründeten oder exzessiven Anträgen, also wenn der Betroffene seine Anfrage z.B. ohne nachvollziehbaren Anlass mehrmals im Jahr wiederholt (§ 15 Abs. 4 KDG).

Die Beweislast hierfür liegt beim Verantwortlichen, nicht beim Anfragenden. Eine Dokumentation der Anfrage ist auch aus diesem Grund erforderlich.

Ausnahmen: § 17 KDG

Gem. § 17 Abs. 6 KDG besteht ein Recht auf Auskunft dann nicht,

- wenn die betroffene Person bereits über die Informationen verfügt (§ 17 Abs. 6 lit a) i.V.m. § 15 Abs. 4 KDG oder
- wenn die Informationserteilung an die betroffene Person einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls insbesondere wegen des Zusammenhangs, in dem die Daten erhoben werden, als gering anzusehen sind (§ 17 Abs. 6 i.V.m. § 15 Abs. 4 KDG) oder
- wenn die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das

Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss (§ 17 Abs. 6 lit. a) i.V.m. § 15 Abs. 5 lit. a) KDG) oder

- wenn - im Falle einer kirchlichen Stelle im Sinne des § 3 Abs. 1 lit. c) KDG (z. B. Krankenhausträger) die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde und nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt (§ 17 Abs. 6 lit. a) i.V.m. § 16 Abs. 5 lit. b) KDG) oder
- wenn die Daten nur noch aufgrund gesetzlicher Aufbewahrungsvorschriften oder satzungsmäßiger Aufbewahrungsfristen gespeichert bleiben müssen (z.B. aus buchhalterischen Gründen) und eine Auskunft unverhältnismäßig aufwendig wäre sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist (§ 17 Abs. 6 lit. b) KDG) oder
- wenn die Daten ausschließlich zu Zwecken der Datensicherheit oder Datenschutzkontrolle dienen.

Die Geheimhaltung kann sich aus einer Rechtsvorschrift oder aus „ihrem Wesen", insbesondere aus „überwiegend berechtigten Interesse eines Dritten", ergeben. Darauf können sich in erster Linie Berufsgeheimnisträger, wie z. B. Rechtsanwälte oder Ärzte berufen.

Weitere Spezialfälle

Darüber hinaus gibt es Ausnahmen für Spezialfälle in folgenden Bereichen:

- Datenverarbeitung zu Zwecken der Forschung oder Statistik und Datenverarbeitung bei kirchlichen Archiven (§ 16 Abs. 4 KDG), wenn ihre Auskunft zu einer Gefährdung der Verwirklichung der Ziele dieser Verarbeitung führen würde.

Kommt eine dieser Ausnahmen zur Anwendung, muss der Verantwortliche dies begründen. Die Gründe muss er dem Betroffenen mitteilen (§ 17 Abs. 7 KDG).

3. Welche Inhalte müssen mitgeteilt werden?

Die Inhalte der Auskunft richten sich nach dem Auskunftsbegehren des Betroffenen.

Maximal besitzt der Betroffene einen gesetzlichen Anspruch auf die folgenden Informationen (§ 17 Abs. 1 KDG):

- Zu welchen **Zwecken** verarbeitet der Verantwortliche die Daten des Betroffenen? Beispiel: zur Erfüllung des Vertrags mit dem Betroffenen.
- Welche **Kategorien** von personenbezogenen Daten verarbeitet er? Es ist hier nicht notwendig, jedes einzelne Datenfeld aufzulisten, sondern es genügt, Oberbegriffe zu nennen.
- An welche **Empfänger** oder Kategorien von Empfängern werden seine Daten ggf. offengelegt? Auch Empfänger in Drittländern außerhalb von EU und EWR müssen genannt werden.
- Nach welchen Kriterien bemisst sich die **Speicherdauer**? Es empfiehlt sich die oft verwendete Aussage, dass Daten „so lange gespeichert werden, so lange sie für die oben genannten Zwecke erforderlich sind und gesetzliche Aufbewahrungsfristen dies verlangen“ durch möglichst konkrete Aufbewahrungsfristen zu ergänzen.
- Hinweis auf die **Betroffenenrechte**, also auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch (§ 17 Abs. 1 lit e) KDG).
- Hinweis auf die Möglichkeit, sich bei einer **Aufsichtsbehörde** über die Datenverarbeitung zu beschweren. Konkrete Kontaktdaten müssen jedoch nicht mitgeteilt werden.
- Stammen die Daten nicht vom Betroffenen, sondern aus einer anderen Quelle: Angaben über alle verfügbaren Informationen zur **Herkunft der Daten** (§ 17 Abs. 1 lit f) KDG).
- Sind die Daten einer **automatisierten Entscheidung**, einschließlich Profiling, unterworfen – im Sinn von § 24 KDG, etwa bei Bonitäts-Scoring oder Verfolgung des Standorts: aussagekräftige Informationen über die zugrunde liegende Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

- Werden die Daten an ein **Drittland** übermittelt, also an ein Land außerhalb der EU und des EWR, besitzt der Anfragende auch das Recht, die Rechtsgrundlage dafür zu erfahren (z.B. EU-Standardvertrag o.Ä.).

4. Form der Auskunftserteilung

Die betroffene Person hat Anspruch darauf, „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", zu erhalten (§ 17 KDG). Der Verantwortliche muss die Daten so herausgeben, wie sie bei ihm vorliegen.

Bei der Form der Auskunft besteht jedoch ein Spielraum. Sie muss nicht zwingend schriftlich erfolgen. Anträge, die in elektronischer Form eingehen, können auch elektronisch beantwortet werden, soweit der Betroffene nichts anderes angibt (§ 17 Abs 3 KDG). Denkbar ist dann etwa die Übermittlung einer PDF-Datei.

Zudem ist darauf zu achten, dass die Datenkopie vollständig ist. Teile zu schwärzen oder wegzulassen, ist nur zulässig,

- wenn eine der Ausnahmen besteht, die oben beschrieben sind, oder
- wenn die Herausgabe die „Rechte und Freiheiten anderer Personen" beeinträchtigt (dazu zählt auch der Verantwortliche selbst) (§ 17 Abs. 4 KDG). Eine solche Beschränkung des Auskunftsrechts kann sich beispielsweise aus Geschäftsgeheimnissen oder aus geistigen Eigentumsrechten, etwa dem Urheberrecht an Software ergeben.

Auch in diesen Fällen muss der Verantwortliche die Auskunft jedoch erteilen. Nur die sensiblen Passagen darf er weglassen oder unkenntlich machen.

Die Auskunft muss kostenfrei erfolgen. Nur wenn der Betroffene z.B. eine zweite oder „weitere Kopie" verlangt, dürfen angemessene Verwaltungskosten erhoben werden (§ 17 Abs. 3 KDG).

5. Ist der Anfragende berechtigt?

Auskunft darf nur derjenige erhalten, um dessen Daten es geht. Der Verantwortliche muss verhindern, dass Unberechtigte Informationen erhalten,

die nicht für sie bestimmt sind. Bekäme ein Unberechtigter eine Auskunft, läge regelmäßig eine Datenpanne vor, die der Verantwortliche bei der Behörde melden müsste (§ 33 KDG).

Um so etwas zu vermeiden, sind klare interne Vorgaben nötig, wie eine Identitätsprüfung stattzufinden hat. Die DS-GVO und das KDG stellen hier allerdings keine allzu hohen Anforderungen. Laut Gesetz darf eine Auskunft bereits erteilt werden, soweit „keine begründeten Zweifel an der Identität" des Anfragenden bestehen (§ 15 Abs. 6 KDG).

Zu raten ist folgendes Vorgehen. Bei einem persönlichen Gespräch sollte zur Identifikation die Vorlage des Ausweises mit Foto gefordert werden, wobei die Anfertigung einer Kopie unterbleiben soll. In anderen Fällen könnte nach Daten gefragt werden, die bereits im System hinterlegt sind, um diese zu vergleichen, etwa Geburtsdatum oder Kundenummer, Krankenhausaufenthalt (Dauer, Klinik, Station etc.).

Bei einem elektronischen Antrag könnte man sich die Postanschrift bestätigen lassen. Soweit der Betroffene Auskunft über besonders sensible Daten begehrt (etwa Gesundheitsdaten), ist es hilfreich, wenn der Anfragende freiwillig eine Kopie seines Ausweises bereitstellt. In dieser Kopie dürfen/sollten dann alle nicht benötigten Angaben geschwärzt sein.

Eine weitere wichtige Maßnahme, um das Risiko einzudämmen, ist, die Auskunft immer nur an diejenige Adresse zu übermitteln, die bereits vor dem Auskunftsersuchen für den Betroffenen hinterlegt war.

Fazit: Auskunftsersuchen ernst nehmen!

Auskunftsersuchen sind unbedingt ernst zu nehmen. Denn unvollständige, unterlassene oder zu späte Antworten sind nicht nur von Geldbußen bedroht, sondern können auch Schadensersatzansprüche für immaterielle Schäden nach sich ziehen, wie eine Entscheidung des Arbeitsgerichts Düsseldorf zeigt (Schadenersatz in Höhe von 5.000 Euro, weil ein früherer Arbeitgeber einen Auskunftsantrag verspätet und unvollständig beantwortet hatte.[43]

Sorgen Sie deshalb vor: Wissen die Mitarbeiter, wie sie in solchen Fällen vorzugehen haben, und ist klar festgelegt, wer für was verantwortlich ist,

43 ArbG Düsseldorf, Urt. v. 05.03.2020, Az. 9 Ca 6557/18

lässt sich die Auskunft fristgerecht und sicher erteilen. Empfehlenswert ist das Vorhandensein von entsprechenden Anweisungen.

3.6 Diebstahl von Digitalkamera mit Speicherkarte im Kindergarten und anderen Einrichtungen

Bereits in unserem letzten Bericht[44] haben wir einen Fall dargestellt, indem es um einen Einbruch in eine Kindertagesstätte ging, bei dem neben IT-Technik auch eine Digitalkamera gestohlen worden ist.

Sofern auf der Speicherkarte Fotos von Kindern oder anderen Personen enthalten sind, handelt es sich um personenbezogen Daten. In diesen Fällen hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau vor unbefugter oder unrechtmäßiger Verarbeitung zu gewährleisten.

Regelmäßig glauben die Verantwortlichen dem Genüge getan zu haben, wenn die Kamera in einem verschlossenen Schrank oder sogar in einem Tresor aufbewahrt wird. Die Praxis zeigt aber, gerade in Kindereinrichtungen und Schulen, dass Einbrecher über einige Erfahrung und hinreichend kriminelle Energie verfügen, um werthaltige Gegenstände aufzuspüren. In Kenntnis dieser Tatsachen sollte deshalb dem Schutz der personenbezogenen Daten besonders Rechnung getragen werden. Häufig wird es den Kriminellen nicht um die auf den Geräten gespeicherten Informationen und personenbezogenen Daten gehen, sondern nur um die Geräte selbst. Dennoch kann nicht mit Sicherheit davon ausgegangen werden, dass nicht, wenn auch nur als „Beifang“, Bilddateien zu Geld gemacht werden. Als technisch-organisatorische Maßnahme ist deshalb die Anweisung erforderlich, Speicherkarten getrennt und datenschutzkonform von Kameras aufzubewahren. Damit kann zumindest in den Fällen, in denen es den Tätern um die Kamera geht, verhindert werden, dass ein Zugriff auf die Bilddateien direkt möglich ist.

44 4. TB 2019, Seite 31 f.

Eine weitere Möglichkeit wäre, die Fotografien nach der Aufnahme auf einen Server zu übertragen und auf der Speicherkarte der Kamera zu löschen.

Da sich die Fotografien auf der Speicherkarte wiederherstellen lassen, wäre der sicherste aber auch aufwendigste Weg, um eine Wiederherstellung der Fotografien auszuschließen, die auf der Speicherkarte hinterlegten Daten mit Hilfe einer besonderen Software unwiederbringlich zu löschen. Für welche dieser Möglichkeiten sich der Verantwortliche entscheidet, ist vom Einzelfall, insbesondere von der Sensibilität der gespeicherten Daten, abhängig. Der Verantwortliche, der keine dieser Sicherungsmaßnahmen ergreift, handelt datenschutzwidrig.

4 Datenschutz im Gesundheitswesen

4.1 Need-to-know-Prinzip (Kenntnis nur bei Bedarf) und in der Praxis gelebtes Berechtigungsmanagement (Rollenkonzepte)

Informationen über Patienten sind Gesundheitsdaten gem. § 4 Nr. 17 KDG und unterliegen einem besonders hohen Schutz (§ 11 KDG). Der Verantwortliche muss gem. § 26 KDG dafür Sorge tragen, dass ein angemessenes Schutzniveau für die Patientendaten gewährleistet ist. Gerade im Hinblick auf die stetig steigende Digitalisierung der krankenhausinternen Vorgänge und die Einführung einer elektronischen Patientenakte sind organisatorische Maßnahmen erforderlich.

Neben der Etablierung und regelmäßigen Kontrolle des Berechtigungsmanagements ist auch erforderlich, dass eine an den IT-Sicherheitsstandards orientierte Infrastruktur samt Kontrollmechanismen vorhanden ist. Grundsätzlich gilt hierzu folgendes:

Ein Zugriff auf Gesundheitsdaten eines Patienten sollte nur bei Bedarf und auch nur aufgrund einer vorher definierten Berechtigung erfolgen. Der im KDG verankerte Grundsatz (Integrität und Vertraulichkeit) verlangt, dass eine angemessene Sicherheit der Verarbeitung personenbezogener Daten

und gerade auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung gewährleistet wird.

In der Regel wird dies durch ein definiertes Berechtigungs- oder Rollenkonzept gewährleistet, welches den Zugriff durch die Ärzteschaft, des pflegerischen Stationspersonals sowie der Mitarbeiter der Administration am Empfang regelt.

Nach dem anzuwendenden need-to-know-Prinzip soll Zugriff auf Patientenakten grundsätzlich nur behandelnden Ärztinnen und Ärzten sowie dem betreuenden Stationspersonal eingeräumt werden. Im Konzept sollten Vertretungen oder Zugriffsrechte in Notfallsituationen geregelt sein, damit die Gesundheitsversorgung nicht hinter dem Datenschutz zurückfällt, gleichzeitig aber ein angemessenes Datenschutzniveau eingehalten werden kann.

Das Berechtigungskonzept muss in einer an IT-Sicherheitsstandards ausgerichteten Infrastruktur eingebettet sein, um Schutz zu bieten. Die Daten im Krankenhausinformationssystem (KIS) müssen vor Verlust und unbefugten Zugriffen von außen gesichert sein. Von Seiten der IT-Abteilung müssen die Rechtevergabe und die Berechtigungen der Krankenhausangehörigen tatsächlich dokumentiert und kontrolliert werden. Zudem muss missbräuchliches Verhalten aufgedeckt und den zuständigen Stellen gemeldet werden.

„Wer sich in ärztliche Behandlung begibt, muss und darf erwarten, dass alles was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim bleibt und nicht zur Kenntnis Unbefugter gelangt".[45]

Diese Feststellung ist in Zeiten der Digitalisierung und elektronischer Patientenakten umso wichtiger und muss vom Verantwortlichen zwingend eingehalten werden. Damit dies erreicht werden kann, muss eine Zusammenarbeit aller Fachabteilungen, von der Krankenhausverwaltung, über die jeweiligen Stationen und Ambulanzen, die IT-Abteilung, das Qualitätsmanagement, die Compliance und den internen bzw. externen Datenschutzbeauftragten erfolgen. In diesem Zusammenhang ist zwingend erforderlich, dass ein an der Größe des Krankenhauses und der dort stattfindenden Anzahl an Datenverarbeitungen ausgerichtetes Datenschutzkonzept erar-

45 BVerfG, 08.03.1972, AZ: - 2 BvR 28/71

beitet, eingerichtet und im Hinblick auf die Einhaltung von Datenschutzstandards regelmäßig überprüft wird.

Das Thema Schutz von Patientendaten ist zu Recht, wie an uns gemeldete Datenschutzverletzungen zeigen, in den Fokus von Aufsichtsbehörden gerückt. Gesundheitsdaten gehören zu den sensibelsten Informationen über einen Menschen.

4.2 Art. 15 DS-GVO vs. § 630g BGB und das Recht auf kostenlose Kopie

Patienten haben umfangreiche Auskunftsrechte. Diese ergeben sich aus unterschiedlichen gesetzlichen Regelungen, die sich teilweise widersprechen. Besonders deutlich zeigt sich dieser Widerspruch anhand der Frage, ob Gesundheitseinrichtungen für die Anfertigung von Kopien der Patientenakte eine Kostenerstattung verlangen können oder die Kopien kostenlos erstellt werden müssen.

4.2.1 Anspruchsgrundlagen für Auskunftsansprüche

Gem. § 630 g BGB hat der Patient das Recht Einsicht in seine vollständigen Patientenunterlagen zu nehmen. Daneben hat der Patient gem. § 17 KDG (Art. 15 DS-GVO) einen Anspruch darauf zu erfahren, ob ihn betreffende personenbezogenen Daten verarbeitet werden.

Die Reichweite bzw. Zielrichtung der Auskunftsrechte nach diesen beiden Vorschriften sind strittig.

Unstreitig steht dem Patienten nach § 630g BGB ein Recht auf Einsichtnahme in die vollständige Patientenakte zu, sofern der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Sinn und Zweck der großen Reichweite dieser Vorschrift ist es, dass der Patient seine Behandlung nachvollziehen kann, sodass auch in der Akte abgelegte Befunde anderer Ärzte und Arztbriefe erfasst sind.

Nach § 17 Abs. 1 KDG hat der „Betroffene“, mithin also auch der Patient, Anspruch auf eine umfassende, zusammenfassende Auskunft über die über ihn geführten und verarbeiteten Daten. Hieraus wird teilweise geschlossen,

dass dieser Anspruch auch einen umfassenden Auskunftsanspruch über die komplette Patientenakte beinhaltet. So verurteilte z. B. das Landgericht Dresden das Universitätsklinikum der Stadt im Mai 2020, einer Patientin eine unentgeltliche Auskunft über ihre „gespeicherten personenbezogenen Daten durch Übermittlung der vollständigen Behandlungsdokumentationen im PDF-Format zu erteilen".[46] Die Klägerin hatte unter Verweis auf die DS-GVO die kostenlose Übermittlung der gewünschten Informationen gefordert.

Demgegenüber vertritt eine andere Meinung, insbesondere auch die einiger Landesdatenschutzbehörden, die Auffassung, dass § 630g BGB einen weitergehenden Auskunftsanspruch, bezogen auf die Besonderheiten des Arzt – Patientenverhältnisses und den Behandlungsvertrag beinhaltet und der Anspruch nach Art. 15 DS-GVO lediglich den Anspruch auf eine Auskunft in der Form einer strukturierten Zusammenfassung begründet. Diese Ansicht hätte zur Folge, dass sich der Anspruch auf Auskunft lediglich darauf beziehen könnte, zu erfahren, ob und wenn ja welche Daten von dem Verantwortlichen verarbeitet werden. Man könnte davon ausgehen, dass maßgeblicher Hintergrund des datenschutzrechtlichen Auskunftsrechts die Überprüfung der technischen Rechtmäßigkeit der Verarbeitung der Daten, d. h. des Verarbeitungsprozesses ist und nicht die Prüfung der Inhalte, wie z. B. spezielle Diagnosen, Befunde etc., die Informationen über die Gesundheit des Betroffenen enthalten. Inhalt des Ankunftsanspruchs gemäß Art. 15 DS-GVO wäre dann allein die Prüfung der Rechtmäßigkeit der Datenverarbeitung an sich.

Für diese Ansicht spricht, dass es wörtlich in Art.15 Abs. 3 DS-GVO heißt: „Der Verantwortliche stellt eine **Kopie der personenbezogenen Daten**, die Gegenstand der Verarbeitung sind, zur Verfügung."

Ausdrücklich nicht erwähnt sind Kopien der betreffenden Akten oder sonstiger Unterlagen. Der Europäische Gerichtshof (EuGH) hat in seiner Entscheidung vom 17.07.2014,[47] zum Umfang eines Auskunftsanspruches ausgeführt, dass es zur Wahrung des Auskunftsrechts genügt, wenn der Antragsteller eine **vollständige Übersicht** seiner Daten in verständlicher

46 LG Dresden, Urteil vom 29. Mai 2020, Az.: 6076/20
47 EuGh, 17.04.2014 - C-141/12 und C-372/12

Form erhält, d. h. in einer Form, die es ihm ermöglicht, von diesen Daten Kenntnis zu erlangen und zu prüfen, ob sie richtig sind.

Nach dem Gesetzeswortlaut des Art. 15 DS-GVO steht dem Betroffenen das Recht zu, von dem Verantwortlichen zu erfahren, ob überhaupt ihn betreffende personenbezogene Daten verarbeitet werden. In einer zweiten Stufe kann er verlangen zu erfahren, welche personenbezogenen Daten gespeichert werden. Zusätzlich hat die betroffene Person Anspruch auf weitere Informationen, die sich aus dem Katalog des Art. 15 Abs. 1 bzw. § 17 Abs. 1 KDG ergeben. Dies umfasst eine Auskunft über

- Die Verarbeitungszwecke
- die Kategorien der verarbeiteten Daten
- die Empfänger bei erfolgter oder beabsichtigter Offenlegung personenbezogener Daten
- die Dauer der Datenspeicherung
- die Betroffenenrechte
- die Herkunft der personenbezogenen Daten, wenn diese nicht bei der Patientin/dem Patienten selbst erhoben wurden

Gegen die Auffassung, dass der datenschutzrechtliche Auskunftsanspruch nach § 17 KDG und das Recht auf Einsicht in die Patientenakte gem. § 630 g BGB dieselbe Zielrichtung verfolgen, spricht auch die Tatsache, dass es der Gesetzgeber selbst bewusst unterlassen hat im entsprechenden Verfahren zum Datenschutz-Anpassungsgesetz § 630g BGB an die Regelung der DS-GVO anzupassen und damit eine Wertung getroffen hat. Durch das am 25.11.2019 verkündete Gesetz sind Anpassungen in rund 150 Gesetzes erforderlich geworden, nicht jedoch in § 630 g BGB. Die Regelung des § 630 g BGB trat erst im Jahr 2013 in Kraft. Dies spricht eindeutig dafür, dass § 630g BGB eine andere Zielrichtung als die Regelung der DS-GVO bzw. des KDG hat.

Dies lässt sich weiterhin auch daran erkennen, dass das Einsichtsrecht nach BGB nur unter engen Grenzen verwehrt werden kann, während für das Auskunftsrecht ein breiterer Spielraum gegeben ist. Auch der Hessische

Landesdatenschutzbeauftragte (HDBI)[48] geht davon aus, „dass der Bundesgesetzgeber in der Akteneinsicht nach § 630g BGB eine von dem Auskunftsanspruch und dem Recht auf Kopie des Art. 15 DS-GVO unabhängige Regelung mit anderem Inhalt und anderem Zweck sieht. § 630g BGB ist damit keine Einschränkung des Rechts auf Auskunft nach Art. 15 DS-GVO. Die Norm dient anderen Patienteninteressen als Art. 15 DS-GVO." Das Bayerische Landesamt für Datenschutz (BayLDA) hat sich zu diesem Thema ebenfalls bereits geäußert.[49] Es geht darin davon aus, dass § 630g BGB, als bereichsspezifische Vorschrift, über den datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DS-GVO hinausgeht. In Bezug auf Art. 15 Abs. 3 DS-GVO („Kopie der personenbezogenen Daten") geht das BayLDA außerdem davon aus, dass nur eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", dem Auskunftsersuchenden zur Verfügung zu stellen sind. Jedoch ist hier nicht die Rede von Kopien der betreffenden Akten oder sonstiger Unterlagen.

Dafür spricht auch, dass der Gesetzgeber mit der Einführung des § 630 g BGB festgehalten hat, dass der Patient ein schutzwürdiges Interesse daran habe, zu wissen, wie mit seiner Gesundheit umgegangen wird, welche Daten sich dabei ergeben haben und wie die Entwicklung hinsichtlich seiner Gesundheit eingeschätzt werde. Die Regelung des § 630 g BGB greift die Rechtsprechung des BVerfG[50] aus dem Jahr 2006 auf und dient insbesondere der Umsetzung des Rechts des Patienten auf informelle Selbstbestimmung.[51] Das BVerfG hatte auf die medizinische Behandlung des Patienten, mithin auf Erkenntnisse seiner eigenen Gesundheit, abgestellt. Die Frage der Rechtmäßigkeit der Verarbeitung der Daten stand nicht im Raum. Der Anspruch aus § 630g BGB gibt dem Betroffenen die Möglichkeit, eine ärztliche Behandlung selbstständig und kritisch überprüfen zu können. Dazu bedarf es der Kenntnis des Krankheitsbildes und des in den Akten dokumentierten Behandlungsverlaufs sowie gestellte gesundheitliche Prognosen.

Unter diesem Blickwinkel ist davon auszugehen, dass es sich um zwei Regelungen mit zwei Zielrichtungen handelt. Das Recht auf Auskunft gem.

48 Beitrag „Einsicht in die Patientenakte nach § 630 g BGB" veröffentlicht auf der Website des HDBI
49 Tätigkeitsbericht 2017/18 S. 46
50 BVerfG 09.01.2006 - AZ: 2 BvR 443/02, NJW 16/06, 1116 ff.
51 Regierungsentwurf zur Verbesserung der Rechte von Patientinnen und Patienten, BT-Drs. 17/10488, S. 26

Art. 15 DS-GVO und auch das Recht gem. § 630 g BGB dient der informationellen Selbstbestimmung des Patienten, beide Rechte haben jedoch, wie bereits dargelegt, einen völlig anderen Gegenstand, Sinn und Zweck. Kurz gesagt, nach Art. 15 DS-GVO interessiert den Betroffenen doch Folgendes: Was weiß man alles von mir, was wird mit diesem Wissen gemacht, wer erhält noch Kenntnis, wie lange wird das aufbewahrt und kann ich etwas dagegen tun. Mit der Einsicht in die Patientenakte möchte der Betroffene in Erfahrung bringen, wie es um seine Gesundheit bestellt ist. Die Informationen, ob und wie Daten gespeichert werden, sind in dieser Situation eher unrelevant.

Beide Rechte bestehen nach unserer Auffassung parallel nebeneinander. Der datenschutzrechtliche Auskunftsanspruch gem. § 17 KDG bzw. Art. 15 DS-GVO ist keine Rechtsgrundlage für eine Einsichtnahme in die Patientenakte.

4.2.2 Modalitäten bei Überlassung einer Kopie der Behandlungsunterlagen

Sofern der Patient sein Auskunftsbegehren allgemein stellt, ohne sich auf eine der genannten Regelungen zu beziehen, ergeben sich auch weitere Abgrenzungsprobleme.

a) Anspruch auf Überlassung in elektronischer Form?

Nach § 630g Abs. 2 BGB kann der Patient „elektronische Abschriften von der Patientenakte verlangen“. Es kann danach bei vorliegender elektronischer Behandlungsdokumentation sowohl ein Ausdruck als auch eine Kopie auf einem Datenträger überlassen werden.

Demgegenüber bestimmt § 17 Abs. 3 KDG ausdrücklich, dass die Datenkopie in einem gängigen elektronischen Format zur Verfügung zu stellen ist, wenn die betroffene Person den Antrag in elektronischer Form stellt. Die Überlassung einer physischen Kopie der Patientenakte (Akte in Papierform oder Ausdruck der elektronischen Akte) ist in diesen Fällen nur noch möglich, wenn der Patient damit ausdrücklich einverstanden ist. Diese Differenzierung wäre jedoch nur relevant, wenn man der Auffassung folgt, dass der Anspruch auf Einsicht in die Parientenakte überhaupt besteht.

b) Anspruch auf Übersendung?

Nach § 630g BGB können Patienten bei Anforderung einer Kopie der Patientenakte grundsätzlich nur verlangen, dass die Kopien zur Abholung bereitgehalten werden. Ein Anspruch auf Übersendung der Aktenkopie besteht danach grundsätzlich nicht. Nach § 630g Abs. 1 Satz 3 i. V. m. § 811 BGB ist der sog. Leistungsort der Einsichtnahme in die Behandlungsunterlagen grundsätzlich der Aufbewahrungsort der Dokumentation.

Dagegen könnte sich aus der DS-GVO bzw. aus dem KDG auch eine Verpflichtung zur Übersendung der angeforderten (elektronischen) Kopie der Behandlungsunterlagen ergeben. In § 17 Abs. 3 KDG ist geregelt, dass der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung ist, zur Verfügung stellt. Folgt man der Auffassung, dass das datenschutzrechtliche Auskunftsrecht auch die Einsicht in die Patientenakte umfasst, hätte der Betroffene einen Anspruch auf Übersendung der Patientenakte.

c) Kostentragung?

Eine zu § 630 g BGB abweichende Regelung besteht nach der DS-GVO und nach dem KDG auch für den Aspekt der Kostentragung für die angefertigten Kopien der Patientenunterlagen. Insoweit bestimmen § 10 Abs. 2 BO und § 630g BGB, dass Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben sind. Es wurden insoweit bislang erstattungsfähige Papierkosten in Höhe von 50 Cent pro Seite bzw. bei elektronischen Patientenunterlagen in Höhe der anfallenden Materialkosten als erstattungsfähig erachtet.[52]

Demgegenüber sieht § 17 Abs. 3 KDG grundsätzlich die kostenfreie Bereitstellung der Datenkopie vor; eine Kostentragungspflicht besteht danach nur bei Anforderung mehrerer Exemplare von Datenkopien ab dem zweiten Exemplar.

d) Auskunftsverweigerung

Auch hinsichtlich der Verweigerung der Einsicht in die Patientenakte ist zu differenzieren. Gem. § 630 g BGB kann die Einsicht verweigert werden,

52 LG München, 19.11.2008 - Az. 9 O 5324; Ratzel/Lippert, Kommentar zur Musterberufsordnung (MBO), 6. Auflage 2015, § 10 Rn. 20.

wenn der Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Eine vergleichbare Regelung enthält Art. 15 DS-GVO bzw. 17 KDG nicht. Eine Verweigerung ist nur aufgrund der in § 17 Abs. 6 KDG genannten Gründe möglich.

Fazit:

Zwei Regelungen, zwei Zielsetzungen. Ein Anspruch auf Einsicht in die Patientenakte oder Übersendung einer Kopie lässt sich aus § 17 KDG nicht begründen.

Im vergangenen Berichtszeitraum haben wir durch Beschwerden von Betroffenen beobachtet, dass Patienten statt des – kostenpflichtigen – Anspruchs auf Anfertigung von Abschriften aus der Patientenakte einen Anspruch auf kostenlose Zurverfügungstellung der Patientenakte auf der Grundlage von Art. 15 der Datenschutz-Grundverordnung (DS-GVO) bzw. § 17 KDG geltend machen.

Den Verantwortlichen haben wir unsere Rechtsauffassung dargelegt und mitgeteilt, dass wir in der Nichtübersendung von Patientenakten keinen Datenschutzverstoß sehen und wir auch derzeit nicht sanktionieren. Gleichzeitig erfolgte aufgrund der derzeitigen Rechtsunsicherheit jedoch der Hinweis auf die hierzu existierende Rechtsprechung der Zivilgerichte, die überwiegend einen Anspruch auf Kopie einer Patientenakte aus Art. 15 Abs. 3 DS-GVO bejaht.[53]

Zu berücksichtigen ist zudem, dass staatliche Gerichte Betroffenen eine Entschädigung wegen des Verstoßes gegen das Auskunftsrecht aus Art. 15 Abs. 1 DS-GVO zugesprochen haben. Das Arbeitsgericht Düsseldorf hat in seinem Urteil vom 05.03.2020 – 9 Ca 6557/18) dem Kläger eine Entschädigung wegen Verstoßes seines Arbeitgebers gegen das Auskunftsrecht aus Art. 15 Abs. 1 DS-GVO in Höhe von 5.000,00 € zugesprochen.

Im Ergebnis wird man insoweit die weitere Entwicklung der Rechtsprechung im Auge behalten müssen. Im Augenblick besteht jedenfalls insoweit keine Rechtssicherheit, sodass auch für die Richtigkeit der hier vertre-

53 LG Dresden, 29. 05 2020 - 6076/20

tenen Auffassung selbstverständlich keine Gewähr übernommen werden kann.

4.3 Unbefugte Offenlegung von Gesundheitsdaten – immer mal wieder!

Der Datenschutzaufsicht wurde in mehreren Fällen gemeldet, dass Patientenunterlagen, wie Arztbriefe, Entlassberichte, Rechnungen oder Zuzahlungsrechnungen an unbeteiligte Dritte versandt worden sind.

In einem Fall wurde gemeldet, dass in einem Kuvert neben dem Arztbrief eines Patienten auch eine Zuzahlungsrechnung eines anderen Patienten einer Dritten Person übersandt worden ist.

Gem. § 51 Abs. 1 i. V. m. § 47 Abs. 6 KDG kann die zuständige Datenschutzaufsicht eine Geldbuße verhängen, wenn der Verantwortliche oder ein Auftragsverarbeiter vorsätzlich oder fährlässig gegen Bestimmungen des KDG verstößt. In diesen Fällen hat der Verantwortliche gegen die Grundsätze der Verarbeitung personenbezogener Daten (§ 7 KDG) verstoßen. Der Verantwortliche hat ferner die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen nicht gewährleistet. In dem Arztbrief und auch in der fehlerhaft übersandten Rechnung sind personenbezogene Daten der besonderen Kategorie gem. § 4 Nr. 2 KDG enthalten. Derartige Gesundheitsdaten sind besonders schützenswert und damit vor unbefugtem Offenlegen durch geeignete technische und organisatorische Maßnahmen zu schützen.

Gem. § 7 Abs. 1 lit. f) und § 26 Abs. 1 S. 2 lit. b) KDG müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich Schutz vor unbefugter Verarbeitung. Diese liegt vor, wenn personenbezogene Daten Personen offengelegt werden, welche zur Einsichtnahme nicht berechtigt waren.

In einem anderen der Aufsicht gemeldetem Fall ist ein Arztbrief an den Ehemann einer Patientin herausgegeben worden, obwohl diese ausdrücklich bei der Aufnahme angeben hat, dass ihrem Ehemann keine Auskünfte zu erteilen sind. Begünstigt wurde dieser Datenschutzverstoß auch durch

die Tatsache, dass das von dem Klinikum verwendeten Krankenhausinformationssystem hinsichtlich der Eintragung von Auskunftserteilungswünschen der Patienten eine Opt-Out-Regelung vorsah. In der verwendeten Maske war vorgesehen, dass eingetragen werden konnte, welchen Personen keine Auskünfte erteilt werden dürfen, sog. Sperrvermerke. Die Eintragung eines Sperrvermerks für Ehepartner oder nahe Angehörige sah die Maske und auch die Datenschutzleitlinie jedoch nicht vor. Dies ist Ausfluss des Umstandes, dass angenommen worden ist, dass Ehepartnern und nahen Angehörigen generell Auskunft erteilt werden kann, wenn der Patient einer Auskunftserteilung nicht widersprochen hat. Bei der Frage, ob eine generelle aktive Benachrichtigung der Angehörigen eines Patienten erlaubt ist, muss beachtet werden, dass bereits allein die Auskunft über den Gesundheitszustand und mithin auch die Information darüber, dass eine Person im Krankenhaus liegt, eine Offenlegung personenbezogener Daten darstellt. Auch diese Information unterfällt der ärztlichen Schweigepflicht.

Unter dem Blickwinkel, dass ein Patient aufgrund seines Gesundheitszustandes möglicherweise nicht in der Lage ist seine Angehörigen über seinen Klinikaufenthalt zu informieren, könnte man u. U. davon ausgehen, dass eine mutmaßliche Einwilligung vorliegt. In einigen Bundesländern hat man diese Überlegung herangezogen und in den Landesgesetzen entsprechende Befugnisnorm festgeschrieben.[54] Keine Regelungen existieren hingegen zum Beispiel in Sachsen-Anhalt, Bayern, Schleswig-Holstein und Thüringen. Der Krankenhausträger kann sich hier nicht auf eine mutmaßliche Einwilligung berufen. Die nicht vorhandene Rechtskenntnis und die praktizierte Opt-Out-Regelung hat den Datenschutzverstoß ermöglicht.

Dass das Offenlegen von Gesundheitsdaten ein nicht unerhebliches Problem ist, zeigt sich auch in einem anderen der Aufsicht gemeldeten Fall, in dem ein Arztbrief, von einer Mitarbeiterin einer Klinik, an einen falschen Empfänger gefaxt worden ist. Eine Kontrolle der Fax-Nr. vor dem Versand erfolgte ebenso nicht, wie eine vorherige telefonische Ankündigung der Übersendung des Arztberichtes per Fax. Auch eine Kontrolle des Sendeberichtes ist nicht erfolgt. Der Fehlversand wurde von der Person, die den Arztbericht versehentlich erhalten hat, gemeldet. In diesem Fall kam

54 Exemplarisch zu nennen sind § 29 S. 1 Ziffer3 BbgKHEG, § 33 Abs. 3 LKHG M-V, § 24 Abs. 5 Ziffer 6 LKHG und § 33 Abs. 3 Ziffer 7 SächsKHG

erschwerend hinzu, dass der Verstoß nicht innerhalb der gesetzlich normierten Frist von 72 Stunden an die Aufsicht gemeldet worden ist. Im gemeldeten Fall konnte die Einrichtung nicht nachweisen, dass die Mitarbeiterin Kenntnis von den existierenden Datenschutzrichtlinien hatte und es offensichtlich deswegen zu der Datenschutzverletzung gekommen ist.

In allen Fällen wurden die Verstöße geahndet.

4.4 Meldungen nach dem Infektionsschutzgesetz an Gesundheitsämter per Fax - Forderung der Gesundheitsämter zur Übersendung von Entlassberichten von COVID-19 Patienten

Der Aufsicht war im Frühjahr 2020 zur Kenntnis gelangt, dass sich Gesundheitsämter mit Schreiben an Klinken in ihrer jeweiligen Region gewandt und diese aufgefordert haben, alle Entlassungsberichte von mit Corona-Viren infizierten Patienten per Fax zu übersenden.

Über ein Rundschreiben hat die Aufsicht alle in ihrem Zuständigkeitsbereich liegenden Kliniken darauf hingewiesen, dass sich aus dem Infektionsschutzgesetz keine Ermächtigungsgrundlage für diese Forderung ergibt. Dargelegt wurde zudem, dass sich Gesundheitsämter, sofern sie diagnostische Daten benötigen, direkt an die betroffene Person wenden müssen, da auch die bestehenden COVID-19 Pandemie die Klinik nicht von der ärztlichen Schweigepflicht entbindet. Die Persönlichkeitsrechte der Betroffenen sind auch in Zeiten der Pandemie zu wahren.

Eine Übermittlung von Patientendaten an die Gesundheitsämter ist nicht nur ein Verstoß gegen geltendes Datenschutzrecht, sondern zudem auch eine Verletzung von Privatgeheimnissen (§ 203 StGB) und mithin eine Straftat. Die Kliniken wurden davon in Kenntnis gesetzt, dass, sollten Patientendaten dann auch noch per Fax übermittelt werden, darin ein mindestens fahrlässiger Verstoß gegen Sicherungspflichten gesehen wird.

Von der Übersendung der Entlassungsberichte an Gesundheitsämter hat die Datenschutzaufsicht daher dringend abgeraten.

5 Datenschutz in Schulen

5.1 Datenschutzrechtliche Aspekte beim Homeschooling

Im Berichtsjahr 2020 war der Unterricht an den Schulen bedeutend durch Maßnahmen zur Eindämmung der Corona-Pandemie geprägt, welche wesentliche Veränderungen des gewohnten Schulbetriebs mit sich brachten.

Viele Schulen waren auf diese Situation nicht vorbereitet und auch die digitalen Möglichkeiten gerade zum Anfang der Pandemie wiesen große datenschutzrechtliche Mängel auf.

So gab es zwar bereits einige etablierte Systeme, die digitalen Unterricht möglich machten, jedoch fehlte es an Erfahrungen, die Bedienungsfehler oder andere Problematiken auslösten.

Unbeachtet blieb daneben auch die oft unzureichende technische Ausstattung der Familien, in denen die Schüler leben, sowie die langsamen Datenverbindungen in vielen Regionen. Daher war oft das Smartphone inklusive kostenloser Messanger das Instrument für den digitalen Unterricht. Dabei sind viele Messanger datenschutzrechtlich bedenklich. Nicht nur, weil diese keine Verschlüsselungstechnik anbieten oder ihren Sitz in den Vereinigten Staaten haben, sondern auch weil viele Dienste vor allem Metadaten erfassen und diese entsprechend auswerten.

Weiterhin gab es bis zum Ende des Berichtsjahres keine verbindlichen Anforderungen an Software oder Online-Lösungen und keine Datenschutzstandards oder erforderliche Sicherheitseinstellungen. Kinder und Jugendliche können die Risiken und Folgen einer Verarbeitung ihrer personenbezogenen Daten noch nicht abschätzen und sind deshalb besonders schützenswert.

Um den Kindern trotz aller Umstände Lernangebote zu unterbreiten, wurden auf Länderebene zahlreiche Handlungsempfehlungen herausgegeben und digitale Lernangebote etabliert. Eine Verbindlichkeit leitet sich daraus jedoch nicht ab.
Weiterhin werden und wurden die Schulen im Rahmen des Digitalpakts

Schule der Bundesregierung mit besserer digitaler Infrastruktur und Medien ausgestattet.
Trotz dieser neuen digitalen Medien darf dabei der Datenschutz nicht auf der Strecke bleiben, aber auch kein Hindernis sein.[55]

5.1.1 Digitale Möglichkeiten zur Vermittlung von Unterrichtsstoff

In diesem Abschnitt soll erklärt werden, welche digitalen und technischen Lösungen es gibt, Unterrichtsstoff im Rahmen eines Distanz- oder Hybridunterrichts zu vermitteln.

Der Begriff Distanzunterricht leitet sich aus dem Fernunterrichtsgesetz ab und bedeutet: „Vermittlung von Kenntnissen und Fähigkeiten, bei der der Lehrende und der Lernende ausschließlich oder überwiegend räumlich getrennt sind und der Lehrende oder sein Beauftragter den Lernerfolg überwachen."[56]

Der Lernprozess findet vorrangig in der häuslichen Umgebung statt und deshalb sollte die Lehrkraft regelmäßig mit dem Schüler in Verbindung stehen. Dazu sind digitale Kommunikationsmöglichkeiten sehr hilfreich.

Findet Hybridunterricht Anwendung, so werden der klassische Präsenzunterricht sowie der Digitalunterricht miteinander kombiniert, d.h. der Lernstoff wird im Klassenraum sowie auch zu Hause vermittelt.[57]

5.1.2 Lernplattformen

Eine Lernplattformen ist eine webbasierte Software, die Lerninhalte bereitstellt und organisiert. Dabei werden jedoch regelmäßig viele personenbezogene Daten von Schülern und Lehrern webbasiert verarbeitet. Aus diesem Grund müssen die Schulen als die für die Datenverarbeitung verantwortliche Stelle datenschutzrechtliche Anforderungen beachten.

55 Deutscher Bundestag Drucksache 19/25069
56 Vgl. Fernunterrichtsgesetz § 1 Abs. 1
57 Impulse und Empfehlungen für den Präsenz- und Distanzunterricht in Sachsen-Anhalt, Hrsg. LISA

Im Idealfall kann die Schule selbst auswählen, welche Module der virtuellen Lernumgebung sie nutzen möchte und welche Daten dabei verarbeitet werden.

Doch welche datenschutzrechtlichen Aspekte gibt es bei dem Einsatz von Lernsoftware zu beachten?

Jedem Benutzer ist ein eigenes Benutzerkonto zur Verfügung zu stellen indem jedem Schüler und jedem Lehrer ein persönlicher Registrierungsschlüssel zugewiesen wird. Dieser Prozess sollte von einem Administrator in der Form kontrolliert werden, dass ein Abgleich der zur Verfügung gestellten Benutzerkonten mit den tatsächlich angelegten Benutzerkonten vorgenommen wird. Somit kann zum einen ausgeschlossen werden, dass sich ein Schüler nicht registriert hat und somit die Lerninhalte auch nicht abrufen kann. Es kann aber auch festgestellt werden, ob sich Schüler oder auch Lehrer doppelt registriert und dadurch eine zweite Identität haben, die sie eventuell missbrauchen könnten.

Datenauswertungen durch den Anbieter der Lernplattform sind nur im Rahmen der Aufgabenwahrnehmung erlaubt. Diese müssen pseudonymisiert stattfinden. Auswertungen beispielsweise Lehrkräften oder Anbietern von Nachhilfe zur Verfügung zu stellen ist verboten.

Welche Auswertemöglichkeiten bestehen und welche personenbezogenen Daten in welcher Form verarbeitet werden, muss den Betroffenen (Nutzer der Lernplattform) sowie auch den Erziehungsberechtigten vorher mitgeteilt werden. Dazu bietet sich ein Informationsschreiben gemäß § 15 KDG an.

Um den Missbrauch des Benutzerkontos durch Dritte zu erschweren sowie auch Auswertungen nur pseudonymisiert vornehmen zu können, sollten die Nutzer neben ihren Benutzernamen einen Anmeldenamen vergeben können. Der Benutzername ist der reale Klarname und zur Identifikation des Schülers oder Lehrers erforderlich. Der Anmeldename als Pseudonym wird zusammen mit einem Passwort zur Anmeldung auf der Lernplattform verwendet.[58]

58 Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht - DSK

Die Pseudonymisierung stellt in diesem Bereich eine nach § 26 KDG geeignete Technische und Organisatorische Maßnahme dar, um die Eintrittswahrscheinlichkeit eines Datenschutzvorfalls deutlich zu minimieren.

Weiterhin ist festzulegen, wo die Inhalte der Lernplattformen, z.B. Aufgabenstellungen an die Schüler, die Lösungen der Schüler, Lernvideos etc. gespeichert werden. Die datenschutzrechtlich bestmögliche Variante ist, dass alle diese Dateien und Inhalte auf einem eigenen Schulserver gespeichert werden. Da aber nicht alle Schulen eigene Server haben, werden in diesem Zusammenhang auch Clouddienste genutzt, d.h. die Datenablage erfolgt nicht dezentral an der Schule, sondern in einer zentralen Cloud. Nach den Bestimmungen des Kirchlichen Datenschutzgesetzes muss die Verarbeitung und Speicherung von Daten ausschließlich auf dem Gebiet der europäischen Union oder innerhalb des europäischen Wirtschaftsraums stattfinden. Die Verarbeitung in einem Drittland darf nur stattfinden, wenn dort ein angemessenes Datenschutzniveau besteht. US-amerikanische Dienste sind daher nicht geeignet.

Die Schule bzw. die verantwortliche Stelle muss sich vor der Einführung einer Lernplattform Gedanken über ein Berechtigungskonzept der einzelnen Funktionalitäten machen. Ebenso müssen Zugriffsrechte festgelegt werden. Diese Regelungen sind schriftlich zu treffen.
Zudem sind die Lehrer sowie auch die Schüler im Umgang mit der Lernplattform zu schulen, um Anwendungsfehler zu vermeiden.

Mit dem Anbieter der Lernplattform ist ein Auftragsverarbeitungsvertrag abzuschließen, da der Anbieter personenbezogene Daten im Auftrag der Schule bzw. des Trägers (Verantwortlicher) verarbeitet. Der Vertrag muss die Anforderungen aus § 29 KDG Verarbeitung personenbezogener Daten im Auftrag erfüllen.

Datenschutzvorfälle im Zusammenhang mit Lernplattformen

Bedingt durch die Schulschließungen im Frühjahr 2020, haben sich vergleichsweise zügig Online-Lernplattformen im Schulleben etabliert. Da zu diesem Zeitpunkt noch Leitlinien bzw. Handlungsempfehlungen fehlten,

war die Beachtung der datenschutzrechtlichen Voraussetzungen für viele Schulen eine große Herausforderung.

So ist es an einigen Schulen passiert, dass Lehrer von einem Mailabsender, der als Verteilerliste für die Schüler der Klasse bestimmt war, andere Lehrer angeschrieben und sich nach Noten von Schülern erkundigt haben. Die angeschriebenen Lehrer haben diesen Fehler nicht bemerkt und haben den anfragenden Lehrern die Noten mitgeteilt indem sie direkt dem Mailabsender geantwortet haben. Somit bekamen alle Schüler dieser Klasse die E-Mail mit Noten zugesandt.

Zensuren von den Schülern vor der Klasse bekannt zu geben ist nicht zulässig. In der Regel werden die erteilten Zensuren vertraulich mitgeteilt und besprochen.

Dieser Verstoß zeigt auf, dass es vor Einführung einer Lernplattform Schulungen und Sensibilisierungsmaßnahmen geben muss. Auch der Umgang muss geübt werden und auf Gefahren hingewiesen werden. Die besten Datenschutzvorkehrungen bringen keinen Erfolg, wenn durch Anwendungsfehler Datenschutzvorfälle entstehen.

An einer anderen Schule bekamen die Eltern der Schüler von der Schule einen Registrierungsschlüssel, mit dem diese ihr Kind bei der Lernplattform anmelden konnten. Dieser Schlüssel war 7 Tage gültig und für alle Schüler derselbe. Eine weitere Verifizierung fand nicht statt. Dies hatte zur Folge, dass es vermutlich zu einem Identitätsmissbrauch kam. So wurden angeblich drei Accounts auf einen Schüler eingerichtet. Über diese Accounts wurden verbotene Inhalte versendet sowie Lehrer beleidigt.
Aufgrund dessen, dass keine weitere Verifizierung in diesem System stattfand und auch nicht überprüft wurde, wieviel Nutzer sich mit dem zur Verfügung gestellten Schlüssel registriert hatten, hat die Schule gegen die Pflicht technisch organisatorische Maßnahmen gemäß § 26 KDG zu etablieren verstoßen.

Vorkehrungen, mit denen Lernplattformen datenschutzfreundlicher gestaltet werden können:

✓	Die Antwort eines Schülers auf gestellte Aufgaben oder andere Unterlagen in Form von Uploads darf nur der Fachlehrer einsehen. Andere Fachlehrer und auch die Mitschüler haben hier keine Zugriffsrechte.
✓	Wenn es Diskussionsforen geben soll, ist zu klären, wer daran teilhaben soll. Empfehlenswert ist eine fachliche Leitung durch den Lehrer.
✓	Wenn Chats zwischen den Schülern erlaubt sind, so darf der Lehrer hier keinen Einblick bekommen.
✓	Auch Chats zwischen einem Schüler und einem Lehrer bedürfen höchster Vertraulichkeit.
✓	Zensuren dürfen nicht an einen Verteiler geschickt werden. Bewertungen sind jedem Schüler persönlich zu übersenden.
✓	Lehrkräfte dürfen nicht erkennen können wie oft und wie lange der Schüler die Lernplattform nutzt.
✓	Es werden nur die Tools freigegeben, die für die Schule bzw. zur Vermittlung von Lerninhalten erforderlich sind.
✓	Nur unbedingt notwendige Stammdaten der Schüler bzw. der Lehrer erfassen.
✓	Eigene Passwörter für jeden Nutzer verwenden, die nach der Registrierung vergeben oder geändert werden müssen.
✓	Regelungen zum Passwort-Verlust treffen.

5.1.3 Clouddienste

Clouddienste können Bestandteil der im vorherigen Punkt genannten Lernplattform sein, wenn in der Schule kein eigener Server zur Verfügung steht. Diese Dienste können aber auch allein genutzt werden, indem Unterrichtsstoff für die Schüler durch die Lehrer in eine Cloud geladen wird. Die Schüler bekommen eine Information, dass der Lernstoff in der Cloud zur Verfügung steht und können sich diesen auf ihr Endgerät herunterladen.

Datenschutzrechtlich sind die Clouddienste genauso zu handhaben wie Lernplattformen, d.h. es muss ein Auftragsverarbeitungsvertrag nach § 29

KDG geschlossen werden, es muss ein Berechtigungskonzept vorhanden sein, es müssen geeignete technische und organisatorische Maßnahmen gemäß § 26 KDG getroffen werden und die Betroffenen müssen nach § 15 KDG informiert werden, inwieweit ihre personenbezogenen Daten verarbeitet werden.

Ein Cloud-Dienst kann ferner auch das Hosting des E-Mail Clients sein. Auch in diesem Fall sind die gesetzlichen Bestimmungen zu beachten.

Vorzugsweise sind Cloud-Anbieter aus dem EU-Raum einzusetzen, da diese im Geltungsbereich der DS-GVO sind.

5.1.4 Interaktive Programme und Online-Anwendungen

Interaktive Programme werden als Web-Anwendungen oder als Apps genutzt. Dies hat den Vorteil, dass kein komplettes Programm installiert werden muss und somit kein Speicherplatz in Anspruch genommen wird. Nachteil ist, dass alle Anwendungen die Daten (auch Auswertungen) bei sich speichern können.

Diese Programme oder Apps werden z.B. von Schulbuchverlagen zur Verfügung gestellt, so dass der vermittelte Lernstoff zusätzlich geübt werden kann.

Interaktive Anwendungen werden bei Distanz- oder Hybridunterricht genutzt, indem die Schüler dort den gelehrten Unterrichtsstoff üben und vertiefen können. Außerdem bieten viele Anwendungen durch Auswertungen auch eine Lernkontrolle für die Schüler an.
Zudem gibt es auch Online-Apps, die von Schulen eingesetzt werden, um Schülern Aufgaben zu übermitteln. Diese Aufgaben können innerhalb dieser Anwendung gelöst werden. Die Ergebnisse sind somit auch für die Lehrkräfte einsehbar.

Ergebnisse und Auswertungen, die einer bestimmten Person zugeordnet werden können, sind aus datenschutzrechtlicher Sicht mit Vorsicht zu betrachten. Eine Zuordnung ist auch mit einer Online-Kennung oder einer IP-Adresse möglich.

Nutzt der Lehrer die Ergebnisse ausschließlich für die Lernzielkontrolle, so ist aus datenschutzrechtlicher Sicht nichts dagegen einzuwenden, wenn

ausreichende technische und organisatorische Maßnahmen i.S.v. § 26 KDG für den Lehrer sowie auch für die Anwendung getroffen wurden.

Ebenfalls sind auch bei diesen Anwendungen die in den vorherigen Abschnitten genannten Regelungen einzuhalten sowie die Betroffenen über die von Ihnen verarbeiteten personenbezogenen Daten zu informieren.

5.1.5 Audio- und Videokonferenzen

Im Rahmen der Corona-Pandemie ist ein Präsenzunterricht vielfach nicht möglich. Um die Inzidenzzahlen zu drücken, werden geteilter Unterricht und die Teilnahme am Unterricht mit Hilfe von Videokonferenzsystemen vorgeschlagen.

Aufgrund dieser Situation wurde unsere Dienststelle im Berichtszeitraum häufig angefragt, ob die Nutzung von Videokonferenzsystemen für Webmeetings oder für den Schulunterricht datenschutzrechtlich zulässig ist bzw. welche Systeme Verwendung finden dürfen.

Eine Produktempfehlung, auch für andere Anwendungsbereiche, können wir in unserer Funktion als Datenschutzaufsicht nicht abgeben. Ob eine Anwendung datenschutzrechtlich unbedenklich ist, lässt sich schon auf Grund der unterschiedlichen Anwendungsfälle sowie der Informationen die darüber verarbeitet und/oder ausgetauscht werden, pauschal nicht beantworten.

Idealerweise steht der Schule oder dem Schulträger eine vom Land bereitgestellte Videokonferenz Plattform oder Lernplattform mit integrierter Videofunktion zur Verfügung. Wenn der Anbieter dann noch aus Deutschland oder der EU kommt und mit der Schule oder dem Träger einen Auftragsdatenverarbeitungsvertrag abschließt, hat die Schule zahlreiche Möglichkeiten zu bestimmen, wie die Daten verarbeitet werden oder wie lange und wo sie gespeichert bleiben.[59]

Weiterhin muss die Datenübertragung verschlüsselt erfolgen und die Konferenzen (Videounterricht) können nur vom Moderator (Lehrer) gestartet werden.

59 https://datenschutz-schule.info/2020/05/03/teilnahme-am-unterricht-ueber-video-geht-das/

Trotz aller datenschutzfreundlichen Maßnahmen, die vom Anbieter oder der Einrichtung vorab eingestellt werden können, sind auch die Anwender (Lehrer und Schüler, ggf. Erziehungsberechtigte) über Möglichkeiten zu informieren, die zu einer datenschutzfreundlichen Gestaltung beitragen.

Während der Teilnahme am Videounterricht von zu Hause aus werden Aufnahmen der privaten Wohnung erstellt, die als Mittelpunkt privater Lebensgestaltung grundrechtlich geschützt sind. Die Einrichtung der Wohnung, das Zusammenleben mit anderen Personen, die Ausübung von Hobbies in privaten Räumen – all das ist privat und persönlich. Es handelt sich um Informationen, die sich auf eine identifizierte Person beziehen und Merkmale der wirtschaftlichen, kulturellen oder sozialen Identität darstellen. Es handelt sich also um personenbezogene Daten i. S. v. § 4 Nr. 1 KDG, teilweise auch um besondere Kategorien personenbezogener Daten i. S. v. § 4 Nr. 2 KDG.

Um diese verarbeiten zu dürfen, bedarf es einer gesetzlichen Grundlage gem. § 6 Abs. 1 KDG. Von den dort aufgeführten Bedingungen kommt nur lit. b), eine Einwilligung des/der Betroffenen, in Betracht. Erforderlich für eine Einwilligung ist, dass sie freiwillig abgegeben wird. Daran fehlte es, hätte der Schüler nur die Möglichkeit, die Kamera und das Mikrofon aktiv zu schalten oder aber nicht am Unterricht teilnehmen zu können. Nach § 7 Abs. 1 lit c) KDG müssen personenbezogene Daten dem Zweck angemessen und auf das für den Zweck erforderliche Maß beschränkt sein. Für den Zweck, die Vermittlung des Unterrichtsstoffes, ist es nicht erforderlich, Bildaufnahmen von Schülern in den Klassenraum zu übertragen. Erst recht ist es nicht erforderlich, Aufnahmen aus dem persönlichen Lebensbereich des Schülers in den Klassenraum zu übertragen. Schülern muss die Möglichkeit eingeräumt werden, die Bildübertagung auszuschließen oder nach Belieben zu unterbrechen, um eine rechtmäßige Freiwilligkeit zu gewährleisten. Das gleiche gilt, wenn der Unterricht ausschließlich über Videokonferenzsysteme organisiert wird. Auch in diesem Fall müssen Schüler entscheiden können, ob ihr Bild an den Lehrer übertragen werden soll.

Ähnlich ist die Bewertung, wenn die Kameraausrichtung so gewählt ist, dass die Bilder der im Klassenraum anwesenden Schüler nach außen übertragen werden. In einem solchen Fall werden mit der Übertragung

von Bildern des Einzelnen auch personenbezogene Daten gem. § 4 Nr. 1 KDG übertragen. Auch hierfür gibt es keine Erforderlichkeit, da es für die Zweckerreichung völlig ausreichend ist, dass der Lehrer im Fokus der Kamera steht und dessen Bild übertragen wird.

In jedem Fall sind die Schüler darauf hinzuweisen, dass von Bild und Ton keine Aufzeichnungen gemacht werden dürfen und ein Verstoß gegen diese Regelung ggf. strafrechtlich verfolgt werden kann.

5.2 Datenverarbeitung durch Lehrkräfte (im häuslichen Bereich)

Nach den einschlägigen Schulgesetzen der Länder dürfen Lehrer nur in begründeten Fällen personenbezogene Daten der Schüler außerhalb der Schule verarbeiten. Dabei bedarf es zum einen der Erlaubnis durch den Schulleiter und zum anderen der Einhaltung des Datenschutzes.

Da Lehrkräfte üblicherweise nicht nur den Arbeitsplatz in der Schule, sondern auch zu Hause einen Arbeitsplatz unterhalten, verarbeiten sie regelmäßig personenbezogenen Daten der Schüler zu Hause, so dass es einiges zu beachten gibt.

5.2.1 Übermittlung von personenbezogenen Daten via E-Mail / Messenger

E-Mails stellen mittlerweile im Schulalltag ein wichtiges Kommunikationsinstrument dar. Besonders in der Pandemie-Zeit hat aber die Bedeutung dieser Kommunikation nochmal erheblich zugenommen.
So lange Unterrichtsmaterial ohne Personenbezug (z.B. Arbeitsblätter oder Übungen) übermittelt wird, ist das ganze eher unproblematisch. Wird aber beispielsweise eine Rückmeldung zum Arbeitsergebnis gegeben, so werden bereits personenbezogene Daten i.S. v. § 4 Nr. 1 KDG verarbeitet.

Beim Übermitteln von personenbezogenen Daten müssen sichere Übertragungswege genutzt werden, so dass die E-Mails entweder verschlüsselt werden oder innerhalb einer sicheren Domain versendet werden müssen.

Das Hauptproblem bei einer sicheren Verschlüsselung ist, dass Sender und Empfänger die gleichen Schlüssel nutzen müssen, damit die vom Sender verschlüsselte E-Mail beim Empfänger entschlüsselt und gelesen werden kann.
Einfacher ist daher die Verwendung einer Domain. Alle Nutzer (Schüler, Lehrer) befinden sich dann in einem geschlossenen Netzwerk und alle E-Mails werden von einem E-Mail Server gesendet und empfangen. Sind dann die Kontoeinstellungen der entsprechenden E-Mail Clients (z.B. Outlook) beim Senden und Empfangen gesichert, so können über diesen Weg personenbezogene Daten sicher versendet werden.

Wenn aber Eltern oder andere Stellen mit der Schule bzw. einem Lehrer über E-Mail kommunizieren möchten, so nutzen diese selten die gleiche Domain, so dass bei einem Austausch von personenbezogenen Daten zusätzliche Maßnahmen getroffen werden müssen. Beispielsweise können die Dokumente, die personenbezogenen Daten enthalten, über ein ZIP Archiv versendet werden, welches mit einem Passwort gesichert ist. Das Passwort sollte über einen anderen Kommunikationsweg, z.B. per Telefon oder mündlicher Bekanntgabe in einem Gespräch übermittelt werden.

Den Lehrern eine dienstliche E-Mailadresse einer schul- oder trägereigenen Domain zur Verfügung zu stellen hat zudem den Vorteil, dass private und dienstliche E-Mail-Nutzung strikt getrennt werden können.

Untersagt ist auch die dienstliche Kommunikation über Messanger-Dienste oder soziale Netzwerke mit den Schülern oder Eltern sowie der Lehrer untereinander, die ihre Daten außerhalb des Gebiets des Europäischen Wirtschaftsraums und der Schweiz speichern sowie keine Verschlüsselung anwenden.

Alternativ kann dazu die dienstliche E-Mail-Adresse genutzt werden oder der Nachrichten-Chat vieler etablierter und sicherer Lernplattformen.

Weiterhin ist bei der Verwendung von E-Mail Verteilerlisten darauf zu achten, dass die Empfänger immer im Bcc Feld einzutragen sind, damit bei den Empfängern keine Mailadressen außer der des Absenders angezeigt werden. Diese Form des Versendens wird häufig von Klassenlehrern genutzt, die den Eltern allgemeine Informationen übermitteln möchten.

Im Rahmen der Kommunikation unter den Lehrern darf eine Nachricht auch an mehrere Lehrer im „An“ oder „Cc“ Feld gesendet werden, sofern dienstliche E-Mail-Adressen genutzt werden und keine persönlichen Informationen zu einer bestimmten Person übermittelt werden.

5.2.2 Arbeitsplatzgestaltung im häuslichen Bereich

Der Arbeitsplatz zu Hause muss so gestaltet sein, dass ein unberechtigter Dritter nicht zufällig personenbezogene Daten einsehen kann. Unberechtigte Dritte können auch die eigenen Familienangehörigen, Mitbewohner oder Besucher sein. Idealerweise ist das Arbeitszimmer verschließbar. Mindestens sollte jedoch ein verschließbarer Schrank vorhanden sein.

Personenbezogene Daten sind in diesem Fall auch Klassenarbeiten oder Hausarbeiten, die durch den Lehrer zu Hause korrigiert werden.

5.2.3 Nutzung von privaten IT-Geräten

Die Nutzung privater IT-Geräte zu dienstlichen Zwecken ist nach § 20 Abs. (1) KDG-DVO unzulässig.

Werden trotzdem private IT-Geräte zur Verarbeitung von Schülerdaten genutzt, so sind umfangreiche technische und organisatorische Maßnahmen zu treffen, um jeden unbefugten Zugriff, z.B. die Mitnutzung durch Familienangehörige, zu verhindern. Die Verwendung von privaten IT-Geräten ist von dem Schulleiter schriftlich zu genehmigen. Die Genehmigung muss mindestens die Regelungen aus § 20 Abs. (2) KDG-DVO beinhalten.

Empfohlen werden kann beispielsweise die Nutzung von verschlüsselten USB-Sticks. Dadurch lassen sich die privaten und dienstlichen Daten einfach trennen.

5.2.4 Maßnahmen zur Vermeidung eines Datenschutzvorfalls

Der Verantwortliche muss durch geeignete Maßnahmen dafür sorgen, dass die Sicherheit der Verarbeitung gewährleistet bleibt. Alle damit ver-

bundenen personenbezogene Daten von Schülern sind demzufolge im Distanzunterricht genauso zu schützen wie in der schulischen Einrichtung. Damit das Datenschutzniveau eingehalten werden kann, sind geeignete Technische und Organisatorische Maßnahmen zu ergreifen, welche u.a. im Verzeichnis von Verarbeitungstätigkeiten dokumentiert werden müssen (§ 31 KDG). Um welche Maßnahmen es im Detail geht, ist in der KDG-DVO unter dem Kapitel 3 aufgeführt. Hier einige weitere Hinweise:

Zur Vermeidung eines Datenschutzvorfalls ist bei der Verarbeitung personenbezogener Daten und der Organisation der technischen und den organisatorischen Maßnahmen unbedingt darauf zu achten, dass alle Familienangehörigen - auch die Eltern - unberechtigte „Dritte" sind. Das bedeutet, dass auch zu Hause Sicherheitsmaßnahmen getroffen werden müssen und alle damit verbunden Unterlagen, Notebook, etc. nach einem „Remote-Unterricht" in verschlossenen Schränken oder Räumen aufbewahrt werden.

Unterlagen mit personenbezogenen oder sicherheitsrelevanten Informationen dürfen weder zu Hausen noch in der Einrichtung im Hausmüll entsorgt werden. Diese müssen ordnungsgemäß vernichtet werden.

Eine wichtige proaktive organisatorische Maßnahme ist die Sensibilisierung und Aufklärung zum Umgang mit den Medien, die verwendet werden sollen. Dafür sollte ein festes Team als Ansprechpartner definiert werden, an das sich Schüler u.a. auch bei Auffälligkeiten wenden können. Eine solche Auffälligkeit wäre beispielsweise ein Verdacht auf einen Computervirus oder ungewöhnliche Chat-Inhalte.

Private Systeme sollten für einen schulischen Unterricht nicht in Frage kommen. Für den Fall das keine betrieblichen (schulischen) Geräte zur Verfügung stehen, so ist auf eine Trennung zwischen einem schulischen Profil und dem privaten Profil zu achten. Bei einem Windows-System wäre dies durch unterschiedliche Anmeldungen möglich, da dadurch in der Dateistruktur unter „Eigene Dateien" auf die Dateien des jeweiligen Benutzers (Profil) zugegriffen werden kann. Aber auch hier liegt die Gefahr darin, dass der Besitzer des Systems auf die anderen Profil-Daten zugreifen kann.

Eine andere technische Möglichkeit wäre die Ausgabe verschlüsselbarer USB-Datenträger an Lehrer und Schüler. Damit könnten alle betrieblichen (schulischen) Daten auf dem USB-Datenträger gespeichert werden. Zusätz-

lich bringt das den Vorteil, dass die Schüler diesen Datenträger auch später noch als „Transfer-Datenträger“ verwenden können.

Die abschließende Übersicht stellt einige wesentliche Maßnahmen zusammen, die zur Vermeidung eines Datenschutzvorfalls beitragen:

✓	Kennwortschutz beim IT-Gerät
✓	Regelmäßige Datensicherung
✓	Regelmäßige Updates beim Betriebssystem, der Firewall und dem Virenscanner
✓	Bildschirmsperre auch bei kurzen Abwesenheiten aktivieren, Entsperrung mit Passwort
✓	Festplattenverschlüsselung für mobile Geräte wie Laptops oder Notebooks
✓	USB Ports an Dienstgeräten sperren
✓	Verschlüsselte USB Sticks nutzen, wenn keine dienstlichen Geräte zur Verfügung stehen
✓	Verschlüsselten Datentransfer organisieren
✓	Berechtigungen und Nutzerprofile vergeben
✓	Nutzung von öffentlichen WiFi-Hotspots untersagen
✓	Datenschutzfolie verhindert ungewollte Einblicke
✓	Daten (auch Unterlagen) auf dem Weg nach Hause schützen
✓	nur notwendige Unterlagen mit nach Hause nehmen (so wenig wie möglich)
✓	Betriebliche Unterlagen nicht im privaten Hausmüll entsorgen
✓	Arbeitszimmer verschließen oder IT-Geräte und Unterlagen wegschließen
✓	Dienstliche Gespräche nicht in der Öffentlichkeit und vor anderen Zuhörern führen
✓	zum Umgang mit E-Mails belehren und sensibilisieren
✓	zur Vertraulichkeit auf das Datengeheimnis sensibilisieren

5.3 Aus der Praxis – Datenschutzthemen an Schulen

5.3.1 Aufnahmebögen / Bewerbungsverfahren

Im Rahmen von anlasslosen Datenschutzüberprüfungen in Form von Befragungen sowie wenigen Vor-Ort-Terminen an Katholischen Schulen konnten wir feststellen, dass die verwendeten Aufnahmebögen in den Bewerbungsverfahren weitaus mehr Daten abfragen, als für die reine Bewerbung erforderlich sind.

So werden regelmäßig noch die Berufe, die Geburtsdaten und Konfessionen der Eltern sowie umfangreiche Kontaktmöglichkeiten der Eltern im Aufnahmeantrag abgefragt. Weiterhin waren in einigen Aufnahmeanträgen Angaben zur Krankenkasse und zur zugehörigen Pfarrgemeinde zu machen. Ausnahmslos sind dies alles personenbezogene Daten i. S. v. § 4 Nr. 1 KDG, die eine gesetzliche Grundlage gem. § 6 Abs. 1 KDG für ihre Verarbeitung erfordern. Auch das alleinige Erfassen stellt ein Verarbeiten i. S. v. § 4 Nr. 3 KDG dar.

Einige Verantwortliche wollten darauf abstellen, dass diese Angaben doch als „freiwillige Angaben" gekennzeichnet sind und von den Erziehungsberechtigten nicht gemacht werden müssen. Gibt es dann aber nicht doch einen Vorteil im Aufnahmeprozess für diejenigen, die diese Angaben trotz Freiwilligkeit gemacht haben?

Auch Passfotos sind für den reinen Aufnahmeantrag nicht erforderlich, da gerade Fotos weitaus mehr personenbezogene Daten als nur das bloße Aussehen enthalten.[60] Jedoch können Fotos nach den durchgeführten Bewerbungs- oder Aufnahmegesprächen eine Gedankenstütze sein, wenn es darum geht im Nachhinein auszuwählen, wer von der Schule aufgenommen wird. Dafür ist es jedoch ausreichend, wenn das Foto zu diesem Gespräch mitgebracht wird.
Gleiches gilt für die Kopie der Geburtsurkunde, des Taufzeugnisses und eventueller Schulzeugnisse. Diese Dokumente enthalten eine Menge per-

60 3. Tätigkeitsbericht KDSA Ost 2018, S.45, Pkt. 6.2 Fotos

sonenbezogener Daten, deren Erfassung erst mit einem Schuleintritt erforderlich wird.

Bisher gab es an vielen Katholischen Schulen nur ein Formular zur "Anmeldung". Dieser als Aufnahmeantrag bezeichnete Fragebogen wurde sowohl als Bewerbungsformular als auch als Schulaufnahmeantrag verwendet. Da aber für die reine Bewerbung auf einen Schulplatz weitaus weniger Daten notwendig sind als für die tatsächliche Aufnahme, wurde seitens unserer Dienststelle die Empfehlung ausgesprochen einen Bewerbungsbogen zu entwickeln. Mit dem Bewerbungsbogen können dann die für die Bewerbung erforderlichen Daten abgefragt werden.
Erlaubt ist damit beispielsweise Daten zu Geschwisterkindern abzufragen, wenn diese bereits die Schule besuchen. Daten zu allen Geschwisterkindern abzufragen und Angaben zu deren Schulen zu machen ist jedoch nicht erforderlich.
Weiterhin ist auch gestattet abzufragen, ob sonderpädagogischer Förderbedarf oder eventuell gesundheitliche Beeinträchtigungen bestehen, wenn die Schulen dieses aus Kapazitätsgründen berücksichtigen müssen oder konzeptionelle Belange dies erfordern.

Ähnliches gilt auch für die Angabe zur Konfession des Kindes. Verlangt die Konzeption der Schule eine bestimmte konfessionelle oder ökumenische Ausrichtung, kann diese Angabe über das Kind mit abgefragt werden.

Aufgrund dieser Ausführungen ist jeder Verantwortliche (Schulleiter oder Schulträger) angehalten für seinen Bewerbungsprozess angepasste Formulare zu erstellen, damit zukünftig nur die für eine Bewerbung erforderlichen Angaben zu einem Kind bzw. seinen Erziehungsberechtigten gemacht werden müssen und ein unbewusstes Profiling aufgrund anderer unnötiger Angaben nicht stattfinden kann.

5.3.2 Aufbewahrungsfristen / Akteneinsicht Klausuren

Darf eine Schule bzw. ein Träger einer Schule einer ehemaligen Schülerin nach Ablauf der Aufbewahrungsfrist die Einsichtnahme und Herausgabe ihrer Abiturklausuren verweigern? Mit diesem Anliegen hatte sich eine Petentin an uns gewandt, da ihr dies verwehrt bleiben sollte.

Bei Abschlussklausuren bzw. Prüfungsarbeiten handelt es sich um personenbezogene Daten gem. § 4 Nr. 1 KDG. Diese Daten sind beim Verantwortlichen zu löschen, wenn dieser sie nicht mehr benötigt. Abschlussarbeiten werden vom Verantwortlichen, also der Schule bzw. dem Träger, nicht mehr benötigt, wenn die Aufbewahrungsfrist nach dem jeweils einschlägigen Schulgesetz bzw. der Schuldatenverordnungen abgelaufen ist.

Den Anspruch auf Löschung der Daten im Sinne von § 19 KDG kann der Verantwortliche auch durch Aushändigung der Prüfungsarbeiten an die Betroffene erfüllen.

Das Auskunftsrecht sowie das Recht auf Einsichtnahme über die gespeicherten Daten zu einer Person haben nach den entsprechenden Schulgesetzen die Schülerinnen und Schüler sowie die Erziehungsberechtigten. Sind die Schülerinnen bzw. Schüler volljährig, so haben nur noch diese ein Auskunftsrecht. Gegenüber den Erziehungsberechtigten ist dann keine Auskunft mehr zu erteilen, es sei denn die Schülerinnen bzw. Schüler haben ihre Einwilligung explizit erteilt.

In diesem Fall wurde der Petentin mitgeteilt, sich mit dem Schulträger in Verbindung zu setzen. Da die Aufbewahrungsfrist der Abschlussprüfung noch nicht abgelaufen war, steht einer Einsichtnahme nichts entgegen. Weiterhin kann die Petentin auch die Herausgabe ihrer Abschlussprüfung nach Ablauf der Aufbewahrungsfrist beantragen.

5.3.3 Befreiung von Mund-Nasen-Bedeckung

Im Berichtszeitraum erreichte unsere Dienststelle eine Beschwerde darüber, dass ein Attest zur Befreiung zum Tragen einer Mund-Nasen-Bedeckung ohne Erlaubnis der Betroffenen von einer Schule an ein Gesundheitsamt geschickt wurde.

In diesem Fall hat die Betroffene der Schulleitung ein ärztliches Attest vorgelegt, aus welchem hervorging, dass sie von der Verpflichtung einen Mund-Nasen-Schutz zu tragen befreit sei. Neben dieser Aussage enthielt das Attest keine weiteren Ausführungen zur Begründung dieses Attestes.

Um aus medizinischen Gründen von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung ausgenommen zu sein, müssen nach der für diese Schu-

le maßgeblichen Infektionsschutz-Maßnahmenverordnung gesundheitliche Beeinträchtigungen vorliegen, aufgrund derer keine Mund-Nasen-Bedeckung getragen werden kann. Das bedeutet, dass das Tragen einer Mund-Nasen-Bedeckung mit dem Risiko einer erheblichen Verschlechterung der Gesundheit der Patientin oder des Patienten verbunden sein muss, um von der Pflicht zum Tragen einer solchen befreit zu sein.

Aus einem ärztlichen Attest zur Ausnahme von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung muss sich nachvollziehbar mindestens ergeben, auf welcher Grundlage die ausstellende Ärztin oder der ausstellende Arzt ihre oder seine Diagnose gestellt hat und wie sich die Krankheit im konkreten Fall darstellt.[61]

Dabei ist die rechtliche Situation nicht vergleichbar mit der Vorlage einer Arbeitsunfähigkeitsbescheinigung gegenüber einem Arbeitgeber. Vorliegend ist Ziel der Betroffenen, mithilfe der ärztlichen Bescheinigung einen rechtlichen Vorteil zu erwirken, nämlich die Erteilung einer Ausnahmegenehmigung. In derartigen Konstellationen muss die Verwaltung - hier die Schulleitung - aufgrund konkreter und nachvollziehbarer Angaben in den ärztlichen Bescheinigungen, in die Lage versetzt werden, das Vorliegen der jeweiligen Tatbestandsvoraussetzungen selbständig zu prüfen.[62]

Nach der Schilderung der Schulleitung ist von der Betroffenen ein Attest vorgelegt worden, welches sie ausschließlich allgemein von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung befreite, ohne weitere, diese Ansicht begründende Ausführungen zu enthalten.

Daher entsprach das vorgelegte Attest nicht den gesetzlichen Anforderungen.

Die Rechtsfolgen eines solchen unzureichenden Attestes, welche sich aus den entsprechenden Infektionsschutzmaßnahmenverordnungen ergeben, wäre der Betroffenen, die ein unzureichendes Attest vorlegt, zunächst der Zutritt zur Schule zu verweigern.

61 VG Neustadt an der Weinstraße, 10.09.2020 - 5 L 757/20.NW; OVG Münster, 24.09.2020, - 13 B 1368/20
62 OVG Nordrhein-Westfalen, 24.09.2020.- 13 B 1368/20; VG Neustadt, 10.09.2020.- 5 L 757/20.NW; VG Würzburg, 16.09.2020.- W 8 E 20.1301

Selbst wenn man sich vergewissern wollte, ob das Attest tatsächlich nicht den Anforderungen entspricht, ist eine Übersendung der personenbezogenen Daten an das Gesundheitsamt nicht erforderlich. Die pseudonymisierte Übertragung an das Gesundheitsamt reicht für die Erreichung des Zwecks aus.

Da der Verantwortliche – hier die Schulleitung – personenbezogene Daten besonderer Kategorie gem. § 4 Nr. 1 und Nr. 2 KDG verarbeitet hat, ohne dass dafür eine Rechtsgrundlage gem. § 6 Abs. 1 und § 11 Abs. 2 KDG vorgelegen hat, war die Verarbeitung rechtswidrig.

Dessen ungeachtet sind die Infektionsschutzmaßnahmen an den Schulen sowie die Anforderungen an Atteste zur Befreiung zum Tragen einer Mund-Nasenbedeckung für Schüler in jedem Bundesland anders geregelt. Teilweise gibt es sogar Schulen-Coronaverordnungen wie beispielsweise in Schleswig-Holstein.

Daher ist immer explizit zu ermitteln, welche Regelungen es in den einzelnen Infektionsschutz-Maßnahmen zu beachten gibt. Dort sind die Anforderungen an Atteste sowie die Verfahrensweise, wenn Atteste die Anforderungen nicht erfüllen, geregelt.

Weiterhin ist auch zu beachten, dass an Atteste für Arbeitsnehmer andere Anforderungen gestellt werden können, nachzulesen im Abschnitt 6.1.1. in diesem Bericht.

6 Datenschutz im Beschäftigtenverhältnis

6.1 Datenschutz im Zusammenhang mit der Pandemiebekämpfung

6.1.1 Datenschutzrechtliche Fragestellungen zum Tragen einer Mund-Nasen-Bedeckung am Arbeitsplatz

Im Zusammenhang mit der Covid-19 Pandemie sind verschiedene Maßnahmen vorgesehen, die in die persönlichen Freiheiten des Einzelnen eingreifen. Dies ist zunächst grundsätzlich gerechtfertigt, wenn eine Gü-

terabwägung ergibt, dass der Eingriff in die Freiheitsrechte des Einzelnen hinter der Bekämpfung der Pandemie und damit hinter den Gesundheitsinteressen der Gesellschaft zurückstehen muss. Der Eingriff in die Freiheit des Einzelnen ist jedoch nur solange gerechtfertigt, wie dies erforderlich ist. Damit verlieren Arbeitnehmer den Schutz ihrer personenbezogenen Daten nicht komplett.

1. Darf der Arbeitgeber das Tragen einer Mund-Nasen-Bedeckung anordnen?

Der Arbeitgeber ist zur Einführung einer Pflicht zum Tragen einer Mund-Nasen-Bedeckung in der Einrichtung grundsätzlich aufgrund seiner Fürsorgepflicht gem. § 618 BGB berechtigt. Bei dieser Vorschrift handelt es sich um eine Teilausprägung der allgemeinen arbeitsvertraglichen Fürsorgepflicht, die ihrerseits wiederum Ausprägung der sich aus § 241 Abs. 2 BGB ergebenden allgemeinen Pflicht jedes Vertragspartners zur gegenseitigen Rücksichtnahme ist.[63] Der Arbeitgeber muss daher für seine Arbeitnehmer Schutzmaßnahmen etablieren, die durch die öffentlich-rechtlichen Arbeitsschutzvorschriften konkretisiert werden.

Die Rangfolge der Schutzmaßnahmen ergibt sich auch für Maßnahmen des betrieblichen Infektionsschutzes aus den Grundsätzen des § 4 ArbSchG.

Die in § 4 ArbSchG normierten Grundsätze zum Gesundheitsschutz der Beschäftigten sind auch für Maßnahmen des betrieblichen Infektionsschutzes zu beachten.

Demnach haben technische Maßnahmen Vorrang vor organisatorischen Maßnahmen und diese wiederum Vorrang vor personenbezogenen Maßnahmen. Die verschiedenen Maßnahmen sind sachgerecht miteinander zu verknüpfen (§ 4 Abs. 4 ArbSchG). Welche dieser Maßnahmen in der konkreten betrieblichen Situation sinnvoll und angezeigt sind, ist abhängig von der Beurteilung der vor Ort bestehenden Gefährdungen.[64] Sofern technische und organisatorische Schutzmaßnahmen die Gefährdung einer Infektion bei der Arbeit nicht minimieren können, sind individuelle Schutzmaßnahmen zu treffen, die auch die Pflicht zum Tragen einer Mund-Nasen-Bedeckung umfassen können.

63 Henssler, in MüKoBGB, 8. Auflage 2020, § 618 Rn. 1 ff.
64 „SARS-CoV-2-Arbeitsschutzregel" Punkt 4.1 (Fassung 18.12.2020)

So ist der Arbeitgeber bei Vorliegen der entsprechenden Voraussetzungen berechtigt, das Tragen einer Mund-Nasen-Bedeckung aufgrund seines Direktionsrechtes anzuordnen.[65] Das Mitbestimmungsrecht des Betriebsrates gem. § 36 Abs. 1 Nr. 10 MAVO ist dabei zu beachten.

2. Befreiung von der Verpflichtung durch Attest

Mitarbeitende, die aus gesundheitlichen Gründen gehindert sind eine Mund-Nasen-Bedeckung zu tragen, müssen dies durch ein ärztliches Attest nachweisen.

Die ärztliche Bescheinigung, eine Mund-Nasen-Bedeckung aus medizinischer Sicht nicht tragen zu können, wird in der Regel nicht zu einer Arbeitsunfähigkeit führen. Der Arbeitnehmer wird seine geschuldete Tätigkeit regelmäßig weiter ausüben können, jedoch ohne dabei der arbeitgeberseitigen Verpflichtung eine Mund-Nasen-Bedeckung zu tragen nachzukommen. Dennoch wird man dem ärztlichen Attest, durch welches eine „Maskenunverträglichkeit" attestiert wird, einen vergleichbar hohen Beweiswert zumessen müssen, wie der Arbeitsunfähigkeitsbescheinigung. Um diesen Beweiswert zu erschüttern, muss der Arbeitgeber Umstände darlegen und beweisen, die zu ernsthaften Zweifeln an der Arbeitsunfähigkeit Anlass geben.[66] Der Beweiswert eines ärztlichen Attestes kann aber nicht allein deshalb bestritten werden, weil darin ohne weitere Ausführungen eine Befreiung von der Tragepflicht einer Mund-Nasen-Bedeckungen jeglicher Art attestiert wird.[67] Auch in einem ärztlichen Attest zur Arbeitsunfähigkeit wird lediglich die Arbeitsunfähigkeit des Arbeitnehmers attestiert, ohne nähere Angaben dazu, worauf diese beruht.

Soweit die Gerichte bei Attesten zur Mund-Nasen-Bedeckung anders urteilen, beruht dies -zumindest teilweise- auf der Unterstellung, dass bei einer Anerkennung die Gefahr besteht, dass durch eine Vielzahl von Gefälligkeitsattesten die grundsätzlich angeordnete Maskenpflicht unterlaufen wird und sie so ihre Wirksamkeit verlieren würde.[68]

65 „SARS-CoV-2-Arbeitsschutzregel" Punkt 4.2.13 (Fassung 18.12.2020)
66 LAG Hamm, 28.10.2009 - 3 Sa 579/09; LAG Düsseldorf, 03.09.2009 - 11 Sa 410/09; BAG 19.02.1997 - 5 AZR 83/96; BAG, 15.07.1992 - 5 AZR 312/91
67 So aber ArbG Siegburg, 16.12.2020 - 4 Ga 18/20
68 VG Würzburg, 16.09.2020 - W 8 E 20.1301

Die Behauptung, mit dem ärztlichen Attest zur Maskenunverträglichkeit soll ein rechtlicher Vorteil erwirkt werden, weshalb dieses nicht mit dem Arbeitsunfähigkeitsattest vergleichbar sei[69], wird in den Urteilen weder begründet, noch kann sie eine entsprechende Unterscheidung tragen.[70]

Bei dieser Betrachtungsweise werden datenschutzrechtliche Vorschriften gänzlich unberücksichtigt gelassen.

3. Inhaltliche Anforderungen an das Attest

Wenn das OVG Münster in seiner Entscheidung vom 24.09.2020 formuliert „Insoweit dürften auch, anders als die Antragsteller meinen, der Benennung konkreter medizinischer Gründe in einer entsprechenden Bescheinigung keine datenschutzrechtlichen Aspekte entgegenstehen. Konkrete Anhaltspunkte, die einen nicht datenschutzkonformen Umgang mit ihren Daten befürchten lassen, haben die Antragsteller im Übrigen nicht vorgetragen“ verkennt das Gericht völlig, den Grundsatz der Datenschutzgrundverordnung (DS-GVO), nach der der Betroffene nicht verpflichtet ist darzulegen, dass seine ohne Rechtsgrund erhobenen personenbezogenen Daten nicht datenschutzkonform verarbeitet werden.

Bei ärztlichen Attesten handelt es sich um Gesundheitsdaten gem. Art. 4 Nr. 15 DS-GVO, die gem. Art. 9 Abs. 1 DS-GVO grundsätzlich nicht verarbeitet werden dürfen. Eine Ausnahme ergibt sich vorliegend auch nicht aus Art. 9 Abs. 2 lit. b) DS-GVO. Der Arbeitgeber ist nicht verpflichtet, den Inhalt ärztlicher Atteste zu hinterfragen. Schon gar nicht besteht eine Verpflichtung zur Erhebung von personenbezogenen Daten besonderer Kategorie (Gesundheitsdaten) durch den Arbeitgeber. Wenn der Arbeitgeber ärztlichen Attesten keinen Glauben schenkt, sollte auch in diesem Fall die Möglichkeit der Überprüfung durch einen Amtsarzt eröffnet sein.

Im Rahmen des Beschäftigungsverhältnisses hat der Arbeitgeber aber niemals das Recht Gesundheitsdaten von Mitarbeitenden zu verarbeiten. Auch bei Einstellungsuntersuchungen oder im Rahmen von Eignungsuntersuchungen im laufenden Beschäftigtenverhältnis hat der Arbeitgeber stets

69 ArbG Siegburg, 16.12.2020 - 4 Ga 18/20; OVG Münster, 24.09.2020 – 13 B 1368/20
70 Diese Argumentation ist auch nicht nachvollziehbar, da mit beiden Attesten das gleiche bewirkt werden soll, nämlich eine negative Beeinträchtigung der Gesundheit. Auch durch die AU-Bescheinigung soll ein Vorteil erwirkt werden, weil der Arbeitnehmer von der Pflicht zur Arbeitsleistung unter Fortzahlung der Bezüge freigestellt wird.

nur die Information zu bekommen, ob der Mitarbeiter für die auszuführende Tätigkeit geeignet ist oder nicht. Gründe in der einen oder anderen Richtung sind aber, selbst wenn der untersuchende Arzt angestellter Betriebsarzt ist, dem Arbeitgeber in keinem Fall mitzuteilen.

Der grundsätzliche Unterschied zwischen der Arbeitsunfähigkeitsbescheinigung und dem ärztlichen Attest zur Befreiung vom Tragen der Mund-Nasen-Bedeckung besteht darin, dass bei ersterem primär der betreffende Arbeitnehmer geschützt werden soll, während bei letzterem der Gesundheitsschutz Dritter, nämlich aller anderen Beschäftigten, betroffen ist. Aber auch diese Tatsache rechtfertigt es nicht den ein Attest vorlegenden Arbeitnehmer dazu zu verpflichten, seine Gesundheitsdaten offenzulegen. Wenn der Arbeitgeber glaubt, von einem Mitarbeiter ohne Mund-Nasen-Bedeckung gehe eine Gefahr aus, muss er diesen zum Schutz der anderen Mitarbeitenden von der Arbeitsleistung freistellen oder mit diesem die Erbringung der Arbeitsleistung im Rahmen mobiler Arbeit ermöglichen.

Das OVG Münster übersieht, dass allein die Verarbeitung von Gesundheitsdaten beim Arbeitgeber einen nicht datenschutzkonformen Umgang mit personenbezogenen Daten darstellt, da weder eine Rechtsgrundlage gem. § 6 Abs. 1 noch gem. § 9 Abs. 2 DS-GVO vorliegt.

Eine rechtswidrige Datenverarbeitung wird auch nicht rechtmäßig, wenn gem. einer Corona-Schutzverordnung das Attest vor unbefugtem Zugriff zu sichern und nach Ablauf des Zeitraumes, für welchen das Attest gilt, unverzüglich zu löschen oder zu vernichten ist.[71]

4. Wer darf das Attest einsehen?

Da das Attest, ebenso wie die Arbeitsunfähigkeitsbescheinigung, den ausstellenden Arzt erkennen lässt, sind über die eigentliche Information damit auch weitere personenbezogene Daten, wie z. B. der Fachrichtung des ausstellenden Arztes, verbunden. Daher ist es erforderlich mit diesem Attest genauso umzugehen, wie mit Attesten zur Arbeitsunfähigkeit.

5. Ist das Attest aufzubewahren?

Für den Arbeitgeber besteht die Verpflichtung sicherzustellen, dass die Arbeitnehmer an ihrem Arbeitsplatz einem nur geringen bis gar keinem

71 So aber OLG Dresden, 06.01.2021 – 6 W 939/20

Risiko ausgesetzt sind. Er muss deshalb darlegen, wie er diese Sicherheit hergestellt hat bzw. warum die Maßnahmen nicht von allen Arbeitnehmern erfüllt werden konnten. Deshalb muss er die Möglichkeit haben die Atteste für die Dauer der Pandemie aufzubewahren, um den Nachweis seiner Verpflichtung erbringen zu können.

6. Zusammenfassung

In der rechtlichen Bewertung steht ein Attest zur Befreiung von der Pflicht eine Mund-Nasen-Bedeckung zu tragen anderen ärztlichen Attesten gleich. Dies führt dazu, dass diesem Attest ein hoher Beweiswert zukommt, der nur durch konkrete und vom Arbeitgeber zu beweisenden Umständen entkräftet werden kann.

Für das Verlangen im Attest konkret Gesundheitsdaten zu offenbaren, die für die Ausstellung des Attestes auschlaggebend waren, fehlt eine Rechtsgrundlage. Ein solches Verlangen ist mithin rechtswidrig.

6.1.2 Vorlage einer Impfbescheinigung / Impfausweis

Ist der Arbeitgeber berechtigt, sich einen Impfausweis von Mitarbeitenden vorlegen zu lassen?

Bei der Frage nach dem Impfstatus handelt es sich um personenbezogene Daten besonderer Kategorie gem. § 4 Nr. 2 i. V. m. Nr. 17 KDG. Solche Daten dürfen gem. § 11 Abs. 1 KDG grundsätzlich nicht verarbeitet werden. Etwas anderes gilt dann, wenn eine der in § 11 Abs. 2 KDG beschriebenen Ausnahmen vorliegt. Zunächst mag es durchaus von Interesse für den Arbeitgeber sein, dass sich Arbeitnehmer*innen gegen ansteckende Krankheiten impfen lassen, um so ihre Arbeitskraft aufrecht zu erhalten. Es ist jedoch keine Rechtsgrundlage ersichtlich, die dem Arbeitgeber das Recht einräumt, seinen Arbeitnehmenden die Vornahme von Impfungen, gleich welcher Art, vorschreiben zu dürfen. Jede Impfung ist ein Eingriff in die körperliche Unversehrtheit der ausschließlich im Ermessen des/der Betroffenen steht. Arbeitgeber haben keinen Anspruch darauf, dass sich Mitarbeitende gesund bzw. gesundheitsfördernd verhalten.

Die Konferenz der katholischen Datenschutzaufsichten hat sich deshalb gegen die Zulässigkeit einer solchen Abfrage des Impfstatus durch den Ar-

beitgeber ausgesprochen. Diese Stellungnahme war wesentlich davon geleitet, dass derzeit nicht belegt ist, inwieweit geimpfte Arbeitnehmer*innen das Coronavirus weitergeben können, ohne selbst daran erkrankt zu sein. Nach dem derzeit belegten Erkenntnisstand schützt eine Impfung die/den Geimpfte/n. Bei einer Abfrage des Impfstatus darf aber für den Arbeitgeber nur von Interesse sein, ob von Mitarbeitenden eine Gefahr für Dritte ausgehen kann. Diese Frage wird aber eben auch bei Vorlage einer Impfbestätigung nach derzeitigem Erkenntnisstand nicht beantwortet. Somit kann der vom Arbeitgeber verfolgte Zweck mit der Auskunft nicht erreicht werden. Damit ist diese nicht erforderlich. Eine Datenverarbeitung die nicht erforderlich ist, ist aber rechtswidrig. Damit ist eine solche Abfrage unzulässig, da eine Ausnahme des § 11 Abs. 2 KDG nicht gegeben ist. Wenn wissenschaftlich erwiesen ist, dass eine Impfung nicht nur Geimpfte schützt, sondern darüber hinaus auch eine Weitergabe des Virus ausschließt, ist über diese Frage ggf. neu zu entscheiden.

6.2 Mitarbeiter-App

In einem Beschäftigungsverhältnis werden zahlreiche Daten von Mitarbeitenden verarbeitet. Das betrifft das Betreten und Verlassen der Einrichtung, die Arbeitszeit, Telefonate, Gehaltsdaten, Krankenversicherung, Fehlzeiten und vieles mehr. Dies alles sind mindestens personenbezogene Daten i. S. d. § 4 Nr. 1 KDG. All diese Daten darf der Arbeitgeber nur im Rahmen der vorgegebenen Zwecke verwenden. Ein weiterer Grundsatz ist der der Datensparsamkeit. Danach dürfen Daten nur für einen bestimmten Zweck und in dem für die Zweckerfüllung notwendigen Maß erhoben werden. Daten, die für die Durchführung des Arbeitsverhältnisses keine Bedeutung haben, sind vom Arbeitgeber also nicht zu verarbeiten.

In einer Einrichtung mit mehr als tausend Mitarbeitenden möchte der Dienstgeber eine sogenannte „Mitarbeiter-App“ einführen. Die Mitarbeitervertretung (MAV) bat uns diesbezüglich um Beratung.

Die App soll nach Angaben der Geschäftsführung ein erweitertes Angebot für die Kommunikation bieten und die „gemeinsame, auf die Belange der Dienstgemeinschaft bezogene betriebliche und private Kommunikation auf einem zeitgemäßen Niveau ermöglichen“. Bei Anmeldung erhält der Mitar-

beiter einen persönlichen Account und kann mit anderen Mitarbeitenden kommunizieren oder sich in Nutzergruppen austauschen. Was bereits bis dahin in von den Mitarbeitenden selbst initiierten Gruppen im Rahmen von Messenger-Diensten geschehen ist, könnte nunmehr auf diese Plattform verlegt werden. Darüber hinaus könnten Einladungen zu Hausveranstaltungen, Meinungsumfragen zu relevanten Themen und Informationen zu Hausaktivitäten über diese App angeboten werden. Nach Angaben der Geschäftsführung könne dies alles „ohne Verpflichtung zu einer zwingenden Teilnahme" geboten werden. Außerdem seien die Inhalte der 1:1-Kommunikation für Außenstehende nicht einsehbar.

Die Datenschutzaufsicht betrachtet es nicht als ihre Aufgabe, bestimmte Applikationen zu prüfen, um eine Empfehlung auszusprechen oder ein datenschutzrechtliches Gütesiegel zu verleihen. Vielmehr geht es darum, zu sensibilisieren, welche datenschutzrechtlichen Risiken vor Einführung einer solchen App zu berücksichtigen sind.

Datenschutz und Datensicherheit befassen sich nicht nur mit Nutzung und Verfügbarkeit von Daten, sondern auch damit, wie personenbezogene Daten interpretiert werden und wie Zusammenhänge und Kontexte hergestellt werden. Probleme entstehen dabei auch, wenn in großem Umfang Beziehungsdaten erfasst werden. Es geht also nicht nur um die vielleicht geschützten Inhalte einer 1:1-Kommunikation, sondern auch um die dabei zum Ausdruck kommenden Netzwerkbeziehungen Mitarbeitender.

Wenn der Dienstgeber selber angibt, zunächst Gruppen für Gruppenchats zu bilden, um dadurch die Nutzer zu motivieren in diesen Gruppen zu kommunizieren und ggf. eigene Gruppen zu gründen, ist es ihm offensichtlich wichtig, eine Kommunikation der Mitarbeitenden in einem von ihm bereitgestellten System zu bündeln. Wenn darüber hinaus angegeben wird, der Dienstgeber würde Gruppen initiieren, in denen über Konfessionelles und Glauben, über Sport, gemeinsame Aktivitäten, aktuelle Gesundheitspolitik u. ä. diskutiert wird, wird deutlich, wie tief der Dienstgeber in die Privatsphäre Mitarbeitender eindringt. Noch deutlicher wird dies, wenn der Dienstgeber erwägt, diese Gruppen von Moderatoren begleiten zu lassen, die die Diskussion und Gedankenaustausche „ein wenig moderieren".

Bereits an dieser Stelle wird offenkundig, dass der Dienstgeber personenbezogene Daten verarbeitet, sie sogar teilweise durch den Moderator erhebt, die für die Durchführung eines Arbeitsverhältnisses nicht erforderlich sind.

Darüber hinaus teilt der Dienstgeber in seiner Beschreibung mit, „der General-Admin hat die grundsätzliche Möglichkeit, personalisierte Nutzerdaten zu erheben und auszuwerten, um für die Dienstgeberin die Kommunikationsstrategie zu überprüfen“. Es ist also offensichtlich beabsichtigt, das Nutzerverhalten zu überwachen. Selbst wenn solche Auswertungen anonymisiert stattfinden, ist es möglich, anhand der sich aus der Analyse ableitenden anonymen Verhaltensraster, einzelne Mitarbeitende zu identifizieren. Bei einer Auswertung der Nutzerdaten können sogenannte Scorewerte vergeben werden. D.h. es könnte bewertet werden, wie häufig sich Mitarbeitende an einer Kommunikation beteiligen, ob Mitarbeitende von anderen häufig gefragt oder um Rat gebeten werden oder ob sie selber nur fragen und Rat suchen. Durch entsprechende Bearbeitung können so sogenannte soziale Graphen erstellt werden, die die informelle Stellung einzelner Mitarbeitender in der Einrichtung erkennen lassen.

Der Moderator kann außerdem Teilnehmende aus der Reserve locken und sie zu persönlichen Stellungnahmen oder privaten Meinungsäußerungen anregen. Da die Stellung des Moderators nicht näher beschrieben ist, könnte er im Auftrag des Dienstgebers Mitarbeitende zu bestimmten Themen ausforschen. Im Netz verlieren Menschen häufig das natürliche Misstrauen, welches sie in einem persönlichen Gespräch unter Anwesenden vielleicht hätten walten lassen.

Auf diese Weise können personenbezogene Daten Mitarbeitender in Form von Meinungen zu betrieblichen aber auch zu gesellschaftlichen Themen aggregiert werden. Dabei wird es sich häufig um Daten zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen u.a. handeln, die unter personenbezogene Daten besonderer Kategorie i. S. v. § 4 Nr. 2 KDG zu subsumieren sind. Die Verarbeitung solcher personenbezogenen Daten ist gem. § 11 Abs. 1 KDG grundsätzlich untersagt.

Wie bereits ausgeführt fallen durch die Nutzung einer solchen App zahlreiche Metadaten an. Neben den Informationen die Mitarbeitende über die App direkt freigeben, eröffnen sich dem Dienstgeber eine Fülle von

Erkenntnissen, wie etwa Hinweise zum allgemeinen Kommunikationsverhalten, der Akzeptanz bei Kollegen oder zu Arbeitsmethoden. Wird darüber hinaus eine Analysesoftware eingesetzt, können aus dem Verhalten in der Gegenwart auch wahrscheinliche Verhaltensweisen in der Zukunft abgeleitet werden.

Aber auch durch Nicht-Teilnahme könnte man sich nicht schützen, wenn es für diejenigen, die sich nicht in die Dienstgemeinschaft einreihen möchten, negative Scorewerte gäbe.

Selbst wenn man dem Dienstgeber unterstellt hier eine moderne Kommunikation in der Einrichtung und einen Zusammenhalt der Dienstgemeinschaft anzustreben, ist zu überlegen, ob die Verarbeitung derartig umfangreicher personenbezogener Daten und personenbezogener Daten besonderer Kategorie rechtlich zulässig ist.

Für eine Rechtmäßigkeit müsste eine der Bedingungen des § 6 Abs. 1 KDG vorliegen. Aus dem dort genannten Katalog kommt nur lit. b), eine Verarbeitung auf der Grundlage einer Einwilligung, in Betracht.

Eine solche Einwilligung im Zusammenhang mit einem Arbeitsverhältnis wurde bislang in der Literatur kritisch betrachtet. Aufgrund des im Arbeitsverhältnis bestehenden Über-Unterordnungsverhältnisses erscheint eine Freiwilligkeit, die eine wesentliche Voraussetzung einer Einwilligung ist, fraglich. Wenn einrichtungsinterne Mitteilungen über die App publiziert werden, dürfte sich der einzelne Mitarbeitende verpflichtet sehen, die App auf seinem Endgerät zu installieren, um nicht in ein Informationsdefizit zu geraten. Nach der Datenschutzgrundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz ist eine Einwilligung im Rahmen des Arbeitsverhältnisses grundsätzlich möglich, jedoch ist das bestehende Abhängigkeitsverhältnis bei der Beurteilung der Freiwilligkeit besonders zu berücksichtigen. Eine solche Regelung sieht das KDG nicht vor. Hält man dennoch auch im Anwendungsbereich dieses Gesetzes eine Einwilligung für möglich, müssen die Umstände der Freiwilligkeit besonders begründet werden.

Zwar ist es nicht zwingend erforderlich, die App auf dem privaten Endgerät zu installieren, jedoch ist auch die Auswertung, ob ein Mitarbeiter dies macht oder nicht, einer Bewertung durch den Arbeitgeber zugänglich. Wer sich sogar in seinem privaten Bereich mit dienstlichen Belangen beschäf-

tigt, wird vom Dienstgeber häufig für motivierter gehalten werden, als jemand der Dienst und Freizeit trennt. Bereits diese Befürchtung wird Mitarbeitende veranlassen, die App auf ihr privates Endgerät herunter zu laden.

Vorliegend ist ein Vorteil für die Mitarbeitenden nicht erkennbar. Soweit der Dienstgeber die App für dienstliche Informationen nutzen möchte, stehen ihm auch bislang schon Kommunikationswege wie z. B. Bekanntgabe im Intranet zur Verfügung. Da nach den eigenen Angaben des Dienstgebers Kommunikation unter Dienstnehmenden auch bisher stattgefunden hat, ist keine Erforderlichkeit gegeben, private Kommunikation nun in den Einflussbereich des Dienstgebers zu verlegen.

Im Rahmen der Beratung haben wir beide Betriebsparteien über unserere Einschätzung gleichermaßen offen informiert. Soweit diesseits bekannt, ist eine Einführung bislang noch nicht erfolgt. Wir gehen aber davon aus, uns nach einer ggf. modifizierten Einführung nochmals mit der Angelegenheit befassen zu müssen.

6.3 Verhängung von Bußgeldern wegen Datenschutzverstoßes gegen Einrichtungen – Haftung von Mitarbeitern

Auch nach dem KDG kann die Datenschutzaufsicht für den Fall eines Verstoßes gegen die dort genannten Regelungen gem. § 51 KDG Bußgelder verhängen.

Bereits in unserem letzten Tätigkeitsbericht[72] hatten wir dargelegt, dass Adressat eines Bußgeldbescheides gem. § 51 Abs. 1 KDG regelmäßig der Verantwortliche bzw. Auftragsverarbeiter ist. Verantwortlicher ist gem. § 4 Nr. 9 KDG eine natürliche oder juristische Person, … die … über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für Mitarbeitende, die im Rahmen ihres Arbeitsvertrages die Interessen und Weisungen des Arbeitgebers umsetzen, trifft dies nicht zu. Eine Ausnahme von diesem Grundsatz gilt nur bei einem bewussten Fehlverhalten des Mitarbeiters, welches nicht im Interesse des Arbeitgebers lag und des-

72 4. TB der KDSA Ost 2019, S. 20

sen unternehmerischem Aufgaben- oder Tätigkeitsbereich nicht zuzurechnen war, sog. Mitarbeiterexzess.[73]

In seiner Entscheidung[74] hat das Interdiözesane Datenschutzgericht diese Rechtsauffassung bestätigt.

Nach der Entscheidung des Gerichts hat der Rechtsträger die rechtliche Befugnis und die tatsächliche Entscheidungsgewalt, den Beanstandungen der Datenschutzaufsichten abzuhelfen. Anders verhält es sich demgegenüber bei Mitarbeitern von juristischen Personen des öffentlichen und privaten Rechts. Sie bieten regelmäßig keine vergleichbare wirtschaftliche Haftungsgrundlage und sie sind wegen ihrer Weisungsgebundenheit nicht in gleich effektiver Weise in der Lage, Beanstandungen der Datenschutzaufsichten abzuhelfen. Mitarbeitern fehlt auch das prägende Eigeninteresse, nämlich die Datenverarbeitung maßgeblich für eigene Zwecke zu gestalten.

Adressat eines Bußgeldbescheides ist danach also die Einrichtung bzw. der Rechtsträger, nicht aber einzelne Mitarbeitende.

Nach wie vor umstritten ist in diesem Zusammenhang aber, ob die Einrichtung für Fehler jedes Mitarbeitenden haftet oder nur für Verstöße, die von Führungskräften der Einrichtung begangen worden sind. Diese Frage drängt sich nach Inkrafttreten des Gesetzes über Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG) deutlicher auf, weil § 25 KDS-VwVfG das Gesetz über Ordnungswidrigkeiten (OWiG) grundsätzlich für Anwendbar erklärt.

Nach § 30 OWiG ist ein Bußgeld gegen ein Unternehmen nur möglich, wenn ein Organ oder ein Mitarbeiter in leitender Position des Unternehmens eine Straftat oder Ordnungswidrigkeit begangen hat und dadurch Pflichten des Unternehmens verletzt oder das Unternehmen bereichert wurde.

Nach § 130 OWiG kann ein Bußgeld gegen ein Unternehmen nur dann verhängt werden, wenn der Inhaber oder ein Organ des Unternehmens schuldhaft Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um Verstöße gegen Straf- oder Bußgeldnormen zu verhindern und es infolge-

73 Ullrich, ZMV 2020, S. 1 ff.
74 IDSG 01/2020 vom 14.12.2020

dessen zu einer Zuwiderhandlung gekommen ist, die durch Aufsichtsmaßnahmen zumindest wesentlich erschwert worden wäre.

Nach diesen Regelungen käme eine Haftung der Einrichtung also nur in Betracht, wenn dessen Organe oder Führungspersonen selbst, schuldhaft gegen datenschutzrechtliche Vorschriften verstoßen hätten oder ihrer eigenen Aufsichtspflicht schuldhaft nicht nachgekommen wären. Eine Haftung für ein Fehlverhalten „einfacher" Mitarbeitender wäre demnach ausgeschlossen.

Der Verweis auf die Regelungen des Ordnungswidrigkeitengesetzes ist zwar für den Bereich des KDG neu, im staatlichen Recht bestand ein solcher Verweis mit § 41 BDSG aber von vornherein. Die deutschen Datenschutzaufsichtsbehörden haben sich deshalb schon 2019 zu dieser Problematik geäußert. Sie gehen[75] davon aus, dass die Regelungen der DS-GVO die Regelungen des deutschen OWiG verdrängen. Ihrer Bewertung legen sie den funktionalen Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) zugrunde, der besagt, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich.

Durch die weitgehende Übernahme der Formulierung des § 41 BDSG in kirchliches Verwaltungsrecht hat der kirchliche Gesetzgeber eine dem staatlichen Recht vergleichbare Rechtssituation herbeigeführt. Es ist deshalb nur folgerichtig, diese auch so zu klären, wie dies im staatlichen Recht geschieht. Nicht zuletzt wegen dem von Art. 91 DS-GVO vorgeschriebenen Einklang der kirchlichen Regelung mit der europäischen Regelung ist auch im Bereich des KDG vom funktionalen Unternehmensbegriff auszugehen, mit der Folge, dass die Einrichtung für das Fehlverhalten aller Mitarbeitenden haftet. Dies auch unabhängig von einer entsprechenden Kenntnis der Geschäftsführung oder anderer Leitungspersonen.

75 Stellungnahme Nr. 97 vom 03.04.2019

7 Technischer Datenschutz

7.1 Das Telefax vs. die E-Mail

Bereits in unserem letzten Tätigkeitsbericht wurde das Thema „Telefax im IP-Netz“[76] behandelt. Doch auch in diesem Berichtszeitraum erreichten uns diesbezüglich technische wie auch organisatorische Fragen, u.a. ob ein Telefaxgerät noch zum Stand der Technik zählen kann. Alle Datenschutzverstöße, die uns zum Faxversand/Faxempfang gemeldet wurden, bezogen sich nicht auf die zugrundeliegende technische Basis. Die Probleme entstanden vielmehr in tatsächlicher und organisatorischer Hinsicht wie z.B. durch Falscheingabe der Telefaxnummer oder durch Zugriff unberechtigter Personen auf die Telefaxausgabe.

Ein Telefaxgerät ist gleich einem Fernkopierer, d.h. wenn ein Fax, sprich eine Fernkopie, versendet wird, wird für die Übertragung ein Telefax-Übertragungsprotokoll verwendet. Bei dem sog. T.38-Protokoll handelt es sich um ein Protokoll, welches den Versand von Faxmitteilungen über Datennetzwerke ermöglicht, indem Faxsignaltöne konvertiert werden. Das Protokoll sorgt dafür, dass am Gerät des Empfängers eine „1:1-Kopie“ ankommt (mit Error Correction Mode/ECM). Dies ist der Grund, warum in vielen Fällen das Telefax als rechtssicher anerkannt ist. Der Inhalt des empfangenen Dokuments (Fax) ist also ein originalgetreues Abbild, daher auch „Fernkopie“ genannt. Das Übertragungsprotokoll sorgt dafür, dass die beiden Endgeräte (Telefaxgeräte) miteinander kommunizieren können. Damit die Endgeräte ganz gezielt „angesprochen“ werden können, erhält jedes Endgerät eine Telefonnummer - die Telefaxnummer. Bei der Kommunikation per E-Mail wäre das die E-Mailadresse.

Und genau an diesem Punkt passieren die meisten Fehler – einmal vertippt und das Fax oder die E-Mail könnte ein unberechtigter Empfänger erhalten. Sind personenbezogene Daten betroffen, kommt es schnell zu einem Datenschutzverstoß. Das trifft natürlich auch für einen aus Versehen falsch adressierten bzw. falsch zugestellten Brief zu. Die Risiken sind bei den hier genannten Zustellformen dieselben.

76 4. TB der KDSA Ost 2019, Abschnitt 7.4

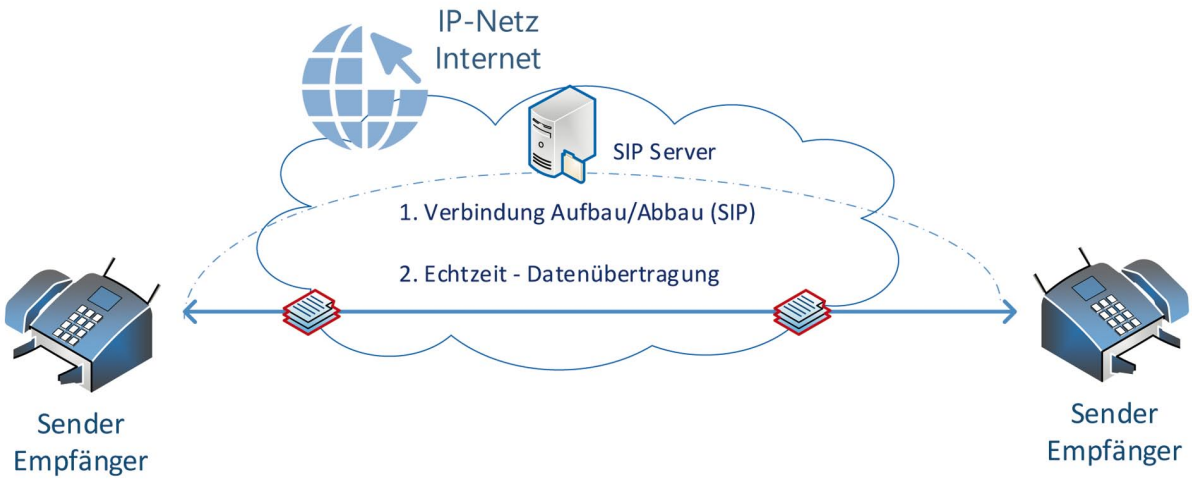
7.1.1 Daten-Orte Fax vs. E-Mail

In den Medien wird das Telefax häufig mit einer unverschlüsselten E-Mail verglichen.

Zum besseren Verständnis soll die nachfolgende grafische Darstellung die Übertragungswege der Daten und deren Ablageort während der Übertragung aufzeigen.

In der folgenden Darstellung bezeichnen wir die Daten-Ablagen (vollständiges Dokument bzw. vollständige Datei) als „Daten-Orte".

Schema 1: Versand per Telefax - versenden eines Dokuments mit Echtzeitübertragung, vorzugsweise mit den T.38 Protokoll Standard mit Fehlerkorrektur (ECM). Es gibt nur zwei Endstellen (Daten-Orte), an denen die Dokumente vollständig vorliegen: beim Sender und beim Empfänger.



Schema 2: Versand per E-Mail über Mailserver bis zur Zustellung

Die beiden Personen stellen die beiden Endstellen dar.

Eine E-Mail kann auf dem Weg zum Empfänger an verschiedenen Stellen (hops) liegen. Bei dieser Übertragung gibt es mehrere Daten-Orte. Deshalb sollte eine Nachricht mit sensiblen Daten nur verschlüsselt versendet werden. Dadurch liegt der Inhalt der Nachricht bei den Daten-Orten nicht lesbar vor. Metadaten, die für eine Datenübertragung an die Adressaten

erforderlich sind, werden nicht mit verschlüsselt. Der Transport von einer Stelle zur anderen Stelle erfolgt in der Regel in verschlüsselter Form (sog. Transportverschlüsselung (TLS).

Die beiden Datenübertragungsverfahren Telefax und E-Mail sind zu unterschiedlich, um sie miteinander vergleichen zu können. Beide Verfahren haben ihre Vorteile und ihre Nachteile. Das Telefax geniest weiterhin den Vorteil der wirklichen Eins-zu-Eins Echtzeitübertragung und der sogenannten „Original-Kopie". Das bedeutet aber auch, dass die Kopie im Klartext am Empfänger, mithin dem Endpunkt ankommt. Eine Verschlüsselung ist praktisch unmöglich. Bei einer E-Mail können Inhalt und Anlagen demgegenüber verschlüsselt werden. Bei einem solchen Verfahren erlangt nur der autorisierte Empfänger Kenntnis vom Inhalt der E-Mail. Fälschlich zugestellte Dokumente könnten so von einem unberechtigtem Empfängerkreis nicht eingesehen werden.

7.1.2 Telefax – zum Stand der Technik

In der Praxis sehen viele Organisationen und Anwender derzeit noch keine Alternative zum Versand von Dokumenten per Briefpost oder per Telefax. Des Weiteren bedeutet ein Versenden von Papierdokumenten per E-Mail, wie beispielsweise unterzeichnete Verträge, einen nicht unerheblichen Mehraufwand und zusätzliche technische Ausstattung. Die Dokumente müssen in eine digital versendbare Datei umgewandelt werden (Digitalisierung). Aufwändiger wird dies bei Dokumenten, die eine Unterschrift benö-

tigen, da u.a. mehrere Arbeitsschritte notwendig werden und einige davon unter Umständen mit einem zusätzlichen Zeitaufwand verbunden sind. Dies soll am nachfolgenden Beispiel aufgezeigt werden:

- Ein elektronisches Formular (z.B. PDF) muss nach dem Abruf, z.B. per E-Mail-Eingang, ausgedruckt und zur Unterzeichnung vorbereitet werden;
- Als nächstes wird es unterzeichnet (ggfs. mit Wartezeit verbunden);
- Danach muss es digitalisiert werden, z.B. Scannen und als Datei in eine entsprechende Datenablage ablegen (ggfs. mit Wartezeit verbunden);
- Nun das Versenden vorbereiten: Webbrowser oder E-Mail-Programm öffnen (Versender benötigt einen Computer, ggfs. mit Wartezeit verbunden),
- Digitalisierte Datei (Anlage) heraussuchen (ggfs. fehleranfällig durch falsche Datei Auswahl)
- Empfänger eintragen (ggfs. Verwechslungsgefahr) und versenden oder per Upload übertragen.

Je nach Datenkategorie noch zusätzlich verschlüsseln und wichtig: Löschfristen auf allen Datenablagen inkl. E-Mail-Ordnern beachten!

Ganz auf das Telefax zu verzichten ist gleichwohl aus heutiger Sicht noch nicht überall praktikabel. Allein deshalb, weil viele Einrichtungen, Ämter und öffentliche Stellen diesen Übertragungsweg als primären Kommunikationskanal vorgeben und damit eine gewisse Abhängigkeit besteht.

Was sollte man beim Einsatz von Telefax zum Stand der Technik beachten?

- Vorzugsweise T.38 auf beiden Gegenstellen mit ECM (ECM bedeutet Fehlerkorrekturverfahren) verwenden. Hier muss der Netzanbieter den Protokoll Standard T.38 unterstützen, ansonsten erfolgt ein Rückfall auf ein anderes Übertragungsprotokoll, aber auch mit Echtzeitübertragung. Die meisten Provider unterstützen T.38.
- Telefax oder Multifunktionsgerät mit einem Kennwort versehen, um die Dokumentenausgabe (Empfangsbox mit Code) zu schützen.

- „Fax-to-internes Fax-Gateway“ (Fax wird per PDF direkt in die dafür vorgesehene Benutzerablage/Fax-Box automatisiert abgelegt).

Grundsätzlich sollte bei der Auswahl eines geeigneten Datenübermittlungs-Verfahrens (Post, Fax, E-Mail, etc.) berücksichtigt werden, in welcher Datenschutz-/Sicherheits-Klasse die zu übertragenen Daten eingestuft sind (siehe KDG-DVO).

Eine Fehlzustellung, insbesondere bei der Übertragung von Telefaxen mit besonders schutzwürdigem Inhalt (personenbezogenen Daten besonderer Kategorie, Sozial-, Steuer-, Personal- oder medizinischen Daten), kann gravierende Folgen für den Absender, den Empfänger und die betroffene Person haben. In dieses Fällen sollte eine unverschlüsselte Datenübertragung unterbleiben.

7.2 Unterschiedliches Verständnis - Ende-zu-Ende Verschlüsselung oder TLS, z.B. bei E-Mail

Eine hohe Zahl von an uns gemeldeten Datenschutzverletzungen bezog sich auf das Versenden von Informationen per E-Mail (zum Teil mit sensiblen personenbezogenen Daten) an falsche Adressaten. In solchen Fällen können unberechtigte Empfänger (Dritte) Einsicht in die darin enthaltenen Informationen erlangen, was zu einem Datenschutz- oder einem IT-Sicherheits-Vorfall führen kann.

Bei den von uns angeforderten Stellungnahmen stellten wir immer wieder fest, dass es ein Verständnisproblem zur Begrifflichkeit „Ende-zu-Ende“ Verschlüsselung gibt. Ein Grund dafür könnte die Pauschalisierung des Begriffs sein. Zur Veranschaulichung versuchen wir im folgenden Abschnitt auf einfache Art die Begrifflichkeiten zu erläutern. Eins gleich vorweg – der pauschale Begriff „Ende-zu-Ende“ ist immer vom Standpunkt und den gemeinten „Enden“ abhängig.

TLS - wie die Abkürzung TLS (Transport Layer Security oder Transport-Verschlüsselung) nahelegt, handelt es sich dabei um einen gesicherten Transportweg, auf dem die Daten von einem „Endpunkt“ zum anderen „Endpunkt“ transportiert werden (in Abbildung 1 als Datenübertragung von „A“ nach „B“ dargestellt). Der gesicherte Transport-/Verbindungsweg wird mit

Hilfe komplexer kryptographischer Verfahren durch Verschlüsselung der Datenpakete erreicht, worauf hier nicht im Detail eingegangen werden soll. Da ein Datenfluss optischer Beobachtung nicht zugänglich ist, soll zur Veranschaulichung im Modell ein fiktives transparentes Rohr zum Datenfluss dienen. Stellen wir uns zur Veranschaulichung dieses Rohr als ein Stück Datenleitung für den Transportweg vor, durch das wir ein paar Daten in Zeitlupe von „A" nach „B" durchschieben werden.

Zuerst schieben wir Daten **ohne TLS durch die Leitung**: Wir können den Transport unserer Datenpakete von dem „Ende A" zu dem „Ende B" nachverfolgen und die Daten während des Transports in der Leitung erkennen. In unserem Modellbeispiel sprechen wir bereits hier von zwei „Enden", was die beiden Endstellen „A" als Start und „B" als Ziel darstellen.

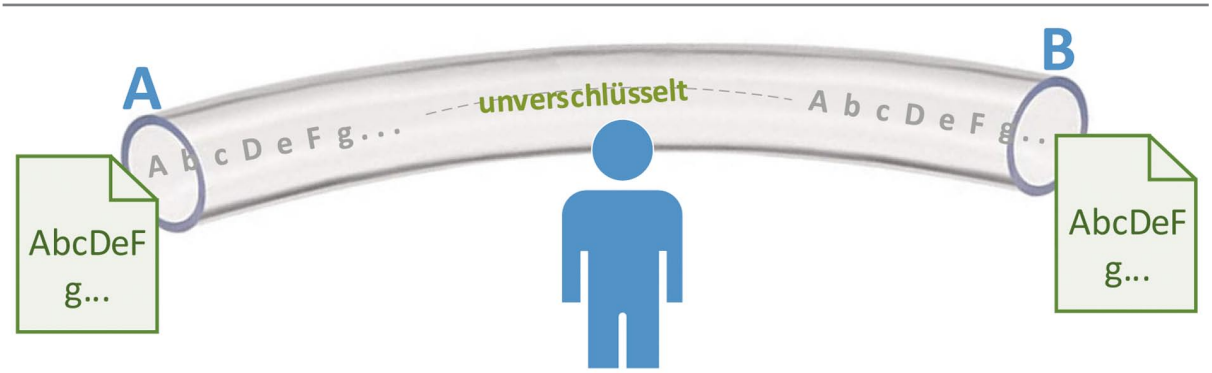


Abbildung 1

Die Zeichenfolge, die wir durch unsere transparente „Rohr-Datenleitung" schieben, können wir an den beiden Enden sowie während des Transports erkennen, sammeln, zusammenbauen und dann ggfs. deuten/lesen. Alle Datenpakete werden in einer Art „Klartext" transportiert - also übertragen. Vertreter einer solchen Datenübertragung sind beispielsweise das normale Webprotokoll „http" oder das E-Mail-Übertragungsprotokoll SMTP (ohne TLS).

Anschließend folgt das **Modell mit TLS**: Wir schicken dieselben Daten von „A" nach „B" auf die Reise (Transport in Abbildung 2). Wie in Abbildung 1 kann unser Beobachter einen Transport der Datenpakete zu dem „Ende B" beobachten. Anders ist hier jedoch, dass die Informationen, die der Beobachter während des Transports ausspionieren möchte, diesmal für ihn kei-

nen aussagekräftigen Sinn ergeben. Die Datenübertragung ist durch den Einsatz von TLS während des Transports durch Kryptographie verschleiert und somit geschützt. In der Praxis spricht man u.a. von einer gesicherten Verbindung. Beispiele dafür wären das gesicherte Webprotokoll „https“ mit TLS (oftmals noch als SSL bezeichnet) oder das E-Mail-Übertragungsprotokoll SMTP mit TLS (SMTPs).

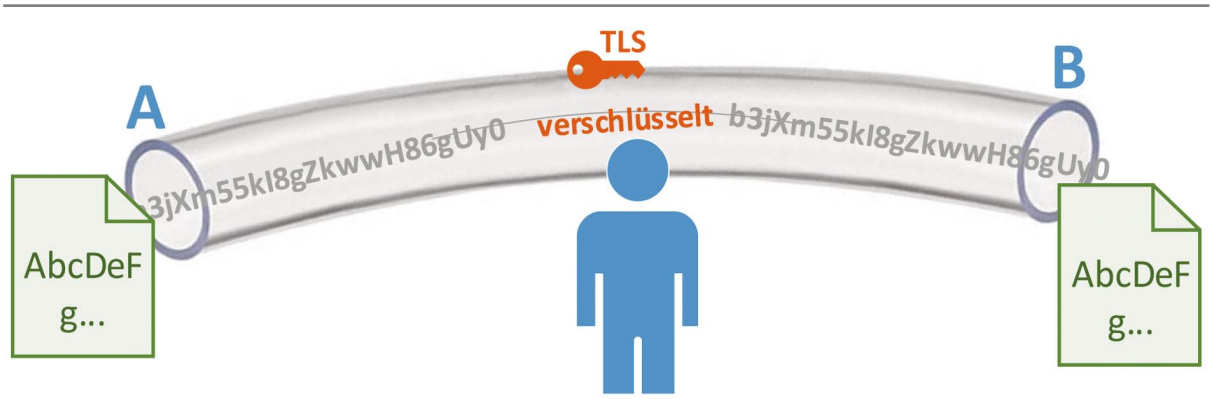


Abbildung 2

Obwohl in diesem Beispiel zwar die Daten verschlüsselt von „Ende A“ zu „Ende B“ übertragen/transportiert werden, ist an den beiden Dokument-Bildchen zu erkennen, dass wir diese ohne weiteres lesen können - also die eigentliche Nachricht nicht zusätzlich verschlüsselt ist. Bei TLS ist der Schutz nur während der Transportphase gewährleistet. Sobald der Transport abgeschlossen ist, befinden sich die Daten unverschlüsselt zur weiteren Verarbeitung auf den Zielsystemen. Die Nachricht erscheint also unverschlüsselt auf der Empfangsseite (Ende) „B“!

Was bedeutet das beim Versenden von Informationen per E-Mail?
Eine normale (unverschlüsselte) E-Mail-Nachricht wird u.U. zwar sicher transportiert, liegt aber im Klartext bei den entsprechenden Endpunkten vor (das können z.B. auch mehrere E-Mail Server sein). Jeder, der diese Nachricht erhält oder darauf zugreifen kann, könnte den Inhalt der Nachricht zur Kenntnis nehmen. Demzufolge auch derjenige, der versehentlich als Adressat eingetragen wurde und dadurch die Nachrichten empfängt.

Welches „Ende-zu-Ende“ ist bei E-Mails gemeint?
Sinnvoller ist es, Informationen in Nachrichten so zu schützen, dass nur

derjenige diese lesen kann, für den sie auch nur bestimmt sind. Dabei kommt auch unsere Ende-zu-Ende Verschlüsslung zum Einsatz, allerdings ändert sich der Standpunkt der „Enden". In dem Fall sind die „Enden" nicht der Transport (unserer hier dargestellte transparente Rohr-Datenleitung mit „A" und „B"), sondern der Sender der Nachricht „Ea" und der/die Empfänger „Eb" der Nachricht. Ziel ist es die Informationen in der Nachricht (oder den Anlagen) so zu verschlüsseln, dass nur die auch dafür autorisierten Empfänger Zugriff auf den Inhalt erhalten. Für alle anderen Empfänger (Dritte) ist der Inhalt nicht lesbar und die sensiblen und/oder personenbezogenen Informationen bleiben für Unbeteiligte verborgen. Versehentlich falsch adressierte Empfänger würden u.U. auch diese Nachrichten erhalten, hätten allerdings keinen Zugriff auf den geschützten Informationsinhalt.

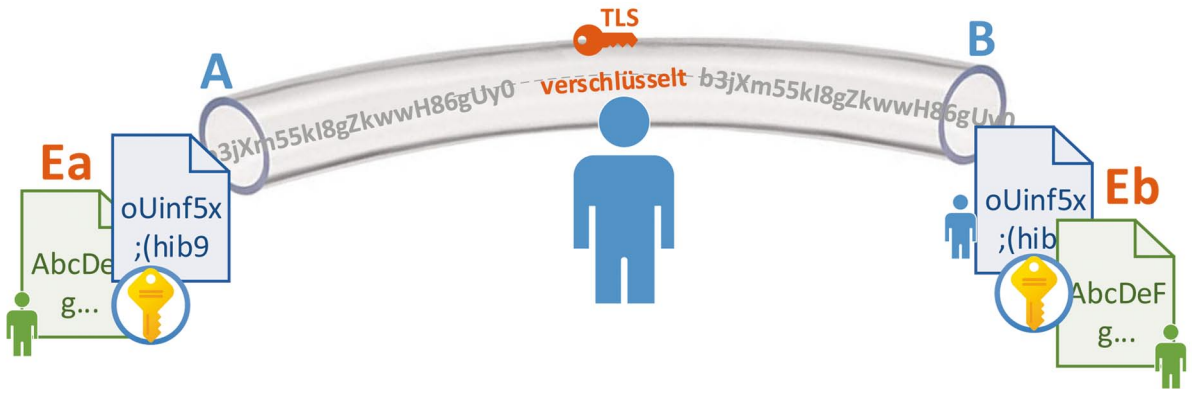


Abbildung 3

Alle haben Recht – die Aussage einer Ende-zu-Ende Verbindung bzw. einer Ende-zu-Ende Verschlüsselung kann je nach Position und Sichtweise des Betrachters unterschiedlich ausfallen. Ein Provider einer Datenverbindung sieht die „Endpunkte" (A und B) an anderer Stelle (seiner Zuständigkeit) als eine Person als Endanwender bei einer E-Mail-Kommunikation oder einer Video-Konferenz (sein Computer als Endgerät).

Übrigens der Weg, den die Daten nehmen, um an das gewünschte Ziel zu gelangen (Routen), ist nicht immer derselbe, was von sehr vielen Faktoren abhängt. Werden sensible Informationen in den Nachrichten durch eine zusätzliche Verschlüsselung geschützt, ist es unerheblich, welchen Weg die Daten nehmen. Auch falls die alternativen Wegstrecken teilweise nicht gesichert sind, bleiben dennoch die Informationen in der Nachricht geschützt.

7.3 Website Check nach Umzug

Im zweiten Halbjahr 2020 haben wir unsere neuen Büroräume in Schönebeck bezogen. Unsere neue Anschrift haben wir direkt per Anschreiben oder über zentrale Informationsblätter publiziert. In diesem Zusammenhang gaben wir zusätzlich den Hinweis zur Überprüfung der Webseiten, falls dort unsere Anschrift mit angegeben wurde.

Bei weiteren betrieblichen Veranstaltungen im vierten Quartal ist auffällig geworden, dass Einrichtungen, die beispielsweise direkt informiert wurden, noch immer eine ältere Anschrift auf ihrer Website haben. Weiterhin war die Datenschutzaufsicht als betrieblicher Datenschutzbeauftragter und nicht als Aufsichtsbehörde dargestellt. In der Folge erreichten uns zahlreiche Anfragen, die in erster Stelle an den betrieblichen Datenschutzbeauftragten hätten gerichtet werden müssen.

Das bevorstehende Jahresende nahmen wir zum Anlass, eine Überprüfung einiger Websiten durchzuführen, um einen Überblick zu erhalten, inwieweit die nicht mehr gültige Anschrift der Datenschutzaufsicht noch verbreitet ist.

Zu diesem Zeitpunkt konnten wir über 140 Websites mit nicht mehr gültigen Anschrift-/Kontaktdaten herausfiltern.

Bei der manuellen Nachbereitung ergaben sich weitere datenschutzrelevante wie auch technische Anhaltspunkte für zukünftig weitreichende Überprüfungen.

7.3.1 Kennen Sie Ihre Website

Viele Verantwortliche bzw. Betreiber einer Website wissen oftmals nicht, welche Datenverarbeitung und welche Dienste auf der eigenen Website integriert und rund um die Uhr (24x7) im Internet verfügbar sind. Das liegt oftmals an der ungenügenden Zusammenarbeit der verantwortlichen Abteilungen mit Dienstleistern und Agenturen, die sich nicht immer mit den rechtlichen Anforderungen auseinandersetzen. Des Weiteren wird oftmals zwar das tech-

nisch machbare empfohlen und dann auch integriert, jedoch ist man sich oftmals der rechtlichen wie auch der sicherheitsrelevanten Konsequenzen nicht bewusst. Die Verantwortung für das Betreiben einer Website bleibt immer beim Betreiber (Impressum) - als verantwortliche Stelle. Im Extremfall muss der Verantwortliche die Haftung dafür übernehmen, was andere integriert haben. Wir konnten auch feststellen, dass bei vielen Website-Projekten betriebliche Datenschutzbeauftragte und/oder Sicherheitsbeauftragte nicht immer eingebunden werden.

Eine weitere bekannte Problematik ist die Pflege einer Website, indem zwar neuer Content (Inhalt) hinzukommt, jedoch älterer, der nicht mehr benötigt wird, nur ausgeblendet und nicht ordentlich von den Systemen entfernt wird. So etwas kann schnell zum Datenschutzverstoß werden und ein Bußgeld nach sich ziehen.

Hier ein Beispiel: Dokumente oder Fotos, welche beanstandet wurden, sind zwar nicht mehr verlinkt, aber auch nicht ordnungsgemäß vom System gelöscht. Oftmals sind diese Daten sogar noch über einen direkten Link (URL) aufrufbar.

Verantwortliche einer Website nehmen **Veränderungen von Rechtsgrundlagen nicht wahr oder nicht immer ernst**: Ein Beispiel hierfür ist das Privacy Shield Abkommen. Dieses wird auf vielen Seiten weiterhin als Rechtsgrundlage für einen Datentransfer zwischen der EU und den USA benannt. Nach einer Entscheidung des EUGH ist dieses Abkommen aber für rechtswidrig erklärt worden und kann deshalb keine Rechtsgrundlage mehr darstellen.

7.3.2 KDSA Website Check 2021

Nach den ernüchterten Ergebnissen unserer anlasslosen Website-Überprüfungen werden wir unsere Testszenarien sukzessive für weitere Überprüfungen ausbauen.

Dies erfolgt in mehreren Phasen. Eine erste Phase wird eine technische Standardüberprüfung beinhalten. Die Berechtigung hierfür ergibt sich aus § 26 KDG.

Werden in dieser Phase grundlegende Mängel festgestellt, wäre zu klären inwieweit die Website noch im Internet für einen unbekannten Personenkreis verfügbar sein darf.

Technische Mängel können sein:

- Systemumgebung ist veraltet und weist Sicherheitsmängel auf oder das System befindet sich nicht mehr im „Software-Lebenszyklus“ (es gibt keine Aktualisierungen mehr)
- SSL/TLS - nicht mehr zugelassene Verschlüsselung (z.B. RC4)
- Formular mit personenbezogenen Daten ohne SSL/TLS (https)

Weitere Prüfpunkte, die Sie kennen sollten:

- Einwilligung - werden Cookies vor einer Auswahl und Einwilligung gesetzt?
- Transparenz - Pflichtinformationen des Website Betreibers sind nicht immer plausibel und transparent zur Webanwendung
- Tracking-Tools, Tracking-Links
- Web-Formulare mit personenbezogenen Daten
- Workflow oder Prozess zur Auskunft über „meine Daten“ die beispielsweise in ein Web-Formular eingetragen wurden (§ 17 KDG). Was passiert mit diesen Daten und über welche Verkehrswege werden diese Daten bis hin zum Bearbeiter übertragen?

7.4 Cookies und Tracking - schon wieder oder immer noch?

Im Rahmen unserer hier genannten Website-Überprüfungen möchten wir in dem Zusammenhang auf das Thema Cookie Behandlung aufmerksam machen und alle Website-Betreiber dafür noch einmal sensibilisieren. Was mit Cookies im Kontext von Websites gemeint ist, sollte für Website-Betreiber allgemein bekannt sein. Deshalb wird hierauf an diese Stelle nicht weiter eingegangen. Bei einigen Internetauftritten wurden Cookies vor einer

Einwilligung gesetzt. Andere Cookies von Drittanbieter wurden beispielsweise gesetzt, bevor die Website überhaupt im Webbrowser sichtbar war, z.B. von Streamingdiensten. Oftmals gab es u.a. keine für uns erkennbare Einwilligung zur lokalen Speicherung der lokalen Cookies. Auch in vielen Datenschutzerklärungen gab es dazu Unstimmigkeiten. Der verantwortliche Betreiber einer Website ist bei einer nicht korrekten Behandlung der lokal gespeicherten Cookies (Session-Cookies ausgenommen) dem Risiko eines Bußgeldes ausgesetzt. Als problematisch betrachten wir auch viele „Consent-Bannern", weil diese häufig keine korrekte Einwilligung darstellen und ein Hinweis auf eine Widerrufsmöglichkeit komplett fehlt.[77]

Aufgabe der Datenschutzgesetze ist es vor einem Missbrauch von personenbezogenen Daten zu schützen. Gelegentlich erschließt sich jedoch nicht ohne weiteres, was der Gesetzgeber genau gemeint hat. So erweist sich beispielsweise aus technischer Sicht beim Thema der „Tracking-Cookies" eine rechtskonforme Umsetzung als nicht ganz trivial. Hier ein Beispiel: Wie soll das Zielsystem – gemeint ist der Webserver, der die Webseite bereitstellt, - wissen, dass die Person, die die Webseite aufruft (also der Surfer), eine Einwilligung gegeben hat, oder nicht. Und wir meinen in dem Beispiel nicht, dass es sich um einen bestimmten Personenkreis handelt, beispielsweise nur um registrierte Benutzer, die sich zuvor bei der Website anmelden müssen. Vielmehr geht es um einen unbestimmten und anonymen Personenkreis, der im Internet surft. Die datenschutzrechtlichen Anforderungen in Bezug auf personenbezogene Daten gehen davon aus, dass immer dieselbe Person, die ein bestimmtes Gerät benutzt und die zuvor eine Einwilligung zum Tracking - egal welcher Technologie - auf einer Website abgegeben hat.

Wenn sich mehrere Personen ein System teilen, trifft diese Annahme aber nicht mehr zu. Gerade in Zeiten von Homeschooling etc. ist das wohl eher die Regel als die Ausnahme. Wer hat auf einer bestimmten Website welche Schalterstellung z.B. im „Consent-Banner" gesetzt und wen soll der Website-Betreiber in Anbetracht seiner „Nachweispflicht" dokumentieren? Mit großer Wahrscheinlichkeit wird in den überwiegenden Fällen die Schalterstellung, die der gerade aktive Website-Besucher gewählt hat, auch

77 Siehe dazu anschaulich https://lfd.niedersachsen.de/startseite/themen/internet/datenschutzkonforme-einwilligungen-auf-webseiten-anforderungen-an-consent-layer-194906.html

in einem lokalen Cookie gespeichert. Doch für welche Person gilt diese Einstellung, wenn doch mehrere Personen mit demselben Benutzerprofil arbeiten? Das kann zu Problemen führen, wenn z. B. eine Person einen Auskunftsanspruch geltend macht. Und noch schwieriger wird es bei einem Widerruf um diesen der richtigen Person zuzuordnen. Der „Cookie-Schalter" würde je nach Benutzer (Person) wahrscheinlich hin und her geschalten werden.

Wer tracken will, weil die gesammelten Informationen wirtschaftlich immer mehr an Bedeutung gewinnen, wird dafür technische Raffinessen und Technologien entwickeln – auch ohne Cookies bzw. solche um rechtliche Fallstricke zu umgehen. Die Informationen, die dort gewonnen werden, sind für Unternehmen zu wichtig, um ein „Website-Tracking" zur Informationsgewinnung und/oder zur Steuerung abzustellen. Vielleicht würde unter Einsatz einer anderen Tracking-Technologie uns der „Consent-Banner" nur in die Irre führen. Weil wir den Cookie-Schalter auf „Ich stimme nicht zu" setzen, wären wir der Annahme, dass die anderen verborgenen Tracking-Mechanismen auch abgestellt wären.

Ein personengebundenes Tracking – unerheblich welches – ohne eine entsprechende Einwilligung sollte grundsätzlich verboten werden. Über ein E-Mail-Tracking im Verborgenen gibt es bislang nur wenige kritische Stimmen, obwohl dies weitaus mehr personenbezogener ist als Surfen. Nicht erkennbar ist auch, ob durch Öffnen einer E-Mail im HTML Format und ein damit verbundener Abruf von weiteren Daten aus dem Internet, auch lokale Cookies gesetzt werden. Einen Hinweis vor dem Lesen einer E-Mail-Nachricht mit der Möglichkeit zu entscheiden, ob man diese lesen möchte und damit dann Tracking/Cookie in Kauf nimmt, oder die Nachricht löschen möchte, gibt es nicht.

Zum Abschluss noch ein weiterer Ansatz zur Datensparsamkeit:

In den Medien werden viele Hersteller dafür kritisiert, dass bei der Einrichtung oder beim Betrieb von Anwendungen nicht die datensparsamsten Optionen voreingestellt sind. Dieser Vorwurf trifft aber in gleicher Weise die Hersteller von Webbrowsern. Diese bieten zwar viele Einstellungen für einen datensparsamen Betrieb, jedoch werden diese nicht in der Standardinstallation voreingestellt. Für den Fall das jetzt schon der eigene Web-

browser so eingerichtet ist, dass er beim Schließen der Anwendung alle Daten wieder löscht, dürfte auch der „Consent-Banner“ per Cookie keine besondere Rolle mehr spielen. Denn alle Cookies sollten beim Schließen des Webbrowsers entfernt sein.

Ein „Aussperren“ einer Technologie wird die eigentliche Problematik nicht lösen, im Gegenteil eine neue Technologie wird sich entwickeln bzw. weiterentwickeln.

7.5 Captcha – I’m not a robot

Auffällig geworden ist auch die Integration von sogenannten Captcha’s (Completely Automated Public Turing test to tell Computers and Humans Apart), die als ein Schutz- und Missbrauchs-Mechanismus für Web-Formulare in Websites integriert sind. Gemeint sind die Bilderrätsel o.ä. Lösungsaufgaben, die zuerst gelöst werden müssen, bevor ein ausgefülltes Web-Formular versendet werden kann. Viele Websites verwenden dafür Service-Angebote von externen Anbietern in Form von Code-Schnipsel oder Plugins etc. Ein in der Praxis häufig eingesetzter Service ist ein Dienst von Google mit „reCaptcha“.

Viele dieser Tools stellen im Hintergrund eine Verbindung zum Service-Anbieter her, wodurch eine Datenübermittlung zwischen dem Webbrowser hin zum Service-Anbieter (ein Dritter) erfolgt. Welche Daten in dem Moment genau übertragen werden, ist abhängig vom Captcha und dem Service-Anbieter. Über diese Art der Datenübermittlung konnten wir in der Mehrheit der Datenschutzerklärungen auf den Internetseiten keine Angaben finden. Es gab weder Informationen zur Datenübermittlung an Dritte, noch gab es eine Information zur Rechtsgrundlage für diese Art der Datenübermittlung.

Verantwortliche der Website sollten kurzfristig prüfen, inwieweit das für sie zutrifft und ggfs. die Dokumentation dahingehend anpassen. Vorab sollte überprüft werden, ob nicht eine lokale Alternative zum eingesetzten externen Service möglich ist.

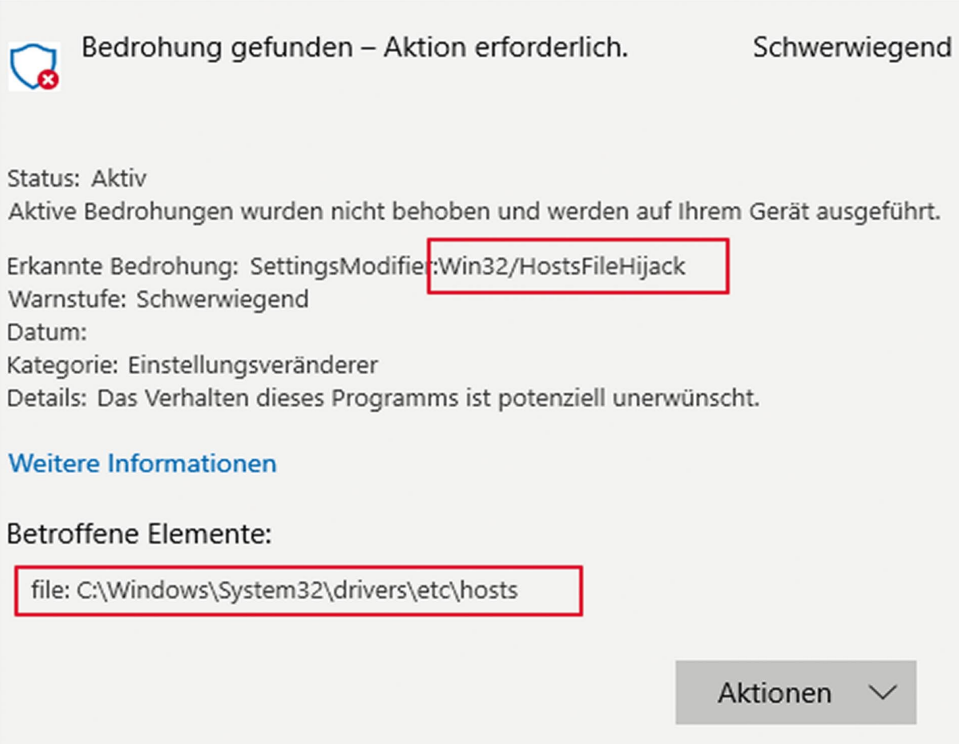
7.6 Windows 10 und FileHijack bei Hosts-Datei

Kurz zur Erinnerung – **Windows 10, Telemetriedaten, Datenschutz** und die intensiven Untersuchungen im Rahmen des Projekts „SiSyPHuS Win10" - als Unterpaket einer allgemeinen Analyse der Windows 10 Telemetrie-Funktionalität.[78] Daraufhin veröffentlichte das BSI eine gut beschriebene Hilfestellung zur Konfigurations- und Protokollierungsempfehlung im Dokument „Analyse der Telemetrie Komponente in Windows 10", Version 1.2. Dort unter dem „Punkt 3.1.5 Lokale DNS-Einträge" gibt es detaillierte Informationen, wie u.a. auch ein **unkontrollierter Datentransfer** von Telemetriedaten durch nicht Erreichen bestimmter Microsoft Domains gestoppt werden kann. Das geht entweder per zentraler Gateway-Systeme oder über lokale Einträge in der sogenannten Windows „Hosts" Datei. Auf die Liste der Domains soll hier nicht weiter eingegangen werden, weil diese im BSI Dokument nachzulesen sind.

Das hatte eine gewisse Zeit funktioniert, bis mit einem Microsoft Update auch der „Microsoft Defender Antivirus" (MS Defender) dahingehend aktualisiert wurde, dass eine Veränderung der Hosts-Datei mit gewissen Microsoft Domains erkannt und blockiert wird. In der Standardkonfiguration des MS Defender können die im BSI Dokument empfohlenen Einträge so einfach wie dort beschrieben nicht mehr vorgenommen werden. Versucht man es trotzdem, so erhält man folgende Bedrohungs-Meldung:

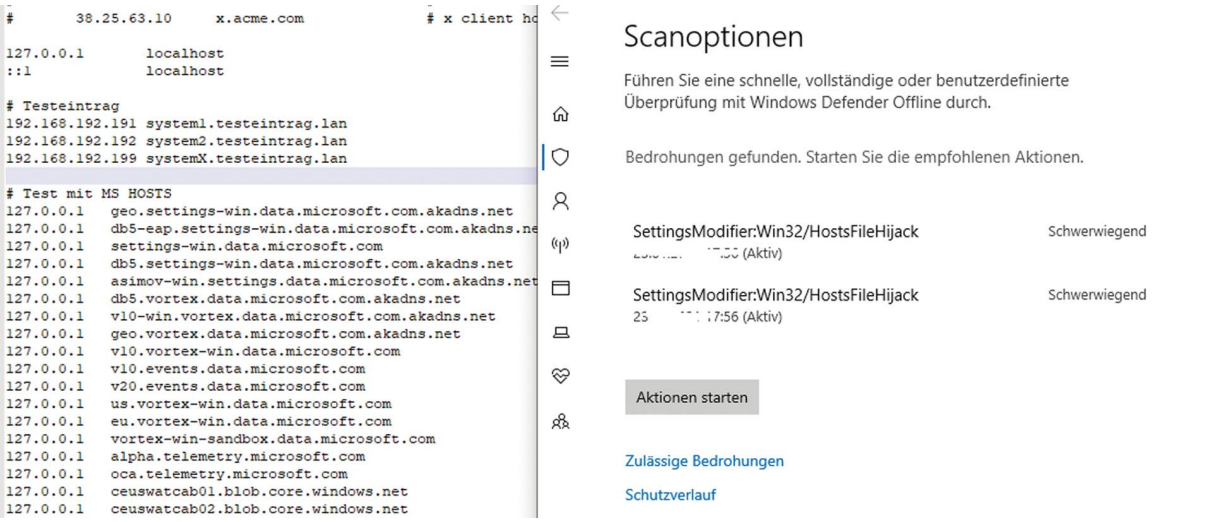
Nun kann man annehmen, dass die Hosts-Datei aus Sicherheitsgründen für alle Einträge, die u.a. auch durch einen Cyberangriff manipuliert werden könnte, blockiert wird. Allerdings - Einträge mit anderen Domains ergaben in einem Test keine dieser Sicherheitshinweise, die Einträge wurden akzeptiert. Setzt man dann wiederum eine mit großer Wahrscheinlichkeit von Microsoft „geschützte Domain" ein, so wird die Hosts-Datei kurz gespeichert, aber nach kurzer Zeit auf einen Windows Standardinhalt zurückgesetzt.

78 BSI: SiSyPHuS Win10: Analyse der Telemetriekomponenten in Windows 10, Konfigurations- und Protokollierungsempfehlung Version 1.2, Abs. 3.1.5 Lokale DNS Einträge
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4.html



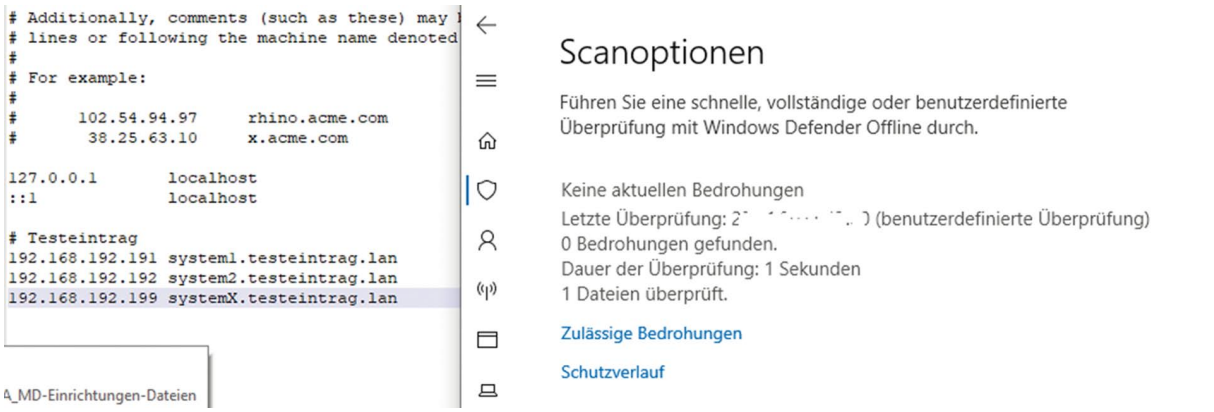
Bei Microsoft ist im Internet dazu folgende Information zu finden: „SettingsModifier: Win32/HostsFileHijack".[79]

Die Manipulation von Hosts-Dateien ist eine häufige Malware- oder Angriffs-Technik, mit der Netzwerkverbindungen verhindert oder umgeleitet werden.



79 https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=SettingsModifier:Win32/HostsFileHijack&threatId=265754

Ein Angreifer kann die Datei ändern, um legitime Verbindungen zu blockieren oder den Netzwerkverkehr an ein vom Angreifer kontrolliertes Ziel umzuleiten, was zum Herunterladen zusätzlicher Malware oder anderer böswilliger Aktivitäten führt.



Aus Sicht der Systemsicherheit ist es schon sinnvoll die Windows Hosts-Datei vor unberechtigter Manipulation zu schützen. Schön wäre es beispielsweise, wenn beim zurücksetzen der Hosts-Datei auf ein schreibgeschütztes Template zurückgegriffenen werden könnte, so dass damit die nicht unberechtigten (also die gewollten) Einstellungen erhalten blieben. Technisch wäre es auch möglich gewesen, die Einträge der Microsoft Domains auf ggfs. falsche IP-Adress-Einträge zu überprüfen und erst dann diese Einträge zurückzunehmen. Mit dieser Maßnahme hat Microsoft die Diskussion um Windows 10 zur Transparenz der übertragenen Telemetriedaten und dem damit verbundenen Datenschutz selber wieder angeheizt.

Es gilt auch hier von Zeit zu Zeit zu überprüfen, inwieweit die eigens konfigurierten Windows Einstellungen für einen datensparsamen Betrieb noch vorhanden sind und damit ihren Zweck erfüllen.

7.7 Webmeeting und Videokonferenz

Aufgrund der Pandemiesituation erhielten wir anfragen, ob eine Nutzung von Videokonferenzsystemen für Webmeetings datenschutzrechtlich zulässig ist und welche Systeme empfohlen werden können.

Produktempfehlung, auch für andere Anwendungsbereiche, können wir in unserer Funktion als Datenschutzaufsicht nicht abgeben. Ob eine Anwendung datenschutzrechtlich unbedenklich ist, lässt sich schon auf Grund der unterschiedlichen Anwendungsfälle sowie der Informationen die darüber verarbeitet und/oder ausgetauscht werden, pauschal nicht beantworten. Der Datenschutz nach dem Gesetz über den Kirchlichen Datenschutz (KDG) ist immer dann betroffen, wenn es sich um personenbezogene oder personenbeziehbare Daten (§ 4 KDG) handelt. Des Weiteren ist neben dem allgemeinen Datenschutz die betriebliche Informationssicherheit zu beachten.

Bei den Webmeeting/Webinare-Systemen werden einerseits Videovorträge angeboten, die auch ohne die Angabe von personenbezogenen Daten abgerufen werden können, andererseits werden Konferenzen durchgeführt wobei u.a. sensible Daten gespeichert und zur Umwandlung in Text verarbeitet werden. Die Frage der datenschutzrechtlichen Zulässigkeit ist also nicht einfach mit „zulässig" oder „unzulässig" zu beantworten. Wir weisen zunächst auf die „Orientierungshilfe Videokonferenzsysteme" [80] und die Checkliste „Datenschutz in Videokonferenzsystemen" [81] der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hin.

Am Beispiel „zoom" (Webmeeting-Service von der zoom Video Communications Inc.) sollen erforderlichen Prüfungen nachfolgend kurz erläutert werden. Was hier den Service von „zoom" (beispielhaft auch für ähnliche Dienste) nach der hier vertretenen Ansicht betrifft, ist ein generelles Verbot der Nutzung aus datenschutzrechtlichen Gründen nicht zwingend veranlasst. Der Webmeeting-Service hat zwischenzeitlich nach Kritik zu diversen Sicherheitsbedenken im Berichtsjahr nachgebessert und damit u.a. auch weitere datenschutzrelevante Einstellmöglichkeiten sowie eine Auswahl der Rechenzentren für die Echtzeitübertragung geschaffen, z.B. die ausschließliche Verwendung von Rechenzentren innerhalb des EU-Raumes.

Zu prüfen ist, ob bei der Nutzung des angebotenen Services (unabhängig vom Standort) personenbezogene Daten verarbeitet werden, die über

80 https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf
81 https://www.datenschutzkonferenz-online.de/media/oh/20201111_checkliste_oh_videokonferenzsysteme.pdf

die IP-Adresse und die zum Betrieb der Videoübertragung naturgemäß erforderlichen personenbezogenen Daten wie Sprache und Bild, hinausgehen. Eine Nutzung im Rahmen von Beratungen, wie z. B. Ehe- Sucht- oder Schuldnerberatung, hat in jedem Fall zu unterbleiben. Demgegenüber erscheint eine Nutzung für Webinare, Vorträge oder Besprechungen in denen keine personenbezogenen oder sicherheitsrelevanten Daten (z.B. Geschäftsgeheimnisse) verwendet werden, möglich.

Weiterhin ist zu prüfen, ob eine Verwendung nach Erteilung einer informierten Einwilligungserklärung, die freiwillig abgegeben wird, möglich ist. Eine Zulässigkeit hängt darüber hinaus von den aktuellen Gegebenheiten ab. Es müsste also vor jeder Nutzung erneut geprüft werden, ob die datenschutzrechtlichen Bedingungen sowohl beim Anbieter noch gegeben sind und auch für den beabsichtigten Zweck beim Verantwortlichen noch verwendet werden dürfen. Da die Entscheidung immer vom Einzelfall abhängig ist, sind diese Prüfungen vom Verantwortlichen mit Unterstützung seines betrieblichen Datenschutzbeauftragten und ggfs. dem IT-Sicherheitsbeauftragten vorzunehmen.

In der Einladung zu einem Webmeeting ist auf die Datenschutzerklärung des Verantwortlichen, also des Einladenden, hinzuweisen. Diese müssen transparente Informationen zur Datenverarbeitung bei Webmeetings enthalten (Informationspflichten). An dieser Stelle kann auch zusätzlich auf die Datenschutzerklärungen des Videoanbieters verwiesen werden. Ein Verweis in der Einladung nur auf die Datenschutzhinweise des Videoanbieters allein ist nicht ausreichend. Zusätzlich wäre auch ein Hinweis zur Verwendung der aktuellsten Softwareversion der Software-Clients hilfreich.

Auf Grund eines einheitlichen Datenschutzniveaus in der Europäischen Gemeinschaft (EU) wird empfohlen, vorzugsweise einen Diensteanbieter aus der EU zu wählen. Was nicht automatisch bedeutet, dass Diensteanbieter innerhalb der EU von einer Prüfung in Hinsicht der geltenden Richtlinien und/oder rechtlichen Vorgaben befreit sind. Als Beispiel sei ein Diensteanbieter, der seine Dienste zwar in der EU anpreist genannt, das Unternehmen aber in den Vereinigten Staaten von Amerika angesiedelt ist. Handelt es sich um einen Dienst aus den Vereinigten Staaten von Amerika, kann das EU-US Privacy-Shield Abkommen nicht mehr als Rechtsgrundlage für eine Datenübermittlungen in Drittstaaten herangezogen werden.

Anhang

Windows 10: Serviceende verschiedener Windows 10 Versionen
Quelle: https://docs.microsoft.com/de-de/windows/release-information/

Version	Letztes Revisionsdatum	Serviceende: Home, Pro, Pro Education, Pro für Workstations und IoT Core	Serviceende für Enterprise, Education und IoT Enterprise
20H2	02.02.2021	10.05.2022	09.05.202
2004	02.02.2021	14.12.2021	14.12.202
1909	21.01.2021	11.05.2021	10.05.202
1809	21.01.2021	Serviceende	11.05.202
1809	21.01.2021	Serviceende	11.05.202
1803	12.01.2021	Serviceende	11.05.202
1803	12.01.2021	Serviceende	11.05.202

Windows 7: Ende des ersten Extended Security Update Year (Erweiterte Sicherheitsupdates (Extended Security Updates, ESU) für Windows 7
Quelle: https://docs.microsoft.com/de-de/lifecycle/products/windows-7

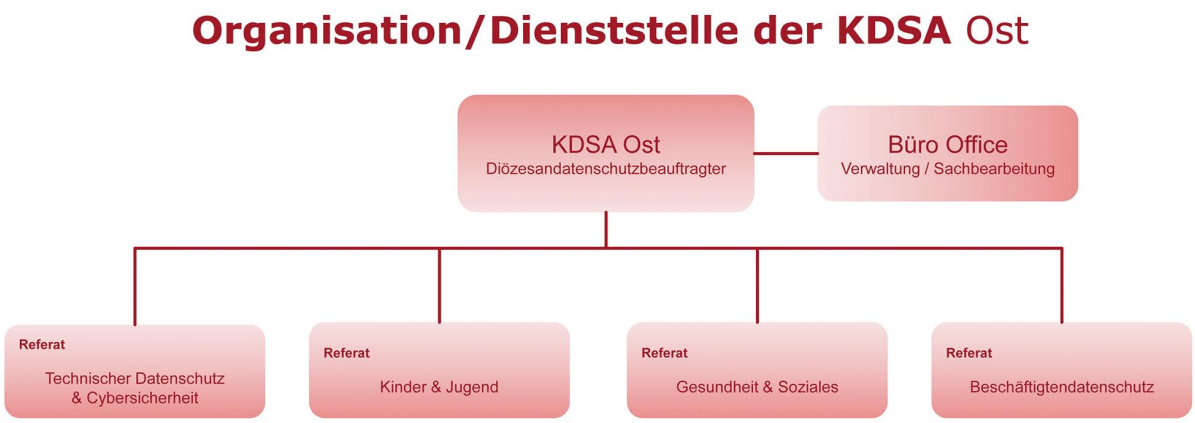
Version	Startdatum	Enddatum
Extended Security Update Year 3*	11.01.2022	10.01.2023
Extended Security Update Year 2*	12.01.2021	11.01.2022
Extended Security Update Year 1*	**14.01.2020**	**12.01.2021**

Die Kirchliche Datenschutzaufsicht Ost

KDSA Ost als Dienststelle

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

Organigramm



Unsere Aufgaben und Befugnisse

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

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

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

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

Abkürzungen

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
ArbG	Arbeitsgericht
ArbSchG	Arbeitsschutzgesetz
BAG	Bundesarbeitsgericht
BayLDA	Bayerische Landesamt für Datenschutz
BbgKHEG	Brandenburgisches Krankenhausentwicklungsgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BO	Berufsordnung
BSI	Bundesamt für Sicherheit und Information
BT-Drs.	Bundestag-Drucksache
BVerfG	Bundesverfassungsgericht
CIC	Codex Juris Canonici
DSB	Datenschutzbehörde
DSK	Datenschutzkonferenz
DS-GVO	Datenschutz-Grundverordnung
ECM	Fehlerkorrekturverfahren
EG	Europäische Gemeinschaft
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
EuGH	Europäischer Gerichtshof
GG	Grundgesetz

GZ	Geschäftszeichen
HTML	Hypertext Markup Language (Auszeichnungssprache für Webseiten)
http	Hypertext Transfer Protokoll (unverschlüsselt)
https	Hypertext Transfer Protokoll Secure (verschlüsselt)
IDSG	Interdiözesane Datenschutzgericht
LAG	Landesarbeitsgericht
LG	Landgericht
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
KDG	Kirchliches Datenschutzgesetz
KDG-DVO	Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz
KDS-VwVfG	Gesetz über das Verwaltungsverfahren im Kirchlichen Datenschutz
MAV	Mitarbeitervertretung
MAVO	Mitarbeitervertretungsordnung
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
SächsKHG	Sächsisches Krankenhausgesetz
SMTP	E-Mail-Übertragungsprotokoll
SSL	Secure Socket Layer (TLS)
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz

TLS	Transport Layer Security
PatDSG	Patienten-Datenschutzgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VDD	Verbandes der Diözesen Deutschlands
VG	Verwaltungsgericht
VwVfG	Verwaltungsverfahrensgesetz
ZMV	Zeitschrift für Mitarbeitervertretung

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