Ein Jahr Gesetz über den Kirchlichen Datenschutz (KDG) - Rückblick und Ausblick

Symposium 2019

Katholisches Datenschutzzentrum

Steffen Pau (Hrsg.)

Ein Jahr Gesetz über den Kirchlichen Datenschutz (KDG) - Rückblick und Ausblick

Symposium 2019

Herausgeber:

Diözesandatenschutzbeauftragter für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und Verbandsdatenschutzbeauftragter des Verbandes der Diözesen Deutschlands (VDD)
Steffen Pau

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231 / 13 89 85 - 0
Fax 0231 / 13 89 85 - 22
E-Mail: info@kdsz.de

Diese Broschüre kann unter www.katholisches-datenschutzzentrum.de in der Infothek abgerufen werden.

Dortmund 2020

Vorwort

Seit dem 25. Mai 2018 gilt die Europäische Datenschutz-Grundverordnung. Am 24. Mai 2018 sind mit dem Gesetz über den Kirchlichen Datenschutz (KDG) auch neue Regelungen für die katholische Kirche in Deutschland in Kraft getreten. Mit den neuen Regelungen wurden die bestehenden Regelungen zum Datenschutz weiterentwickelt und an die aktuellen Gegebenheiten angepasst.

Das Katholische Datenschutzzentrum hat dies zum Anlass genommen, um im Mai 2019 ein Symposium mit dem Thema „Ein Jahr Gesetz über den Kirchlichen Datenschutz (KDG) – Rückblick und Ausblick" im Katholisch Sozialen-Institut des Erzbistums Köln in Siegburg durchzuführen. Dabei wurden die neuen Regelungen aus staatlicher und kirchlicher Sicht betrachtet und eingeordnet.

Mit diesem Band wollen wir die auf dem Symposium gehaltenen Vorträge dokumentieren. Ich danke den Vortragenden, dass Sie uns Ihre Beiträge für diesen Band zur Verfügung gestellt haben.

Den Vortragenden, den Kolleginnen und Kollegen des Katholischen Datenschutzzentrums und allen, die am erfolgreichen Tagungsverlauf und an dieser Dokumentation mitgewirkt haben, danke ich ganz herzlich.

Dortmund 2020 Steffen Pau

Inhaltsverzeichnis

Zur Datenschutzgesetzgebung in den katholischen Diözesen Deutschlands

Marcus Baumann-Gretza*

Die seit dem 25. Mai 2018 geltende Datenschutzgrundverordnung (DSGVO)[1] stellt in vielerlei Hinsicht eine Zäsur dar. Ein besonderes Augenmerk verdient aus Sicht der Kirchen Artikel 91 DSGVO. Dieser bestimmt nicht nur deren Recht zur weiteren Anwendung eigener Datenschutzregelungen, wenn diese mit der Verordnung „in Einklang" gebracht werden. Es kann darüber hinaus eine kircheneigene Datenschutzaufsicht eingerichtet werden, soweit diese die in Kapitel VI DSGVO niedergelegten Bedingungen erfüllt.

Im Gegensatz zum Bundesdatenschutzgesetz trifft die DSGVO damit eine explizite Aussage zu den Möglichkeiten und Grenzen kirchlicher Datenschutzgesetzgebung. Bekanntermaßen verhält sich das BDSG dazu seit jeher nicht. Weder existierte oder existiert eine Bestimmung, wonach sich das Gesetz auch auf die öffentlich-rechtlichen Kirchen und Religionsgesellschaften erstreckt, noch enthielt oder enthält es eine Exemtionsklausel zu deren Gunsten. Durch dieses „beredte Schweigen" - die Nichterwähnung der Kirchen geht letztlich auf eine bewusste Entscheidung des Gesetzgebers zurück[2] - waren und sind die Kirchen von der Geltung

* Bei dem Beitrag handelt es sich um eine redigierte Fassung des mündlichen Vortrags beim Symposium „Ein Jahr Gesetz über den kirchlichen Datenschutz (KDG) - Rückblick und Ausblick" am 28.05.2019 in Siegburg.

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Warenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 04.05.2016, S. 1, ber. ABl. L 314 vom 22.11.2016, S. 72.

2 Ziegenhorn/Aswege, Kirchlicher Datenschutz nach staatlichen Gesetzen?, KuR 2015, S. 198 (203 f.).

des BDSG ausgenommen[3]. Diese Sichtweise entspricht im Ergebnis auch der deutschen Verfassungslage. Aufgrund Artikel 140 GG i. V. m. Artikel 137 Absatz 3 Satz 1 WRV kommt den Kirchen nämlich eine grundsätzliche Regelungskompetenz zur Verwirklichung des verfassungsrechtlich verankerten Datenschutzprinzips zu[4]. Das gilt grundsätzlich auch mit Blick auf die der verfassten Kirche zugeordneten privatrechtlich organisierten Einrichtungen[5].

1. Zur Entstehungsgeschichte des kirchlichen Datenschutzrechts

Kirchliche Datenschutzgesetze sind keine Erfindung des 21. Jahrhunderts. Erste Überlegungen zur Schaffung eigener Datenschutzregelungen gab es schon zu Beginn der 1970er Jahre, ausgelöst durch das erste hessische Landesdatenschutzgesetz von 1970[6]. Die hessischen Diözesen

3 Für generelle Exemtion: von Campenhausen/de Wall, Staatskirchenrecht, 4. A. 2006, S. 289 (293 ff.); Lorenz, Personenstandswesen, Meldewesen, Datenschutz, HdbStKirchR I, Berlin 1994, S. 717 (734 ff.); ders., „Die Stellung der Kirchen nach dem Bundesdatenschutzgesetz 1990", ZevKR 37 (1992), S. 29 f.; ders., Datenschutz im kirchlichen Bereich, Essener Gespräche zum Thema Staat und Kirche, Bd. 15, Münster 1981, S. 84 (91). - Staatliches Datenschutzrecht als subsidiären Ausfalltatbestand bejahend: Hoeren, Kirchen und Datenschutz, Essen 1986, S. 56 (66 f.); ders., Die Kirchen und das neue Bundesdatenschutzgesetz, NVwZ 1993, S. 650 (652). - Für eine Beschränkung auf Kernbereiche kirchlichen Handelns: Dammann, Die Anwendung des neuen Bundesdatenschutzgesetzes auf die öffentlich-rechtlichen Religionsgesellschaften, NVwZ 1992, S. 1147, sowie (Subsumtionslösung): Germann, Das kirchliche Datenschutzrecht als Ausdruck kirchlicher Selbstbestimmung, ZevKR2003, S. 466 f. - Zu den unterschiedlichen Ansätzen im Schrifttum vgl. Ronellenfitsch, Bestandsschutz der Religionsgemeinschaften nach der DSGVO, DÖV 2018, 1019 (1020 f.) sowie die ausführliche Zusammenstellung bei: Sydow/Hense, Europäische Datenschutzgrundverordnung, Baden Baden 2017, Artikel 91, Rn. 6 f.

4 Lorenz, Personenstandswesen (Fn. 3), S. 734 ff.; Stolleis, Staatliche und kirchliche Zuständigkeit im Datenschutzrecht, ZevKR 23 (1978), S. 233; Ziekow, Datenschutz und evangelisches Kirchenrecht, Tübingen 2002, S. 51 f.

5 Hoeren, Kirchen und Datenschutz (Fn. 3) S. 68 ff.; Lorenz, Personenstandswesen (Fn. 3), S. 736 f.; ders., Datenschutz im kirchlichen Bereich (Fn. 3), S. 104 ff.; Specht/Mantz/Paschke, Handbuch Europäisches und deutsches Datenschutzrecht, München 2019, § 27, Rn. 2; Ziegenhorn/Aswege (Fn. 2), S. 206; Ziekow (Fn. 4), S. 125 f.; a. A.: Dammann, Die Anwendung des neuen Bundesdatenschutzgesetzes auf die öffentlich-rechtlichen Religionsgesellschaften, NVwZ 1992, S. 1147 (1151); Simitis/ders., Kommentar zum Bundesdatenschutzgesetz, 8. A. 2014, § 2, Rn. 107 f. Differenzierend: Germann (Fn. 3), S. 460 f., 472 f.

6 Hessisches Datenschutzgesetz (HDSG) vom 7.10.1970, GVBl. I S. 625.

und Landeskirchen hatten sich bereits in damaligem Kontext zum Erlass „ausreichender Datenschutzbestimmungen" verpflichtet[7]. Annähernd zeitgleiche Planungen des Bundesgesetzgebers zum erstmaligen Erlass eines Melde- und eines Datenschutzgesetzes[8] ließen vermuten, dass - dem hessischen Vorbild folgend - die Übermittlung von Meldedaten an die Kirchen[9] bundesweit an ähnliche datenschutzrechtliche Voraussetzungen geknüpft würde. Diese Entwicklung manifestierte sich schließlich in § 10 Abs. 2 BDSG-1977, wonach Datenübermittlungen nur noch bei Schaffung ausreichender Datenschutzregelungen durch die Kirchen möglich sein sollten. Man wird also als gesichert annehmen dürfen, dass es den Kirchen anfangs weniger darum ging, aus theologischer Reflektion zu agieren, sondern vielmehr in Reaktion auf die staatliche Gesetzgebung die Meldedatenübermittlung sicherzustellen[10]. Hieraus erklärt sich wohl auch die auffällige Regelungsübereinstimmung zwischen staatlichem und kirchlichem Recht, die in Teilen der Literatur schon früh zu der Kritik führte, die staatlichen Regelungen seien mit allen Vor- und Nachteilen „unkritisch übernommen worden"[11]. Erforderlich wäre eine derart weitgehende Kongruenz wohl auch nicht gewesen. Die kirchlichen Regelungen hätten lediglich in ihrer Summe einen dem staatlichen Bereich vergleichbaren Datenschutzstandard garantieren müssen[12].

Schon bald nach Inkrafttreten des ersten BDSG zum 01.01.1978[13] traten im katholischen Bereich inhaltsgleiche „Anordnungen über den kirchlichen Datenschutz - KDO"[14] und „Anordnungen über das kirchliche Meldewesen - KMAO"[15] in Kraft[16]. In zahlreichen Diözesen wurden neben KDO-Durch-

7 Ziekow, (Fn. 4), S. 7.
8 Vgl. hierzu im Einzelnen: Ziekow (Fn. 4), S. 5 ff.
9 Zur Frage des Meldedatentransfers grundlegend: Lorenz, Personenstandswesen (Fn. 3), S. 717 (731 f.); Meyer-Teschendorf, Die Weitergabe von Meldedaten an die Kirchen, Essener Gespräche zum Thema Staat und Kirche, Bd. 15, Münster 1981, S. 7 ff.
10 Ziekow, (Fn. 4), S. 19 f., 129 ff.
11 Hoeren, Kirchen und Datenschutz (Fn. 3), S. 31.
12 Hoeren, Kirchen und Datenschutz (Fn. 3), S. 103; Lorenz, Personenstandswesen (Fn. 3), S. 741; Ziekow (Fn. 4), S. 132 f.
13 Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) vom 01.02.1977, BGBl. I, S. 201.
14 Exemplarisch: Anordnung über den kirchlichen Datenschutz - KDO - für das Erzbistum Paderborn, Diözesangesetz vom 23.03.1979, KA Paderborn 1979, Nr. 59.
15 Statt vieler: Anordnung über das kirchliche Meldewesen (Kirchenmeldewesenanordnung - KMAO), Diözesangesetz vom 20.06.1978, KA Paderborn 1978, Nr. 152.
16 Vgl. hierzu: Hoeren, Kirchen und Datenschutz, (Fn. 3), S. 31.

führungsverordnungen sukzessive auch bereichsspezifische Regelungen für den Patientendatenschutz[17], den Sozialdatenschutz[18] oder für die katholischen Schulen[19] erlassen. Im Bereich der EKD galt seit Ende der 1970er Jahre das „Kirchengesetz über den Datenschutz (DSG-EKD)[20]. Trotz zunächst enger Abstimmung bei der Erarbeitung der Gesetzentwürfe kam es letztlich zu in Teilen unterschiedlichen Datenschutzregelungen im Bereich der katholischen Diözesen einerseits und der EKD andererseits.

Was den katholischen Bereich betrifft, stellt eine systematische, in sich geschlossene Datenschutzgesetzgebung auf gesamtkirchlicher Ebene nach wie vor ein Desiderat dar. Gleichwohl finden sich im Codex Iuris Canonici (CIC) von 1983 einzelne Bestimmungen mit im weiteren Sinne datenschutzrechtlichem Charakter. So normieren c. 220 CIC das Recht auf Schutz des guten Rufes und auf Wahrung der Intimsphäre („ad propriam intimitatem tuendam")[21], cc. 983, 984 CIC das Beichtgeheimnis und cc. 472 2°, 1455 § 1, 1457 CIC den Grundsatz der Amtsverschwiegen-

17 So z. B. das Gesetz zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Erzbistum Paderborn, Diözesangesetz vom 19.05.1995, KA Paderborn 1995, Nr. 79. Grundlegende Hinweise zum kirchlichen Patientendatenschutz finden sich in der Handreichung: „Datenschutz im katholischen Krankenhaus - Erläuterungen für die Praxis", herausgegeben von den Arbeitsgemeinschaften katholischer Krankenhäuser Rheinland Pfalz und Saarland sowie der Arbeitsgemeinschaft der katholischen Krankenhäuser in Hessen, Neufassung, Trier/Limburg 2007, S. 10 ff.

18 Statt vieler: Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft, Diözesangesetz vom 14.01.2004, KA Köln 2004, Nr. 92.

19 Exemplarisch: Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft im Erzbistum Paderborn (KDO-Schulen), Diözesangesetz vom 24.06.1998, KA Paderborn 1998, Nr. 99. Vorgängerregelung waren die Ausführungsbestimmungen zur Anordnung über den kirchlichen Datenschutz (KDO) vom 23.03.1979 für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft des Erzbistums Paderborn, KA Paderborn 1991, Nr. 170.

20 Kirchengesetz über den Datenschutz (KiDSG) vom 10.11.1977, ABl. EKD, 1978, S. 2; VO DSG-EKD vom 21.03.1986, ABl. EKD 1986, S. 117. Zu Entstehungsgeschichte und Grundstrukturen des DSG-EKD eingehend: Germann (Fn. 3), S. 473 ff.; Ziekow (Fn. 4), S. 5 ff.

21 Grundlegend zu c. 220 CIC als Ansatz eines „binnenkirchlichen Fundamentalrechtsschutzes": Hoeren, Kirchen und Datenschutz, (Fn. 3), S, 129 ff.

heit[22]. Der CIC 1983 hätte für die katholischen Diözesen in Deutschland Anlass bieten können, bei der nächsten Novellierung eine explizite Rückbindung der KDO an die dort verankerten Prinzipien vorzunehmen. Dazu kam es bisher allerdings nicht[23].

Insbesondere die diözesanen KDOen und das DSG-EKD haben im Laufe der Zeit diverse Novellierungen erfahren. Anlass waren in der Regel entsprechende Änderungen des BDSG, die durch die Rechtsprechung, etwa das Volkszählungsurteil des BVerfG vom 15.12.1983[24], und seit Mitte der 1990er Jahre zunehmend durch europäisches Recht hervorgerufen waren[25]. Zu erwähnen ist in diesem Kontext insbesondere die Änderung der diözesanen KDOen ab dem Jahre 2003. Diese erfolgte letztlich in Folge der europäischen Richtlinie 95/46/EG vom 24.10.1995, die durch den nationalen Gesetzgeber mit dem BDSG vom 23.05.2001 in deutsches Recht transferiert worden war[26].

Stärkere kirchenspezifische Ausgestaltungen zeigten sich indes bei einigen bereichsspezifischen Regelungen, insbesondere bei den katholischen Patientendatenschutzordnungen. Diese wurden allerdings nicht flächendeckend, sondern zumeist nur für diejenigen Diözesen erlassen, in denen katholische Krankenhäuser existierten und von daher ein entsprechender Regelungsbedarf bestand. Neben anderem enthielten diese Regelungen explizite Bestimmungen über die Weitergabe von Patientendaten an die Krankenhausseelsorge bzw. den Pfarrer der jeweiligen Heimatgemeinde. Gleichwohl fanden sich aber auch in den kirchlichen Patientendaten-

22 Vgl. hierzu: Kalde, Kirchlicher Datenschutz, HdbKathKR, 3. Auflage, Regenburg 2015, S.1760; Reinhardt, MK CIC (Stand: Oktober 1987), c. 220, Rn. 7. - Kritisch zur rechtssystematischen Einordnung des ev. Beicht- und Seelsorgegeheimnisses unter das Recht auf informationelle Selbstbestimmung: Germann, (Fn. 3), S. 447 (474). Ganz grundlegend zum Verhältnis des DSG-EKD zum ev. Beicht- und Seelsorgegeheimnis und i. E. ebenfalls kritisch: Ziekow (Fn. 4), S. 150 ff.

23 Hoeren, Die Kirchen und das neue Bundesdatenschutzgesetz (Fn.3), S. 652, betrachtet die KDO allerdings als Konkretisierung der in c. 220 CIC grundgelegten Prinzipien.

24 BVerfGE 65, 1; NJW 1984, 419; zum Novellierungsbedarf nach dem Volkszählungsurteil des BVerfG vgl.: Hoeren, Die Kirchen und das neue Bundesdatenschutzgesetz (Fn. 3), 652.

25 Eine prägnante Darstellung der Rechtsentwicklung findet sich bei: Kalde (Fn. 22), S. 1760 f. - Zu Systematik und Regelungsinhalten der KDOen von 1994/95/96 im Einzelnen: Fachet, Datenschutz in der katholischen Kirche, Neuwied 1998.

26 Eingehend hierzu: Lorenz, Die Novellierung des Bundesdatenschutzgesetzes in ihren Auswirkungen auf die Kirchen, DVBl 2001, 428 ff.

schutzordnungen erkennbare Parallelen zum staatlichen Recht, so im Bereich NRW zum Gesundheitsdatenschutzgesetz des Landes.

Im Kontext der Kirchenspezifika zu erwähnen sind ebenso die für die NRW-Diözesen erlassenen Ausführungsrichtlinien zur KDO[27], die das Datenschutzrecht in Bezug auf die Nutzung personenbezogener Daten im pfarramtlichen Bereich konkretisierten. Nahezu deckungsgleich mit den landesrechtlichen Regelungen waren die KDO-Schulen der NRW-Diözesen. Die katholischen Sozialdatenschutzordnungen hingegen verwiesen nahezu vollständig in den staatlichen Sozialdatenschutz.

In der Gesamtschau lässt sich von 1978 bis 2018 somit eine durchgehende Linie dergestalt konstatieren, dass sich kirchlicher Datenschutz - zumindest was die Hauptregelungswerke betrifft - konsequent an den Regelungen des staatlichen Rechts, insbesondere des BDSG, ausgerichtet hat. Das Motiv bestand primär in der Sicherung des Meldedatentransfers und in der Ausfüllung des von Verfassungs wegen bestehenden Selbstbestimmungsrechts der Kirchen.

2. Kirchlicher Datenschutz im Lichte der DSGVO

Der bereits eingangs erwähnte Artikel 91 DSGVO hat eine aufschlussreiche Entwicklungsgeschichte vorzuweisen[28]. Letztlich ist die Regelung Ausfluss des primärrechtlich in Artikel 17 Abs. 1 AEUV grundgelegten Prinzips, wonach die Union den Status achtet, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedsstaaten nach deren Rechtsvorschriften genießen, und ihn nicht beeinträchtigt; so auch zum

27 Exemplarisch: Änderung und Neufassung der Ausführungsrichtlinien über den kirchlichen Datenschutz - KDO - für den pfarramtlichen Bereich vom 01.06.2013, KA Münster 2013, Art. 153.

28 Vgl. hierzu näher: Sydow/Hense (Fn. 3), Art. 91, Rn. 12; Kühling/Buchner/Herbst, Datenschutzgrundverordnung/BDSG, 2. A. München 2018, Art. 91, Rn. 4 ff.; Losem, Arbeitnehmerdatenschutz in der Kirche im Spannungsfeld zwischen europäischem und nationalem Recht, KuR 2013, S. 231 (240 ff.); Simitis/Seifert, Datenschutzrecht - DSGVO mit BDSG, Baden-Baden 2019, Rn. 4 ff. Grundlegend zur Entstehung und Systematik des Art. 91 DSGVO auch: Ronellenfitsch (Fn. 3), S. 1023 ff.

Ausdruck gekommen in Erwägungsgrund 165[29]. Das bedeutet freilich keine „Bereichsausnahme" im Sinne einer generellen Exemtion kirchlichen Datenschutzes von den europäischen Vorgaben[30]. Die kirchlichen Regelungen müssen mit den Vorgaben der DSGVO - wie es Artikel 91 Abs. 1 DSGVO beschreibt - „in Einklang" stehen. Das beinhaltet allerdings auch nicht die Verpflichtung, das europäische Recht wortgetreu zu übernehmen. Die Kirchen sind in der Formulierung und Ausgestaltung ihrer Regelungen frei, solange sie das Schutzniveau der DSGVO nicht unterlaufen bzw. absenken[31], d. h. den vom europäischen Recht gesetzten Rahmen von Sinn und Zielrichtung her einhalten.

In den beiden großen Kirchen wurde relativ frühzeitig entschieden, den mit dem europäischen Recht umschriebenen Freiraum auszufüllen und damit den eigenen Datenschutzweg fortzuführen. Konkret bedeutete dies, das kirchliche Recht dem Schutzniveau der DSGVO anzupassen. Das beinhaltete zugleich eine nicht zu unterschätzende Herausforderung. Denn auch wenn man unter dem BDSG bereits einen kirchlichen Eigenweg gefunden und etabliert hatte, bedeutete die Anpassung an das Datenschutzniveau der DSGVO in vielerlei Hinsicht das Betreten von Neuland. Es gab schlicht keine „Blaupausen" oder Erfahrungswerte. Um die Unterschiede zwischen evangelischem und katholischem Recht möglichst zu minimieren, setzte man bei der Erarbeitung der Gesetzentwürfe von Beginn an auf eine möglichst enge interkonfessionelle Abstimmung.

29 Zur Bedeutung des Artikel 17 AEUV für das (kirchliche) Datenschutzrecht eingehend: Classen, „Die Bedeutung von Art. 17 AEUV - zwanzig Jahre nach der Erklärung von Amsterdam", ZevKR 61 (2016), S. 333 (338 ff.).

30 Gola, Datenschutzgrundverordnung - Kommentar, 2. A. München 2018, Art. 91, Rn. 1; Sydow/Hense (Fn. 3), Art. 91, Rn. 1.

31 Bergmann/Möhrle/Herb, Datenschutzrecht, Stuttgart 1977 (Stand: Februar 2018), Bd. 3, Art. 91, Rn. 27 ff.; Golland, Reformation 2.0 - Umsetzung der Anforderungen der Datenschutz-Grundverordnung durch die evangelische Kirche, RDV 2018, S. 10 f.; Sydow/Hense (Fn. 3), Art. 91, Rn. 21 ff.; Auernhammer/Jacob, DSGVO BDSG - Kommentar, 6. A. 2018, Art. 91, Rn. 13; Specht/Mantz/Paschke (Fn. 5), Rn. 1 ff.; Simitis/Seifert (Fn. 28), Art. 91, Rn. 11; Ziegenhorn/Drossel, Die Anwendung kirchlicher Regelungen zum Datenschutz unter der EU-Datenschutz-Grundverordnung am Beispiel des § 2 Absatz 8 KDO", KuR 2016, S. 230 (240 ff.). - Kühling/Buchner/Herbst (Fn. 26), Art. 91, Rn. 15, sieht in diesem Zusammenhang auch eine Abweichung vom Schutzniveau der DSGVO „nach oben" als unzulässig an. Nach der abweichenden, i. E. abzulehnenden Auffassung bei: Paal/Pauly, Datenschutzgrundverordnung - Bundesdatenschutzgesetz, 2. A. München 2018, Art. 91, Rn. 16, reduziert sich der Gestaltungsspielraum der Kirchen auf eine Konkretisierung der Vorschriften der DSGVO.

Eine der ersten Grundentscheidungen fiel dahingehend, sich mit dem KDG und dem DSG-EKD eng am Wortlaut der DSGVO zu orientieren. Insbesondere unter dem Aspekt der Rechtssicherheit und Praktikabilität schien es vorzugswürdig, Systematik und Begriffsdefinitionen der DSGVO grundsätzlich zu übernehmen. Staatlicher und kirchlicher Datenschutz bleiben somit nicht nur „in Einklang", sondern in den wesentlichen Grundzügen vergleichbar. Auch wenn diese Vorgehensweise von Einzelstimmen vorschnell als „copy and paste job" abgetan wurde[32], werden die meisten Praktiker dies wohl anders beurteilen. Zum einen bietet der gefundene Weg ein Mehr an Rechtssicherheit. Entscheidungen und Kommentierungen zur DSGVO können zur Normauslegung mit herangezogen werden[33]. Und auch mit Blick auf die vielfältigen Berührungsfelder zwischen Staat und Kirche, etwa beim Meldedatentransfer, dürfte eine mit dem staatlichen Bereich ad hoc kompatible Lösung rechtliche Risiken erheblich vermindern. Zum anderen bieten sich Vorteile auch im Bereich der technischen und organisatorischen Maßnahmen; die wenigsten Anbieter von Hard- und Softwarelösungen wären wohl Willens oder in der Lage, abweichende und als solche möglicherweise auch wenig profitable „Nischenlösungen" für den kirchlichen Bereich zu kreieren.

Zumindest im Bereich der katholischen Kirche sprach auch das für eine Neuregelung zur Verfügung stehende Zeitfenster für eine enge Orientierung an der DSGVO. Mit Blick auf das Wirksamwerden der EU-Neuregelungen zum 25.05.2018 bedurfte es wegen der kirchenintern zu beachtenden Beratungs- und Gremienvorbehalte einer Finalisierung der kirchlichen Gesetzentwürfe bis zum September 2017. Der finale Text der DSGVO stand wegen der im Laufe des EU-Trilogs erfolgten Änderungen aber erst relativ spät verbindlich fest. Eine zeitliche Zuspitzung ergab sich zudem daraus, dass das im Sommer 2017 novellierte BDSG[34] ebenfalls Berücksichtigung finden sollte.

32 Schüller, Bürokratisches Monster - Die katholische Kirche und das neue Datenschutzrecht, HK 8/2018, S. 22 (23 f.), der sich zu der Kritik versteigt, die DSGVO sei weithin „stupide abgeschrieben" und kirchenrechtlich kanonisiert worden. Entgegnend: Kämper, Verantwortlicher Umgang mit einer großen Herausforderung, HK 10/2018, S. 48 (49).

33 Kämper (Fn. 32), S. 49.

34 Bundesdatenschutzgesetz vom 30.06.2017, BGBl. I S. 2097.

3. Anmerkungen zu einigen ausgewählten Aspekten kirchlicher Datenschutzgesetzgebung

Bezüglich der kirchlichen Neuregelungen sei an dieser Stelle lediglich exemplarisch auf einige ausgewählte Gesichtspunkte hingewiesen[35]:

Der organisatorische Anwendungsbereich des KDG deckt sich mit den Regelungen der bisherigen KDO. Neben dem verfasst kirchlichen Bereich gilt das KDG somit auch für den Bereich der Caritas sowie für die kirchlichen Körperschaften, Stiftungen, Anstalten, Werke, Einrichtungen und die sonstigen kirchlichen Rechtsträger ohne Rücksicht auf ihre Rechtsform. In § 2 Abs. 1 DSG-EKD verhält es sich insoweit ähnlich, als der Anwendungsbereich auch dort über den verfasst kirchlichen Bereich hinausgeht.

Die Begriffsbestimmungen des § 4 KDG / § 4 DSG-EKD entsprechen weitgehend denen der DSGVO. Abweichend wird im KDG die kirchliche Datenschutzaufsicht als „Diözesandatenschutzbeauftragter" bezeichnet, womit eine bereits seit geraumer Zeit etablierte Begrifflichkeit beibehalten wird; ferner werden unter den Begriff der „Beschäftigten" auch kirchenspezifische Funktionsträger wie Kleriker, Weihekandidaten oder Ordensangehörige subsumiert.

Anders als in Artikel 7 DSGVO hat sich der katholische Gesetzgeber in Bezug auf die Einwilligung dafür entschieden, in § 8 Abs. 2 KDG die Schriftform als Regelfall festzulegen. Diese Regelung hat in der Praxis viel Kritik erfahren[36], wobei die ratio legis vielfach in den Hintergrund trat. Die DSGVO schreibt zwar keine Schriftform vor, legt dem Verantwortlichen jedoch die Beweislast auf. Die Schriftform als Regelfall wurde vor diesem Hintergrund für geeigneter gehalten, um insbesondere dem Aspekt der Rechtssicherheit Rechnung zu tragen. Des Weiteren ist zu berücksichtigen, dass

35 Ein kursorischer Vergleich der kirchlichen Neuregelungen mit der DSGVO findet sich u. a. bei: Gola (Fn. 30), Art. 91, Rn. 10 ff. sowie: Hoeren, „Kirchlicher Datenschutz nach der Datenschutzgrundverordnung", NVwZ 2018, S. 373 ff. - Zum neuen DSG-EKD vgl. eingehend: Golland (Fn. 31), S. 8 ff. Zur Einführung des KDG prägnant: Gottwald, Das neue kirchliche Datenschutzrecht steht nun fest, Solidaris Information 1/2018, S. 12 f.

36 Exemplarisch: Schüller (Fn. 32), S. 23.

nach § 8 Abs. 2 KDG bereits jetzt auf die Schriftform verzichtet werden kann, wenn wegen der besonderen Umstände eine andere Form angemessen ist[37].

Informationspflichten des Verantwortlichen und Rechte des Betroffenen sind in §§ 14 ff. KDG bzw. §§ 16 DSG-EKD enthalten. Die Regelungen orientieren sich weitgehend am Regelungsinhalt der DSGVO.

§§ 36 ff. KDG bzw. §§ 36 ff. DSG-EKD sehen die Bestellung betrieblicher bzw. örtlicher Datenschutzbeauftragter vor. Damit entsprechen sie der Regelung des Artikels 37 DSGVO, der die Benennung von Datenschutzbeauftragten zum Inhalt hat. KDG und DSG-EKD sehen die Bestellung allerdings erst dann verpflichtend vor, wenn in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind, oder die Kerntätigkeit der verantwortlichen Stelle in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht. In der Praxis führt diese Regelung dazu, dass in nahezu allen kirchlichen Bereichen betriebliche bzw. örtliche Datenschutzbeauftragte zu bestellen sind.

Artikel 51 bis 59 DSGVO schreiben „für die Überwachung der Einhaltung dieser Verordnung" die Existenz unabhängiger Aufsichtsbehörden vor. Die Kirchen sind dem gefolgt und haben ihrerseits Datenschutzaufsichten installiert. Die EKD hat sich mit dem „Beauftragten für den Datenschutz der EKD" in Hannover für ein zentrales Modell entschieden. Im katholischen Bereich wurden nach dem Regionalprinzip fünf unabhängige Datenschutzaufsichten errichtet, die ihren Sitz in Bremen, Dortmund, Frankfurt/Main, München und Schönebeck (bei Magdeburg) haben.

Verschiedentlich ist die Frage nach der Unabhängigkeit dieser kirchlichen Aufsichten gestellt worden[38]. Zunächst sei darauf hingewiesen, dass erste Schritte zur Schaffung unabhängiger Datenschutzaufsichten bereits vor

37 Zur Einwilligung nach dem KDG vgl.: KDG-Praxishilfe Nr. 17, „Rechtmäßigkeit der Verarbeitung/Einwilligung nach dem neuen Gesetz über den kirchlichen Datenschutz (KDG)", herausgegeben von der Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschlands, Stand: 24.01.2018, https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2018/04/PH-17-KDG-Rechtm%C3%A4%C3%9Figkeit-der-Verarbeitung-Einwilligung-Rev-2.0.pdf, zuletzt abgerufen am 28.05.2019.

38 Simitis/Seifert (Fn. 28), Art. 91, Rn. 26.

dem Inkrafttreten der DSGVO unternommen wurden, und zwar infolge der EuGH-Entscheidung zur völligen Unabhängigkeit der Datenschutzaufsichten[39]. Die in den NRW-Diözesen daraufhin angestellten Überlegungen mündeten schließlich in die Errichtung des „Katholischen Datenschutzzentrums" (KDSZ) mit Sitz in Dortmund. Anders als im evangelischen Bereich stellt die Anforderung der Unabhängigkeit im Bereich der katholischen Kirche vor dem Hintergrund ihrer weltkirchlich kodifizierten Eigenverfassung eine gewisse Herausforderung dar. Mit der Entscheidung, das KDSZ in NRW als eigenständige Körperschaft des öffentlichen Rechts zu errichten, die auch qua Satzung[40] über die erforderliche Unabhängigkeit verfügt, ist man jedoch einen Weg gegangen, der die vom EuGH - und später auch von der DSGVO - aufgestellten Kriterien[41] in besonderer Weise erfüllt. Der Umstand, dass die Einrichtung ihren Dienstsitz in Dortmund und damit in keiner der fünf in NRW gelegenen Bischofsstädte hat, unterstreicht diese Unabhängigkeit auch in örtlicher Hinsicht. Es sollte von Beginn an auch nur der Anschein vermieden werden, bei der kirchlichen Datenschutzaufsicht handele es sich um einen lediglich separierten Teil der Diözesanverwaltungen.

Die Datenschutzaufsichten können nach § 51 KDG / § 45 DSG-EKD - und das ist für den kirchlichen Bereich ein Novum - Bußgelder bis zu maximal 500.000 EUR verhängen. Die Abweichung von Art. 83 Abs. 4 und 5 DSGVO ist insbesondere durch den Umstand gerechtfertigt, dass Geldbußen von maximal 500.000 EUR im kirchlichen Bereich dem Erfordernis der Wirksamkeit, Verhältnismäßigkeit und Abschreckung (Art. 83 Abs. 1 DSGVO) hinreichend Rechnung tragen. Zudem wurden kirchliche Teilbereiche gemäß § 51 Abs. 6 KDG / § 45 Abs. 1 S. 2 DSG-EKD grundsätzlich von der Verhängung von Geldbußen ausgenommen[42]. Im katholischen Bereich betrifft dies alle im weltlichen Rechtskreis öffentlich-rechtlich verfassten

39 Urteil des EuGH (Große Kammer) vom 09.03.2010, Az. C 518/07; EuZW 2010, 296; NJW 2010, 1265; vgl. hierzu auch die Ausführungen bei: Auernhammer/Jacob (Fn. 31), Rn. 16.

40 MBl. NRW 2015, S. 822, 825.

41 Vgl. hierzu weiterführend: Gola (Fn. 30), Art. 91, Rn. 13 ff.; Sydow/Hense (Fn. 3), Art. 91, Rn. 26 ff.; Kühling/Buchner/Herbst (Fn. 28), Art. 91, Rn. 17 ff.; Paal/Pauly (Fn. 31), Art. 91, Rn. 20 ff.; Simitis/Seifert (Fn. 28), Art. 91, Rn. 24.

42 Kritsch hierzu: Golland (Fn. 31), S. 12; Hoeren, Kirchlicher Datenschutz (Fn. 35), S. 373 (374); Schüller (Fn. 32), S 24. Zur Verhängung von Geldbußen nach dem DSG-EKD vgl.: Kurzpapier Nr. 2, „Befugnisse der Aufsichtsbehörden und Geldbußen", herausgegeben vom BfD-EKD, https://datenschutz.ekd.de/wp-content/uploads/2018/04/02-Kurzpapier-Aufsichtsbefugnisse-und-Sanktionen.pdf, zuletzt abgerufen am 28.05.2019.

kirchlichen Stellen, soweit diese nicht als Unternehmen am Wettbewerb teilnehmen. Eine ähnliche Einschränkung findet sich im DSG-EKD. Der kirchliche Gesetzgeber orientiert sich damit am Vorbild des Bundesgesetzgebers, der in § 43 BDSG-2017 festgelegt hat, dass gegen Behörden und andere öffentliche Stellen i. S. des § 2 Abs. 1 BDSG keine Bußgelder verhängt werden.

4. Versuch einer Zwischenbetrachtung

Welches Zwischenfazit bleibt nach einem Jahr kirchlicher Datenschutzgesetzgebung in Form des KDG somit zu ziehen?

Die Feststellung, dass der Datenschutz „stört" ist beinahe so alt wie der Datenschutz selbst[43]. So hat auch das KDG im ersten Jahr seines Bestehens neben Anerkennung und Lob auch Kritik erfahren[44]. Zum Teil berechtigt, zum Teil sehr vorschnell. Es ist zu vermuten, dass vieles davon auch emotionale Ursachen hat und einer näheren rechtlichen Prüfung nicht standhält. Praktische Lösungen - etwa bei der Einwilligung - sind oft naheliegender als in erster Reaktion vermutet. Gleichwohl fühlen sich viele Verantwortliche mit der Thematik überfordert. Die Neuregelungen werden als sperrig, kompliziert und lebensfremd empfunden. Das hat viele Ursachen, begründet nicht zuletzt in den Vorgaben der DSGVO selbst. Den Kirchen wird mitunter vorgehalten, diese unreflektiert übernommen und nicht für kürzere, handhabbarere Texte gesorgt zu haben. Das ist vor dem Hintergrund des „In-Einklang-Bringens" leichter gesagt als getan; und es bleibt fraglich, ob die Kirchen mit einem solchen Eigenweg perspektivisch wirklich besser und vor allem rechtssicherer gefahren wären.

Die neue Datenschutzgesetzgebung hinterfragt nicht nur liebgewordene und eingeübte Gewohnheiten, sondern beinhaltet auch empfindliche Sanktionsmöglichkeiten. Insofern ist es bedingt verständlich, dass mancherorts die vermeintlich „guten alten Zeiten" glorifiziert werden. Bemerkenswert ist jedoch, dass das Gros der Normadressaten weniger die Vorteile und den hinter dem Gesetz liegenden Schutzgedanken, als

43 Vgl. hierzu die einführende Darstellung bei: Germann (Fn. 3), S. 447.

44 Exemplarisch: „Kirchlicher Datenschutz: Gut gemeint, schlecht umgesetzt" vom 24.05.2018, https://www.katholisch.de/aktuelles/aktuelle-artikel/kirchlicher-datenschutz-gut-gemeint-schlecht-umgesetzt zuletzt abgerufen am 28.05.2019.

vielmehr die vermeintlichen Nachteile zu rezipieren scheint. Ein im Grunde bedenklicher Befund, dient der Datenschutz doch zuvörderst dem Schutz des Persönlichkeitsrechts und des freien Datenverkehrs. Ferner ist zu berücksichtigen, dass manche vermeintliche Neuerung bereits unter der früheren Datenschutzgesetzgebung existent war - so etwa die Verpflichtung zum Ergreifen der erforderlichen technischen und organisatorischen Maßnahmen - oder schlicht und einfach Ausfluss der Rechtsprechung ist[45].

Erschwerend kommt hinzu, dass der Datenschutz ein Bündel von gesetzlichen Regelungen komplettiert, die insbesondere im Bereich des kirchlichen Ehrenamtes in den vergangenen Jahren für erhebliche Mehrbelastungen gesorgt haben. Jedes Feld für sich genommen wäre sicherlich handhabbar, in der Gesamtschau ergibt sich jedoch immer häufiger das Bild zunehmender Ratlosigkeit und mitunter auch Überforderung.

Doch trotz aller Kritik bleibt zu konstatieren, dass die Kirchen unter den gegebenen Voraussetzungen besser aufgestellt sind, als es die landläufige Stimmung vermuten lässt. Es ist nicht nur gelungen, in einem relativ engen Zeitfenster ein eigenes, funktionsfähiges Datenschutzrecht zu schaffen und unabhängige Aufsichtsbehörden zu installieren[46]. Hinzu kommt im katholischen Bereich eine mit römischer Zustimmung[47]

45 Beispielhaft sei verwiesen auf die Rechtsprechung des EuGH zur Verantwortlichkeit der Betreiber von Facebook-Fanpages, Urteil des Gerichtshofs (Große Kammer) vom 05.06.2018, Az.: C-210/16; EuZW 2018, 534; NJW 2018, 2537, ferner auf den in diesem Kontext gefassten Beschluss der Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschlands vom 10.10.2018, https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2018/11/KDB-Facebook-Fanpages.pdf, zuletzt abgerufen am 28.05.2019, sowie auf die diesbezügliche Kommentierung: „Kompliziert, komplizierter, kirchlicher Datenschutz", https://www.katholisch.de/aktuelles/standpunkt/kompliziert-komplizierter-kirchlicher-datenschutz, zuletzt abgerufen am 28.05.2019.

46 Ziegenhorn/Drossel (Fn. 31), S. 232, sprechen in Bezug auf die Umsetzungserfordernisse zutreffend von einer „Herkulesaufgabe".

47 Die zum 24.05.2018 in Kraft getretene Kirchliche Datenschutzgerichtsordnung (KDSGO) wurde gemäß c. 455 § 1 CIC aufgrund eines besonderen Mandats des Apostolischen Stuhls am 22.02.2018 von der Vollversammlung der Deutschen Bischofskonferenz approbiert, durch Dekret der Apostolischen Signatur vom 03.05.2018 recognosziert und durch Schreiben des Vorsitzenden der Deutschen Bischofskonferenz vom 14.05.2018 promulgiert; die KDSGO ist veröffentlicht u. a. in: KA Essen 2018, Nr. 32.

errichtete kirchliche Datenschutzgerichtsbarkeit[48], die - wenn auch als Sondergerichtsbarkeit - bereits manches vorwegnimmt, was in der Kirche aktuell unter dem Titel „Verwaltungsgerichtsbarkeit" diskutiert wird.

Der kirchliche Datenschutz ist somit weit besser als sein Ruf. Es bleibt der Auftrag, ihn im Interesse aller Beteiligten konstruktiv-kritisch zu begleiten und kontinuierlich fortzuentwickeln. Die in § 58 Absatz 2 KDG angeordnete Evaluation innerhalb von drei Jahren kann dazu eine erste Gelegenheit bieten. Es wäre gleichermaßen zu wünschen wie zu hoffen, dass die Beteiligten im Datenschutz mehr die Vorteile als die Nachteile und mehr die Schutzfunktion als die Reglementierung entdecken.

48 Vgl. hierzu: Gola (Fn. 30), Art. 91, Rn. 20; Sydow/Hense (Fn. 3), Rn. 30; Hoeren, Kirchlicher Datenschutz (Fn. 35), S. 375; Kämper (Fn. 32), S. 49; Specht/Mantz/Paschke (Fn. 5), Rn. 17 f.; Schüller (Fn. 32), S. 24 f.

Erfahrungen mit und Entwicklungen bei der Datenschutz-Grundverordnung

Prof. Dr. Dieter Kugelmann

1. Einschätzungen der DS-GVO

a. Die öffentliche Aufmerksamkeit

Die Datenschutz-Grundverordnung ist am 25. Mai 2018 wirksam geworden. Seitdem hat ihre Wirkung in der Öffentlichkeit unterschiedliche Phasen durchlaufen. Zunächst wurden einzelne Fragen nahezu hysterisch diskutiert und auch durch Teile der Presse mit der Absicht pointiert dargestellt, die Grundverordnung insgesamt zu diskreditieren. Gerade im April, Mai und Juni des Jahres 2018 war insbesondere bei Vereinen und ehrenamtlich Tätigen eine erhebliche Unsicherheit zu verzeichnen, die sich in zahllosen Anfragen und Anrufen an die Datenschutzaufsichtsbehörden und andere mit Datenschutz beschäftigte Stellen niederschlug. Diese erste Phase der Unruhe ist abgeebbt.

Inzwischen ist stattdessen eine kontinuierliche und stabile Wahrnehmung des Datenschutzes eingekehrt. Diese kontinuierliche Wertung des Datenschutzes als wichtiges Element in der digitalen Informationsgesellschaft muss wachgehalten und weiterbetrieben werden. Dies ist nicht zuletzt Aufgabe der Datenschutzaufsichtsbehörden des Bundes, der Länder und auch der Kirchen. Ziel ist, dass die Wachsamkeit anhält. Denn es besteht durchaus die Gefahr, dass aufgrund unterschiedlicher Signale eine Reihe von Verantwortlichen in ihrer Wachsamkeit nachlassen und der Datenschutz teilweise in die Sphäre mangelnder Wahrnehmung zurückfällt. Die Datenschutzaufsichtsbehörden sind daher berufen, beständig weiter zu informieren, zu sensibilisieren und auch durch das effektive Ergreifen von Maßnahmen deutlich zu machen, dass Verstöße gegen den Datenschutz nicht geduldet werden und nunmehr auch mit empfindlichen Sanktionen belegt werden können.

Im Ergebnis hat die Datenschutz-Grundverordnung wesentlich zur Besserung in der Wahrnehmung des Datenschutzes in der Öffentlichkeit geführt. Datenschutz ist präsent. Als Teil der Rahmenbedingungen, in

denen sich Datenverarbeitungen und damit Aktivitäten in Wirtschaft und Gesellschaft abspielen, ist er fester Bestandteil der Diskussionen. Damit hat die Datenschutz-Grundverordnung eines ihrer Ziele erreicht.

b. Die internationale Ebene

Auf der internationalen Ebene hat die Datenschutz-Grundverordnung erhebliche Wirkungen erzielt. Sie ist weltweit das Vorbild für modernen Datenschutz. Trotz oder gerade wegen ihrer Abstraktheit, trotz ihrer Schwächen im Hinblick auf Trennschärfe und einheitliche Verwendung von Begriffen und trotz der nicht hinreichenden Möglichkeiten, zwischen Verantwortlichen im Hinblick auf deren Pflichten zu differenzieren, sind ihre Konzepte und Lösungen das Modernste an Datenschutz, was es seit langem auf der internationalen Ebene gibt. Eine Verordnung, die für 28 Mitgliedstaaten und über 500 Millionen Bürgerinnen und Bürger gilt und den Datenschutz auf eine gemeinsame Grundlage stellt, eignet sich als Modell für kleine wie große Staaten.

Diesem Modell sind denn auch einige gefolgt. Das Datenschutzrecht in Mexiko ist ebenso modernisiert worden wie das Datenschutzrecht in Brasilien. Kalifornien hat als erster Staat der Vereinigten Staaten von Amerika Datenschutzelemente gesetzlich in einer Weise festgelegt, die den Mechanismen der Datenschutz-Grundverordnung nahe kommt. Der Europarat hat die Datenschutz-Konvention Nr. 108 in Anlehnung an das Unionsrecht geändert. Die inhaltlichen Lösungen, die Regelungen der Datenschutz-Grundverordnung für den Datenschutz anbieten, sind Anregungen und Hilfestellungen für diejenigen Gesetzgeber und Normsetzer, die entsprechende Regelungen treffen wollen.

Die Datenschutz-Grundverordnung führt bei international aufgestellten Unternehmen vielfach zur Harmonisierung ihrer Aktivitäten des Datenschutzmanagements. Global agierende Unternehmen müssen sich fragen, ob sie sich unterschiedliche Standards im Datenschutz leisten können und wollen. Hier greift das Ziel der Datenschutz-Grundverordnung, in der Europäischen Union harmonisierte Regelungen für den digitalen Binnenmarkt zu schaffen. Konsequenz ist, dass eine Reihe internationaler Unternehmen ihr Datenschutzmanagement ganz auf die Datenschutz-Grundverordnung eingestellt hat. Damit ist für diese Unternehmen ein einheitlicher und zugleich hoher Standard in ihren europäischen

und teilweise auch globalen Tätigkeiten zu verzeichnen.

c. Auf dem Weg zur Rechtssicherheit

Die Erfolgsgeschichte auf der internationalen Ebene soll nicht den Blick darauf verstellen, dass in der Anwendung der Datenschutz-Grundverordnung nach wie vor Unsicherheit in Einzelfragen besteht. Die abstrakten Regelungen, die technikoffen und grenzüberschreitend gelten und wirken sollen, bedürfen der Konkretisierung in Einzelfällen und damit auch einer konkretisierenden generellen Interpretation.

Erste Konkretisierungen erfolgen durch die Datenschutzaufsichtsbehörden. Kirchliche oder staatliche Behörden geben mit ihren allgemeinen Hinweisen und ihrer konkreten Handhabung der Regelungen vor, wie die Datenschutz-Grundverordnung verstanden werden soll. Die Anwendungspraxis führt bereits zu Handlungssicherheit. Dabei mögen die Ergebnisse und Interpretationen nicht allen Verantwortlichen gefallen. Oftmals geht es aber schlicht darum, dass die Verantwortlichen wissen, woran sie sind. Dies ist in der Wirtschaft regelmäßig zu beobachten.

Die Konkretisierung der Regelungen wird wesentlich durch die Gerichte geleistet. Die zunehmende Zahl von Entscheidungen unterschiedlichster Gerichte in den Mitgliedstaaten und auf der Ebene der EU selbst führen zur Verringerung von Unsicherheiten. Allerdings sind diese Urteile jeweils auf konkrete Kontexte bezogen und daher darauf zu prüfen, ob ihre Aussagen verallgemeinert werden können.

Der Europäische Datenschutzausschuss nach Art. 68 DS-GVO hat insbesondere die Aufgabe, die einheitliche Anwendung der DS-GVO sicherzustellen (Art. 70 DS-GVO). Dazu erarbeitet er Leitlinien, Empfehlungen und bewährte Verfahren. Dies hat der Europäische Datenschutzausschuss in beeindruckender Weise getan. Zunächst wurden die Arbeitspapiere der Art. 29-Gruppe, der Vorgängereinrichtung aufgrund der Richtlinie 95/46, daraufhin geprüft, ob sie übernommen werden können. Dies hat der Europäische Datenschutzausschuss dann festgelegt. Hinzu tritt eine ganze Reihe von Hilfestellungen, Leitlinien und Papieren, die als Unterstützung für eine datenschutzgerechte Anwendung der Regelungen der DS-GVO gedacht sind.

In die gleiche Richtung gehen die Hilfestellungen durch die DSK. Sie hat bereits im Mai 2018 Kurzpapiere erarbeitet, in denen eine Reihe von wichtigen Grundfragen der DS-GVO erläutert und beleuchtet worden sind. Hinzu kommen seitdem ständig neue Positionsbestimmungen und Beschlüsse, um die Unsicherheiten der Anwendungspraxis zu verringern. Die gleiche Aufgabenstellung nimmt auch der kirchliche Datenschutz durch seine entsprechenden Papiere für seine Zielgruppe wahr. Sicherlich fallen die Positionen an der einen oder anderen Stelle auseinander und bedürfen weiterer Zuspitzung und Konkretisierung. Dies wird durch die Anwendungspraxis und die Rechtsprechung jedoch im Laufe der Zeit eintreten. Die Datenschutz-Grundverordnung gerät damit in solideres und ruhigeres Fahrwasser.

d. Evaluationen

Nach Art. 97 der Datenschutz-Grundverordnung erfolgt eine Evaluierung, da die Europäische Kommission einen Bericht über die Bewertung und Überprüfung der Verordnung vorlegt. Zu diesem Bericht wollen viele beitragen. Dies gilt für die Interessengruppen in Wirtschaft und Gesellschaft ebenso wie für die Datenschutzaufsichtsbehörden. Die Konferenz der Unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat einen Unterarbeitskreis eingesetzt, der einen Beitrag für diesen Evaluationsbericht erstellt. Die Aufgabe geht aber darüber hinaus, weil die Erfahrungen der Datenschutzaufsichtsbehörden selbst zusammengeführt und im Hinblick auf Rechtsänderungen bewertet werden sollen.

2. Datenschutzmanagement

Die Datenschutz-Grundverordnung hat in vielen Bereichen Prozesse angestoßen, bei denen die Datenverarbeitung darauf geprüft wird, ob sie erforderlich ist und wie sie sich vollzieht. Für die Verantwortlichen geht es darum, die Datenverarbeitung im eigenen Verantwortungsbereich zu kennen und zu optimieren. Dieser digitale Kassensturz hat in vielen Bereichen dazu geführt, dass Prozesse verbessert und verschlankt werden konnten. Vereinzelt hat damit die Datenschutz-Grundverordnung in der Wirtschaft sogar zu Kosteneinsparungen geführt.

Dies soll nicht verdecken, dass bei der Anpassung von Datenverarbeitungen an die Anforderungen der Datenschutz-Grundverordnung auch Kosten und Aufwand entstehen können. Gerade der Verwaltungsaufwand ist oftmals groß. Dennoch haben zumindest mittlere und größere Unternehmen ersichtlich nicht nur die Notwendigkeit gesehen, ein angemessenes Datenmanagement einzuführen, sondern auch den Anreiz genutzt, ihre internen Abläufe auf die Anforderungen moderner Digitalisierung einzustellen. Kleine und mittlere Unternehmen haben hier sehr viel mehr Probleme, zumindest wenn sie nicht die Datenverarbeitung als Kernaufgabe wahrnehmen. Ihre datenschutzrechtlichen Aufgaben können sie teils nicht ohne fremde Hilfe durch Beratung erfüllen. Zu befürchten ist, dass manche kleine und mittlere Unternehmen und andere Verantwortliche immer noch versuchen, den Kopf in den Sand zu stecken und zu hoffen, nicht erwischt zu werden. Dies wird auf Dauer nicht haltbar sein, weil die verstärkte Achtsamkeit der Nutzerinnen und Nutzer zur Wahrnehmung von Rechten oder zu Fragen an den Verantwortlichen führen. Hinzu treten Hinweise und Beschwerden gegenüber den Datenschutzaufsichtsbehörden. Die Wahrscheinlichkeit der Entdeckung von Datenschutzverstößen wird immer höher.

Die Datenschutz-Grundverordnung antwortet auf die Herausforderungen, die sich aus ihrer Anwendbarkeit auf alle Verantwortlichen vom kleinen Mittelständler bis zum großen Weltunternehmen ergeben mit einem risikobasierten Ansatz. Je höher das Risiko ist, dass eine Datenverarbeitung zu Verstößen gegen das Datenschutzrecht führen kann, desto mehr muss unternommen werden, um dies zu verhindern. Dieser risikobasierte Ansatz ist allerdings insoweit umstritten, als zum Teil vorgetragen wird, dass unter dem Strich die Datenschutz-Grundverordnung doch dazu führe, dass zu viele zu ähnlich behandelt würden. Der risikobasierte Ansatz sei nicht ernsthaft durchgeführt.

Jedoch sind die Ansätze in der Datenschutz-Grundverordnung vielfältig, in denen das Risiko, seine Einschätzung und damit die Konsequenzen aus dieser Einschätzung eine wichtige Rolle spielen. Hier sind noch weitere Ausschärfungen sinnvoll und erforderlich. Zumal für Verantwortliche, die Datenverarbeitung in nur geringem Umfang oder Datenverarbeitung von geringer Risiko-Intensität wahrnehmen, könnten weitere Ausfaltungen der Anforderungen und Erleichterungen der Pflichten herbeigeführt werden. Wer lediglich Kundendaten verwaltet, steht vor anderen

Herausforderungen als der Verantwortliche, der ein Online-Portal betreibt. Nach gegenwärtigem Stand wird dies durch die vernünftige Anwendung der Regelung der Datenschutz-Grundverordnung durch die Datenschutzaufsichtsbehörden aufgefangen. Dabei ist allerdings festzuhalten, dass letztlich die Datenschutz-Grundverordnung auf die Selbstregulierung der Verantwortlichen baut. Der Verantwortliche ist eben selbst verantwortlich, dass die Datenverarbeitung in seinem Bereich den Anforderungen der Datenschutz-Grundverordnung entspricht.

3. Befugnisse des LfDI und ihre Ausübung

Die Befugnisse der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder folgen aus Art. 58 DS-GVO. Danach stehen ihnen umfassende rechtliche Handlungsmöglichkeiten zu. Es gibt eine ganze Bandbreite von möglichen Maßnahmen und Sanktionen, um in verhältnismäßiger Anwendung der Regelungen der DS-GVO dem Einzelfall gerecht zu werden.

Die Untersuchungsbefugnisse des Art. 58 Abs. 1 DS-GVO ermöglichen, dass die Datenschutzaufsichtsbehörden den Sachverhalt kennen, die Einzelheiten ermitteln und eine solide Grundlage für weitere Entscheidungen herbeiführen. Sie haben Zugang zu allen Daten und Geschäftsräumen und können Datenschutzüberprüfungen in umfassender Weise vornehmen. Vor-Ort-Untersuchungen erlauben, sich ein Bild von der konkreten Datenverarbeitung auch und gerade in technischer und organisatorischer Weise zu machen.

Die vielfältigen Abhilfebefugnisse des Art. 58 Abs. 2 DS-GVO erlauben ein gestuftes Vorgehen. Mit unterschiedlicher Intensität greifen sie in die rechtlichen Positionen des Verantwortlichen ein. Die Verwarnung gewissermaßen als gelbe Karte betrifft weniger intensive Verstöße. Die Anweisung oder Anordnung zur Vornahme oder zum Unterlassen einer bestimmten Datenverarbeitung kann durchaus weitgehende Folgen haben. Dabei ist nicht zu unterschätzen, dass die Anordnung der Behörde, bestimmte Datenverarbeitungen in bestimmter Weise durchzuführen, auch erhebliche Kostenfolgen nach sich ziehen kann. Die Genehmigungsbefugnisse des Art. 58 Abs. 3 DS-GVO betreffen vorrangig die internationale Datenübermittlung.

Der LfDI Rheinland-Pfalz hat in seiner Praxis insbesondere die zentralen Maßnahmen in Anspruch genommen, die der unterschiedlichen Intensität von Verstößen gegen den Datenschutz angemessen Rechnung tragen. Die Verwarnung wird als Maßnahme ergriffen, um Verstöße in der Vergangenheit zu kennzeichnen. Der Verantwortliche wird damit sanktioniert, indem ihm ein belastender Verwaltungsakt die Rechtswidrigkeit seines Tuns bescheinigt. Gegenüber öffentlichen Stellen enthält das Landesdatenschutzgesetz Rheinland-Pfalz das Instrument der Beanstandung, das in ähnlicher Weise entsprechende Feststellungen zulässt. Der Verstoß gegen den Datenschutz wird gegenüber einer Behörde beanstandet. Damit ist verbunden, dass derartige Verstöße künftig zu vermeiden sind, indem etwa Umstellungen der Datenverarbeitung oder der Organisation vorgenommen werden müssen. Das Instrument der Beanstandung war bereits vor Inkrafttreten der DS-GVO Teil des Landesdatenschutzrechts. Damals handelte es sich um die am stärksten einschneidende Maßnahme, die der LfDI gegenüber Behörden treffen konnte. Dies ist angesichts der weiteren Befugnisse, die Art. 58 DS-GVO enthält, nunmehr anders. Daher hat sich der Charakter des Instruments der Beanstandung gewandelt, da es nun nicht mehr in seltenen Fällen von besonderem Gewicht sondern zur Ahndung im Regelfall angewendet wird. Der LfDI Rheinland-Pfalz sanktioniert jeden Verstoß gegen das Datenschutzrecht mit einer Maßnahme. Im Fall der öffentlichen Stellen hat daher die Beanstandung den Charakter der Regelreaktion angenommen.

Anweisungen und Anordnungen sind belastende Verwaltungsakte und Eingriffe von erheblicher Intensität. Ziel ist das Verhindern von Verstößen in der Zukunft. Deshalb ist die Datenverarbeitung darauf zu prüfen, welche konkrete Anweisung geeignet ist, um die Verstöße abzustellen und künftig zu verhindern. Geldbußen nach Art. 83 DS-GVO werden gegenüber privaten Stellen verhängt. Das Landesdatenschutzgesetz wie das Bundesdatenschutzgesetz schließen Geldbußen gegen öffentliche Stellen aus. Im Rahmen der Privatwirtschaft ist die Geldbuße dagegen von zentraler Bedeutung, gerade auch durch die gesteigerte öffentliche Wahrnehmung entsprechender Verfahren. An dieser Stelle gilt es besonders deutlich zu machen, dass die Zahnlosigkeit des Datenschutzes Vergangenheit ist. Die Datenschutzaufsichtsbehörden haben nicht das vorrangige Ziel, Geldbußen zu verhängen. Sie zögern aber auch nicht, wenn die Geldbuße das angemessene Mittel ist, um den Verstoß gegen den Datenschutz zu ahnden.

4. Europäische Kooperation

Die Datenschutzaufsichtsbehörden in Europa arbeiten auf der Grundlage der Datenschutz-Grundverordnung in teils formalisierter Weise zusammen. Eine Reihe von Vorschriften der Datenschutz-Grundverordnung enthält Vorgaben für diese Kooperation. Da die Datenschutz-Grundverordnung letztlich auf eine Harmonisierung im digitalen Binnenmarkt abzielt und zugleich grenzüberschreitendes wirtschaftliches Tätigwerden erleichtern soll, wird parallel ein Netzwerk der Verwaltungskooperation zur Rechtsdurchsetzung errichtet.

Im Falle der Grenzüberschreitung eines Vorgangs, der in mehreren Mitgliedstaaten der Europäischen Union spielt, wird die Kooperation ausgelöst. Eine betroffene Person kann eine Beschwerde gegenüber jeder Datenschutzaufsichtsbehörde in der EU einlegen. Es ist dann Aufgabe der Behörden dafür zu sorgen, dass die Beschwerde rechtmäßig behandelt wird und zu einem entsprechenden Erfolg führt. Dazu gibt es eine Plattform, die die Kooperation der mitgliedstaatlichen Behörden erleichtern soll, die sog. IMI-Plattform. Das erste Ziel der IMI-Plattform ist die Feststellung der Zuständigkeit nach Art. 56 DS-GVO. Die Behörde, die einen Fall in IMI einstellt, muss auch angeben, welche Behörde ihrer Ansicht nach die federführende Behörde ist. Die Federführung folgt der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen oder Auftragsverarbeiters (Art. 56 Abs. 1 DS-GVO).

Die federführende Aufsichtsbehörde arbeitet mit den anderen betroffenen Aufsichtsbehörden nach Maßgabe des Art. 60 DS-GVO zusammen. Auch diese Zusammenarbeit vollzieht sich über IMI. Weitere Kontaktaufnahmen und Dialogformen können hinzutreten. Hier geht es um Informationsaustausch, etwa über die Inhalte der Beschwerde oder die wirtschaftliche Konstruktion des Verantwortlichen. In einem nächsten Schritt kann nach Art. 61 DS-GVO Amtshilfe geleistet werden. Das am Weitesten reichende Verfahren ist das Kohärenzverfahren der Art. 63 ff. DS-GVO. Hier gibt der Europäische Datenschutzausschuss (EDSA) Stellungnahmen ab, die von den betroffenen Aufsichtsbehörden erbeten werden können. Nach Art. 65 DS-GVO kann der Europäische Datenschutzausschuss in Einzelfällen sogar einen verbindlichen Beschluss fassen. Dies ist bisher in keinem einzigen Fall erforderlich gewesen. Die Datenschutzaufsichtsbehörden in der Europäischen Union arbeiten vielmehr in einer Weise zusammen, die

eine angemessene Entscheidung der Fallgestaltung in kooperativer Form herbeiführt.

5. Entwicklungen in der Aufsichtspraxis

a. Steigerung der Fallzahlen

Die Datenschutz-Grundverordnung hat das Bewusstsein für Datenschutz gestärkt. Logische Konsequenz ist ein verstärktes Aufkommen von Beschwerden, Anfragen und Hinweisen bei den Datenschutzaufsichtsbehörden. Dies ist erfreulich, weil damit das Ziel erreicht wird, den Datenschutz verstärkt ins öffentliche Bewusstsein zu rücken. Die Kehrseite ist die enorm gestiegene und andauernd hohe Belastung der Mitarbeiterinnen und Mitarbeiter in den Datenschutzaufsichtsbehörden.

Nach Art. 78 Abs. 2 DS-GVO hat die zuständige Aufsichtsbehörde sich mit der Beschwerde zu befassen und zumindest innerhalb von drei Monaten die betroffene Person über den Stand oder das Ergebnis in Kenntnis zu setzen. Damit sind Beschwerden erste Priorität. Hier gilt eine Bearbeitungsfrist. Der Bürger oder die Bürgerin fühlt sich in seinen Rechten verletzt. Die Beschwerde ist damit Ausdruck der Verteidigung grundrechtlicher Positionen.

Zur Einreichung einer Beschwerde haben die Datenschutzaufsichtsbehörden Online-Formulare zur Verfügung gestellt. Damit soll eine vereinfachte und beschleunigte Bearbeitung möglich werden. Die Anzahl der Beschwerden hat sich seit Wirksamwerden der Datenschutz-Grundverordnung beim LfDI RP verdreifacht. Ähnliches berichten andere Datenschutzaufsichtsbehörden. In Rheinland-Pfalz sind zwischen dem 25.05.2018 und dem 31.12.2018 704 Beschwerden eingegangen. Im ersten Halbjahr des Jahres 2019 waren es bereits 413. Damit scheint sich die Quantität auf hohem Niveau zu stabilisieren.

Parallel dazu sind die Meldungen von Verletzungen des Datenschutzes nach Art. 33 DS-GVO geradezu explodiert. Hier geht es darum, dass der Verantwortliche unverzüglich und möglichst binnen 72 Stunden einen Datenschutzverstoß der zuständigen Datenschutzaufsichtsbehörde meldet. Voraussetzungen sind bei größeren Einrichtungen oder Unternehmen

interne Meldewege, die eine entsprechende Meldung nach außen erlauben. Die Datenschutzaufsichtsbehörden haben auch hierzu Online-Formulare zur Verfügung gestellt. Während beim LfDI RP noch zwischen dem 01.01. und 24.05.2018 nach altem Recht lediglich 10 Meldungen eingingen, sind in der zweiten Jahreshälfte 2018 bereits 105 Meldungen zu verzeichnen. Zwischen dem 01.01. und dem 07.05.2019 waren es bereits 59. Hinter diesen Meldungen stehen Datenschutzverstöße, die ggf. ein weiteres Tätigwerden und Vorgehen der Datenschutzaufsichtsbehörden erfordern.

Einen großen Teil der Eingänge bei dem LfDI Rheinland-Pfalz bilden Wünsche, Hinweise, Beratungen und Stellungnahmen. Zumeist geht es um die Unterstützung von betroffenen Personen und von Verantwortlichen. Die telefonischen Beratungen werden beim LfDI Rheinland-Pfalz gar nicht erst gezählt. Dennoch sind die Zahlen gewaltig gestiegen. Schon im ersten Halbjahr 2018 wurden 413 Beratungen gezählt, die meist bereits durch die DS-GVO veranlasst waren, im zweiten Halbjahr waren es 1031. Hier sind insbesondere Vereine, Ehrenamtliche und kleine und mittlere Unternehmen zu nennen, die Rat suchten. Vor dem Hintergrund dieses Anstiegs der Quantität sah sich der LfDI Rheinland-Pfalz gezwungen, eine restriktivere Praxis der Beratung einzuführen. Dies äußert sich zum einen in der Verkürzung der Sprechzeiten, zum anderen in der Vorgehensweise, dass grundsätzlich keine Individualberatungen mehr vorgenommen werden. Dies hat zu einer Verringerung der statistisch gezählten Fälle geführt, so dass im ersten Halbjahr 2019 knapp 300 Beratungen verzeichnet wurden.

b. Änderung der Bearbeitung von Verfahren

Nicht nur die Zahlen sind erheblich angestiegen, die Verfahren tragen auch anspruchsvolleren und aufwändigeren Charakter als nach altem Recht. Dabei spielt die zunehmende informationstechnische Komplexität der zu bewertenden Datenverarbeitungen eine Rolle. Der Hauptgrund liegt aber darin, dass viele Maßnahmen, die nach Art. 58 der DS-GVO ergriffen werden können, als Verwaltungsakte zu qualifizieren sind. Damit kommen die Regelungen des innerstaatlichen Verwaltungsverfahrensrechts zum Tragen. Verwaltungsverfahrensgesetze oder Verwaltungsvollstreckungsgesetze führen zu bestimmten Erfordernissen.

Zunächst ist eine solide Ermittlung des Sachverhalts erforderlich, um dann die rechtsstaatlich erforderliche Anhörung des Betroffenen durchzuführen (§ 28 VwVfG) und ggf. weitere Beteiligungserfordernisse zu berücksichtigen. Die Verfahren dauern insgesamt länger, als unter der Geltung des alten BDSG, das auch weniger formelle Vorgehensweisen angezeigt sein ließ. Die Entscheidungen des LfDI werden sorgfältig getroffen, um zum einen den Interessen der Bürgerinnen und Bürger gerecht zu werden und zum anderen auch um gegenüber dem Begehren von Rechtsschutz gewappnet zu sein. Die Zahl der Klagen gegen den LfDI hat in erheblichem Maße zugenommen, da die Bürgerinnen und Bürger von ihrem Recht Gebrauch machen, sich gegen belastende Verwaltungsakte zu wehren. Für den LfDI wiederum bedeutet dies, dass nun auch die Bearbeitung der Klagen vermehrt Ressourcen beansprucht.

c. Ergriffene Maßnahmen

Im zweiten Halbjahr 2018 hat der LfDI gegenüber öffentlichen Stellen neun Beanstandungen ausgesprochen. Bis zum 07.05. waren es im Jahr 2019 bereits vier. Hinzu tritt eine Reihe von Zwangsgeldern, die nach Verwaltungsvollstreckungsrecht festgesetzt werden. Die Informationsersuchen des LfDI gegenüber dem Verantwortlichen werden teilweise nicht beantwortet. Das Mittel, um eine Antwort durch den Verantwortlichen herbeizuführen, ist die Androhung und ggf. Festsetzung eines Zwangsgeldes. Hier hat der LfDI vor dem Verwaltungsgericht Mainz einen wichtigen Erfolg erzielt, weil in einem Fall ein Zwangsgeld in Höhe von 5000 Euro in vollem Umfang für rechtmäßig erachtet wurde. Das Verwaltungsgericht hat zudem Ausführungen zu dem Verwaltungsverfahren gemacht, die über die konkrete Situation hinaus von Bedeutung sind.

Warnungen nach der DS-GVO hat der LfDI im zweiten Halbjahr 2018 zwei ausgesprochen, im ersten Halbjahr 2019 war es eine Warnung. Die Warnungen verfolgen das Ziel, einen Verantwortlichen davon abzuhalten, in einen Datenschutzverstoß hineinzulaufen. Wenn dem LfDI der Sachverhalt bekannt wird, ist der Verstoß zumeist bereits geschehen. Folgerichtig wurden im zweiten Halbjahr 2018 16 Verwarnungen ausgesprochen, bis zum 07.05.2019 erfolgten 7 weitere Verwarnungen. Adressaten der Verwarnungen waren nicht nur private Stellen, sondern auch öffentliche Stellen des Landes Rheinland-Pfalz.

Das Mittel der Anordnung bereitet deshalb Aufwand, weil sie hinreichend bestimmt sein muss. Aus diesem Grund löst die Vorbereitung einer Anordnung einen durchaus nicht unerheblichen Ermittlungsaufwand aus. Vom 25.05. bis zum 31.12.2018 wurde lediglich eine Anordnung ausgesprochen.

Das Mittel der Geldbuße wurde in dem Zeitraum seit Inkrafttreten der Datenschutz-Grundverordnung bis 31.12.2018 drei Mal angewendet. Vom 01.01.2019 bis zum 07.05.2019 gelangte es bereits zweimal zur Anwendung. Hier handelt es sich oftmals um kleinere Einzelfälle, etwa im Fall der rechtswidrigen Nutzung einer Dashcam oder einer rechtwidrigen Datenübermittlung. Größere Fälle werden auch mit höheren Geldbußen belegt werden.

Der LfDI hat eine Reihe von Vor-Ort-Untersuchungen durchgeführt. Gegenstand waren überwiegend Fälle der Videoüberwachung. Vom 25.05.2018 bis zum 07.05.2019 kam es zu 25 Vor-Ort-Untersuchungen, bei denen Bedienstete des LfDI sich vor Ort von der Rechtmäßigkeit der Datenverarbeitung ein Bild machen wollten.

d. Inhaltliche Schwerpunkte

Ordnet man die Eingänge beim LfDI Rheinland-Pfalz nach inhaltlichen Kriterien, ist für das erste Jahr nach Wirksamwerden der Datenschutz-Grundverordnung eine Steigerung der Fälle mit grenzüberschreitenden oder internationalen Bezug festzustellen. Beschwerden gegen Facebook, Google oder Amazon haben zugenommen. Auch damit wird dem Ziel der Datenschutz-Grundverordnung Rechnung getragen, gerade auch bei grenzüberschreitenden Datenverarbeitungen und Großunternehmen, die sich mit Datenverarbeitung befassen, Bürgerinnen und Bürgern einfacher die Gelegenheit zu geben, ihre Rechte wahrzunehmen.

Bei Verstößen im Internet insgesamt steigen die Fallzahlen an. Hier wurden eine Reihe von Ansprüchen auf Löschung nach Art. 17 DS-GVO geltend gemacht. Einen deutlichen Schwerpunkt bildet die Verweigerung oder Nichterteilung der Auskunft nach Art. 15 DS-GVO. Mit unterschiedlichen Adressaten aus dem privaten und öffentlichen Bereich erweist sich diese Fallkonstellation als Kristallisationspunkt der Durchsetzung von Individualrechten. Die Bürgerinnen und Bürger tragen dabei oft vor, dass

ihrem Recht auf Auskunft nicht in hinreichendem Maße von dem Verantwortlichen Rechnung getragen wurde. Selbstverständlich sind nicht alle diese Beschwerden berechtigt. Dennoch ist hier auch empirisch ein Schwerpunkt im Hinblick auf die Wahrnehmung von Betroffenenrechten der DS-GVO festzustellen.

6. Kernpunkte der Diskussion zur DS-GVO

Wie bereits vor dem Wirksamwerden der DS-GVO stellt sich auch unter ihrem Rechtsregime immer wieder die Frage der zutreffenden Rechtsgrundlage für die Datenverarbeitung. Durch die Datenschutz-Grundverordnung ist dies verstärkt in den Blick der Verantwortlichen gerückt. Dabei spielt die Reichweite der einschlägigen Rechtsgrundlagen eine erhebliche Rolle. Zum Vertrag (Art. 6 Abs. 1 lit. b DS-GVO) hat der europäische Datenschutzausschuss die Leitlinien 2/2019 erlassen, um darzulegen, dass Datenverarbeitung auf vertraglicher Grundlage von zentraler Wichtigkeit ist. Zugleich hat der Vertrag aber auch seine Grenzen, insbesondere wenn es um über die Vertragsbeziehung hinausgehende Werbung oder Ansprache der Betroffenen geht.

Die Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) hat in der Öffentlichkeit große Aufmerksamkeit gefunden. Nach dem 25.05.2018 wurde vielfach der Eindruck erweckt, dass man für nahezu jede Datenverarbeitung eine Einwilligung brauche. Diese fälschliche Übertreibung konnte nach und nach zurechtgerückt werden. Die Einwilligung bleibt für die Beziehungen im Privatrechtsverkehr nach wie vor ein zentrales Element. Dabei sind die Fragen der Informiertheit und der Freiwilligkeit immer wieder zu diskutieren.

Am schwersten fassbar ist die Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 lit. f DS-GVO). Es handelt sich dabei deshalb nicht um einen Auffangtatbestand, weil zunächst Vertrag und Einwilligung zu prüfen sind, dann aber nicht automatisch das berechtigte Interesse greift. Vielmehr bedarf die Inanspruchnahme eines berechtigten Interesses einer Begründung und grundsätzlich auch der Dokumentation dieser Begründung. Es muss klar sein, warum der Verantwortliche in dem konkreten Zusammenhang ein berechtigtes Interesse hat. In der Datenschutz-Grundverordnung ausdrücklich genannt ist die Direktwerbung als

Ausdruck berechtigten Interesses (Erwägungsgrund 75). Das berechtigte Interesse stellt jedoch keinen Freibrief für jedwede Datenverarbeitung dar.

In der Praxis spielen die Informationspflichten der Art. 13 und 14 DS-GVO eine erhebliche Rolle. Dies betrifft nicht zuletzt die Datenschutzerklärungen im Internet hinsichtlich des Besuches von Webseiten. Die Informationspflichten treffen etwas zu undifferenziert alle Verantwortlichen. Zugleich sind die Regelungen detailliert und ausgefeilt. Die Kombination von Verpflichtung zur Information und weitreichenden Anforderungen an die Aussagekraft der Information erlegt kleineren und mittleren Unternehmen oder einzelnen Verantwortlichen nicht unerhebliche Lasten auf. Auf der anderen Seite ist zu betonen, dass die Information der Betroffenen unabdingbar ist, um diesen die Entscheidung über das Ob und das Wie der Datenverarbeitung zu ermöglichen. Es ist eine zentrale Vorbedingung für die Inanspruchnahme einer Webseite oder die Beantragung eines Newsletters, dass über Umfang und Zweck der Datenverarbeitung informiert wird.

Das in der Praxis zentrale Auskunftsrecht ist inhaltlich in seiner Reichweite umstritten. Der Art. 15 DS-GVO enthält nicht nur das Recht auf Auskunft, sondern auch das Recht auf Kopie. Das Verhältnis dieser Berechtigungen zueinander und die Frage, ob damit eine begrenzte oder umfassende Auskunftserteilung erzielt werden kann, sind nicht letztlich entschieden. Eine Reihe von Entscheidungen der Gerichte beschäftigt sich mit diesen Fragen. Dem Grunde nach ist festzuhalten, dass das Auskunftsrecht sich nicht notwendig auf Überblicke und Listen beschränkt, sondern durchaus auch einzelne Informationen über den Betroffenen beinhaltet, die beim Verantwortlichen vorliegen. Allerdings kann ein gestuftes Vorgehen sinnvoll sein, bei dem zunächst ein Überblick beim Verantwortlichen abgefragt wird, der dann ein konkretisiertes und bestimmteres Auskunftsersuchen der betroffenen Person ermöglicht, das der Verantwortliche effektiv erfüllen kann.

In der Praxis und in der Theorie relevant ist auch die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO. Zwar war dieses Rechtsinstrument bereits in der Richtlinie 95/46 enthalten, wurde aber in der Bundesrepublik Deutschland nicht zur Anwendung gebracht. Daher liegt hier nun ein für die Bundesrepublik neues Instrument vor, das ausgestaltet werden muss. Die Abgrenzung zu den Fällen der Auftragsverarbeitung nach Art. 28 DS-GVO

scheint eigentlich rechtlich klar zu sein. Dennoch bestehen im faktischen Geschäftsverkehr zwischen Privaten Probleme, weil Unsicherheit über die Rechtsgrundlagen herrscht. Dennoch wird die gemeinsame Verantwortlichkeit von vielen Unternehmen genutzt, um Kooperationen im Hinblick auf die Datenverarbeitung zu gestalten.

Als weitere rechtliche Diskussionspunkte, die auch praktische Auswirkungen haben, stellen sich das Führen des Verzeichnisses der Verarbeitungstätigkeit nach Art. 30 DS-GVO und die Ausgestaltung der Meldepflichten nach Art. 33 DS-GVO dar. Das Verzeichnis der Verarbeitungstätigkeiten muss zumindest einen mittleren Abstraktionsgrad aufweisen. Es darf nicht zu allgemein sein, weil es den Verantwortlichen dazu anhalten soll, sich der Datenverarbeitung bewusst zu machen und Risiken von Verletzungen des Datenschutzrechts zu verringern. Auf der anderen Seite ist eine zu detaillierte Ausfeilung nicht angezeigt, weil hier möglicherweise ein überzogener Aufwand betrieben werden muss, der dem Ziel des Verzeichnisses nicht entspricht. Die Meldepflicht des Art. 33 DS-GVO entsteht dann, wenn ein Datenschutzverstoß vorliegt. Es entfällt nur dann, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 Satz 1 DS-GVO). In welchen Fällen dies zutrifft, ist in der Praxis umstritten und wird auch unterschiedlich gehandhabt. Hier bedarf es weiterer Konkretisierung durch die Praxis der Behörden.

7. Entwicklungen

Die Datenschutz-Grundverordnung wird in ihrem Kerngerüst auf absehbare Zeit unverändert bleiben. Vereinzelte Stellschrauben mögen bewegt werden, etwa in der Ausgestaltung des innerstaatlichen Rechts. Dies hat etwa das zweite Datenschutz-Anpassungs- und Umsetzungsgesetz getan, indem das BDSG im Jahr 2019 erneut geändert wird. Danach wird die Benennungsschwelle des § 38 Abs. 1 BDSG von 10 auf 20 Beschäftigte gehoben. Dies soll allerdings nicht als Signal verstanden werden, dass der Datenschutz nun eine geringere Rolle spielt als im Jahr 2017 oder 2018. Vielmehr ist eine Entlastung von kleinen und mittleren Unternehmen oder auch Vereinen bezweckt. Die Sinnhaftigkeit dieser Gesetzesänderung kann dahinstehen. Jedenfalls ist klar, dass die weiteren Verpflichtungen der Datenschutz-Grundverordnung in Kraft bleiben.

Daneben sind weitere rechtspolitische Entwicklungen von Bedeutung auch für den Datenschutz. Der Brexit kann dazu führen, dass das Vereinigte Königreich von Großbritannien und Nordirland nicht mehr der DS-GVO unterliegt. Ein No-Deal-Brexit könnte also auch auf diesem Gebiet zu einem teils chaotischen Zustand führen. Möglichst schnell sind hier Rahmenbedingungen herzustellen, indem etwa das Vereinigte Königreich die Regelungen der Datenschutz-Grundverordnung in paralleler Weise für sich in Kraft setzt. Die Vorbilder Norwegen und Schweiz können hier Anregungen bieten.

Ein weiterer Fakt der Unwägbarkeit ist die E-Privacy-Verordnung. Sie ist weiter in der Diskussion, aber immer noch nicht in Kraft. Ihre Inhalte, die gerade den Datenschutz im Internet bei Telekommunikation und Telemedien sowie sozialen Netzwerken betreffen, sind weiter offen.

Die Kooperation der Datenschutzaufsichtsbehörden in Deutschland und Europa ist weiter zu verbessern. Denn die Harmonisierung der Anwendungspraxis in Europa bedarf weiterer Anstrengungen. Effektive Durchsetzung des Datenschutzrechts ist ein wichtiges Element der Datenschutz-Grundverordnung, weil sie Voraussetzung für die Harmonisierung der Bedingungen für den digitalen Binnenmarkt ist.

8. Ausblick

Die Datenschutz-Grundverordnung ist ein Erfolg. Trotz aller mehr oder weniger berechtigter Kritik an einzelnen Vorschriften hat sie eine Reihe von generellen Zielen erreicht. Datenschutz wird mehr und besser wahrgenommen. Die Effektivität der Durchsetzung konnte gesteigert werden. Eine Harmonisierung der Rahmenbedingungen für Datenverarbeitungen innerhalb der EU ist zumindest bis zu einem gewissen Grad möglich. Die Wirtschaft setzt allerdings insoweit mit Kritik an, als ergänzende innerstaatliche Regelungen doch wieder zu Unterschieden führen. Derartige Regelungen betreffen ergänzendes Datenschutzrecht wie das BDSG, aber auch Regelungen des innerstaatlichen Arbeitsrechts, Steuerrechts oder Handels- und Gesellschaftsrechts.

Wirksamer Datenschutz ist eine Aufgabe, die alle gemeinsam betrifft. Die betroffenen Bürgerinnen und Bürger können und sollten ihre Rechte offensiv wahrnehmen. Zentrales Instrument ist die Beschwerde. Die Verantwortlichen sind aufgrund ihrer Selbstregulierung gehalten, Datenverarbeitungen datenschutzkonform durchzuführen. Dies ist eine Daueraufgabe, die ein konsistentes und kontinuierliches Datenmanagement erzwingt. Die Datenschutzaufsichtsbehörden des Bundes und der Länder, und für die Datenschutzaufsicht der Kirchen gilt nichts anderes, werden weiter mit Augenmaß und Durchschlagskraft dem Datenschutz zur Geltung verhelfen. Denn Datenschutz ist Grundrechtsschutz und die Wahrung der Grundrechte ist die vornehmste Aufgabe der Datenschutzaufsichtsbehörden.

Erfahrungsbericht zum KDG aus Sicht einer kirchlichen Datenschutzaufsicht

Steffen Pau

Seit Ende Mai 2018 begleitet uns das neue Datenschutzrecht. In ihren Beiträgen berichten Herr Prof. Dr. Kugelmann über die Erfahrungen der staatlichen Datenschutzaufsichten mit dem neuen Recht und Herr Baumann-Gretza aus der Perspektive des kirchlichen Gesetzgebers über den Weg zum neuen kirchlichen Datenschutzrecht und die Rückmeldungen aus einem Jahr Anwendung der Regelungen. Diese Ausführungen sollen nachfolgend um die Perspektive der kirchlichen Datenschutzaufsichten ergänzt werden.

1. Neue Aufgaben und Befugnisse für die Datenschutzaufsichten

Im letzten Jahr standen die kirchlichen Datenschutzaufsichten vor mehreren Herausforderungen. Teils decken sich diese Herausforderungen mit denen, die auch die staatlichen Datenschutzaufsichten zu bewältigen hatten. Teils waren diese Herausforderungen aber auch kirchenspezifisch.

Das neue Gesetz über den Kirchlichen Datenschutz (KDG) brachte nicht nur für die kirchlichen Einrichtungen, sondern auch für die Datenschutzaufsichten neue Aufgaben und Umsetzungsaufträge mit sich, die bis zum Inkrafttreten des neuen Gesetzes im Mai 2018 zu erledigen waren. Ebenso wie die staatlichen Datenschutzaufsichten standen auch das Katholische Datenschutzzentrum und die anderen kirchlichen Datenschutzaufsichten vor der Aufgabe, die Anforderungen des neuen Datenschutzrechts an die Aufsichten zu identifizieren und umzusetzen. Ein Beispiel dafür ist die elektronische Plattform zur Meldung von Datenschutzverletzungen und zur Meldung der betrieblichen Datenschutzbeauftragten an die Datenschutzaufsicht, die das Katholische Datenschutzzentrum zusammen mit den anderen Diözesandatenschutzbeauftragten rechtzeitig zum Inkrafttreten des neuen Gesetzes im Mai 2018 bereitgestellt hat.

Neben diesen nach außen sichtbaren Veränderungen wurden auch interne Arbeitsabläufe umgestellt. Interne Prozesse zur Bearbeitung von Beschwerden wurden vor dem Hintergrund neuer Sanktionsmöglichkeiten und der gerichtlichen Überprüfbarkeit der Entscheidungen durch das kirchliche Datenschutzgericht überprüft und angepasst. Auch so vermeintlich einfache Aufgaben wie die Erstellung neuer Muster und Vordrucke konnten nicht immer so schnell erledigt werden, wie die kirchlichen Einrichtungen sich dies gewünscht hätten. Die grundlegenden, notwendigen Muster haben die Datenschutzaufsichten aber rechtzeitig zur Verfügung stellen können und diese anschließend durch weitere Hilfen fortlaufend ergänzt.

2. Herausforderung Umsetzungsfrist

Dabei war für alle kirchlichen Stellen die kurze Umsetzungsfrist für das neue kirchliche Gesetz eine Herausforderung. Dies war aber ein kirchenspezifisches Problem. Im Gegensatz zu den außerkirchlichen Stellen, die zwei Jahre im Voraus den Text der Europäischen Datenschutzgrundverordnung (DSGVO) kannten, wurde der Mustertext des neuen kirchlichen Gesetzes von den Gremien des Verbandes der Diözesen Deutschlands (VDD) erst im November 2017 verabschiedet - ein halbes Jahr vor dem geplanten Inkrafttreten. Auch wenn auf Grund der Regelung des Art. 91 Abs. 1 DSGVO abzusehen war, dass sich das neue kirchliche Datenschutzgesetz an der DSGVO orientieren würde, waren der Wortlaut und die genaue Umsetzung der Vorgaben der DSGVO erst mit dem Vorliegen des Mustertextes des VDD bekannt. Dies haben die kirchlichen Datenschutzaufsichten auch in den Wochen nach dem Inkrafttreten des neuen Gesetzes im Blick gehabt, wenn in Beschwerdefällen oder bei sonstigen Prüfungen eine noch nicht vollständige Umsetzung der neuen Regelungen erkennbar war. Aber die Anforderungen des neuen Gesetzes mussten umgesetzt werden, auch wenn dies aus nachvollziehbaren Gründen teilweise vielleicht erst nach Inkrafttreten des KDG erfolgt ist.

3. Neues Gesetz – neuer Datenschutz?

Die kirchlichen Datenschutzaufsichten erreichten vor allem im ersten Halbjahr 2018 viele Rückmeldungen zu dem neuen Gesetz, die eine Umsetzung aller neuen Anforderungen für nicht möglich hielten in der kurzen Zeit bis zum Inkrafttreten und auch darüber hinaus. Haben sich mit dem neuen Gesetz aber wirklich alle datenschutzrechtlichen Anforderungen verändert? Oder hatte die Berichterstattung über die neuen Datenschutzgesetze und der enorm gestiegene Bußgeldrahmen der DSGVO dazu geführt, dass die Sensibilität für das Thema Datenschutz und die Anforderungen des Gesetzes gestiegen war?

Wenn man die Diskussionen der letzten Monate betrachtet, kann der Eindruck entstehen, dass von mancher Seite die neuen Regelungen abgelehnt werden, weil das neue Gesetz bisherige Prozesse zur Datenverarbeitung in Frage stellt. Auch war in der durch viele Berichte verunsicherten Stimmung ein deutlich erhöhter Bedarf an externer Beratung vorhanden.

Schon im Vorfeld der Verabschiedung der DSGVO auf europäischer Ebene hatte eine enorme Lobbyarbeit gegen die geplanten Regelungen der DSGVO eingesetzt. Auch durch diese Arbeit wurden alleine auf der Ebene des Europäischen Parlaments mehrere Tausend Änderungsanträge zum Entwurf der EU-Kommission eingebracht und beraten. Alleine schon dieser Umstand erklärt – zumindest teilweise – warum die DSGVO noch Ecken und Kanten hat. Hier mussten im parlamentarischen Verfahren Textelemente aus verschiedensten Quellen als Kompromiss gegenläufiger Änderungsanträge zum finalen Entwurf zusammengefasst werden.

Leider konnte man bei manchen Diskussionen, die seit der Verabschiedung der DSGVO im April 2016 in der Öffentlichkeit geführt wurden, den Eindruck gewinnen, dass es teilweise nur darum geht, die Unsinnigkeit der neuen Regelungen zu beweisen und nicht darum, das Ziel des Schutzes personenbezogener Daten bestmöglich zu erreichen. Ein Beispiel dafür war z.B. die Diskussion um die Frage, ob unsere Namen zukünftig noch auf den Klingelschildern stehen dürfen.

Neben diesen allgemein kritischen Debatten wurden aber auch noch kirchenspezifische Diskussionen geführt und (angebliche) Mängel des kirchlichen Gesetzes gerügt. So wird z.B. immer wieder vorgetragen, dass das

KDG beim Thema der Einwilligung erheblich von den Vorgaben der DSGVO abweiche. Hier sei das KDG viel schärfer als die DSGVO, da das KDG die Schriftform der Einwilligung als Standard verlange. Bei einem ersten Blick in den § 8 Abs. 2 KDG im Vergleich mit Art. 7 DSGVO scheint sich dieses Ergebnis auch zu bestätigen. Schaut man aber weiter, so findet sich im KDG der Hinweis, dass die Schriftform nicht notwendig ist, wenn wegen besonderer Umstände eine andere Form angemessen ist. Das KDG kennt also keineswegs nur die schriftliche Einwilligung. Auf der anderen Seite ist in Art. 7 Abs. 1 DSGVO vorgegeben, dass der Verantwortliche die Einwilligung nachweisen können muss. Dies wird er in der Regel aber nur dann können, wenn er die Einwilligung schriftlich vorliegen hat. Auf der einen Seite steht also das kirchliche Gesetz, das zwar Schriftform als Regelfall voraussetzt, aber je nach Sachverhalt auch Abweichungen von der Schriftform ermöglicht. Auf der anderen Seite gibt es eine EU-Verordnung, die zwar kein generelles Schriftformerfordernis kennt, aber den Verantwortlichen dazu verpflichtet, die Einwilligung nachweisen zu können. Überträgt man diese Anforderungen in die Praxis, so führen die beiden unterschiedlichen Formulierungen überwiegend zu gleichen Ergebnissen. Die meisten wichtigen Einwilligungen nach DSGVO werden auch weiterhin schriftlich eingeholt werden und Sonderfälle können auch nach KDG ohne Schriftform geregelt werden. An diesem Beispiel wird deutlich, dass eine sachliche und durchaus auch kritische Auseinandersetzung mit den Anforderungen des Gesetzes und daraus evtl. folgende Forderungen nach Gesetzesänderungen auch immer einen Blick auf die praktischen Auswirkungen der möglichen Änderungen haben sollten.

An anderen Stellen herrschte in den letzten Monaten Unsicherheit bei der Anwendung der neuen Regelungen, die vereinzelt auch heute noch nicht völlig ausgeräumt werden konnte. So haben wir als Datenschutzaufsichten der katholischen Kirche beispielsweise im letzten Jahr durchgehend über das Thema der Veröffentlichung von Fotos und die Voraussetzungen dazu beraten. Eine Diskussion, die - wie an vielen anderen Stellen auch - nicht kirchenspezifisch war und die im außerkirchlichen Bereich auch geführt wurde und noch geführt wird. Die Lösungsfindung in der Konferenz der Diözesandatenschutzbeauftragten ist begleitet von Diskussionen zwischen den Aufsichten und innerhalb der Häuser – immer geleitet vom Wunsch, die beste Lösung – gesetzeskonform und praktikabel – zu finden. Dabei haben wir den jeweiligen Meinungsstand in der Literatur, die wenigen Gerichtsentscheidungen zu dem Thema und natürlich auch die

Äußerungen der anderen Datenschutzaufsichten im Auge behalten und unsere Beschlüsse angepasst, soweit uns dies notwendig erschien.

4. Vergleich konkreter Aufgaben nach altem und neuem Recht

Auch wenn das KDG neue Elemente enthält, so zeigt ein Vergleich ausgewählter Instrumente des Gesetzes nach altem und nach neuem Recht die Kontinuität der Grundlagen des Datenschutzes und der sich ergebenden Handlungsfelder zur Umsetzung des Datenschutzes in den Einrichtungen.

4.1 Verarbeitungsübersicht / Verfahrensverzeichnis

Bis 24. Mai 2018 verpflichtete § 3a KDO die verantwortlichen Stellen, ein Verzeichnis der Verfahren automatisierter Verarbeitungen zu führen. Nun sieht § 31 KDG vor, dass der Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten führen muss. Ein Vergleich der jeweils aufgeführten Pflichtinhalte des alten und des neuen Verzeichnisses zeigt, dass die grundlegenden Informationen gleichgeblieben sind. Im neuen Verzeichnis sind nur einige Informationen zusätzlich angelegt. Die vorhandenen Verzeichnisse nach KDO bilden daher eine gute Grundlage, um die Anforderungen an die neuen Verzeichnisse nach dem KDG abzubilden. Auf Basis des vorhandenen Verzeichnisses nach altem Recht kann die neue Anforderung umgesetzt werden, ohne die Einrichtungen zu überfordern. Das KDG gibt hier also keine neue Aufgabe auf, sondern modifiziert eine schon bestehende Aufgabe.

4.2 Verträge zur Auftragsverarbeitung / Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung war nach alter Rechtslage in § 8 KDO geregelt. Danach war unter den dort genannten Voraussetzungen ein Vertrag mit den Mindestinhalten des § 8 Abs. 2 KDO zu schließen. Die neue Rechtslage sieht in § 29 KDG ebenfalls einen schriftlichen Vertrag mit dem Auftragsverarbeiter vor. Dabei wird der Mindestinhalt in § 29 Abs. 3 und 4 KDG jetzt etwas ausdifferenzierter dargestellt. Die notwendigen Kern-

punkte der vertraglichen Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter sind aber vergleichbar. Auch hier konnten die schon nach altem Recht notwendigen Verträge als eine gute Grundlage für die Neufassung der Verträge dienen. Auch hier hat das KDG keine vollkommen neue Anforderung an die kirchlichen Stellen aufgestellt.

4.3 Datenschutz-Folgenabschätzung / Vorabkontrolle

Die Vorabkontrolle nach § 3 Abs. 5 KDO sah eine Prüfung automatisierter Verarbeitungen vor, wenn diese besondere Gefahren für die Rechte und Freiheiten der Betroffenen aufwiesen. Das neue Recht sieht in § 35 KDG die Datenschutz-Folgenabschätzung vor, die bei einem erwarteten hohen Risiko durch die geplante Verarbeitung durchzuführen ist. Auch hier ähneln sich beide Instrumente, mit denen jeweils im Vorfeld einer geplanten Verarbeitung personenbezogener Daten eine Risikofolgenabschätzung durchgeführt werden soll. Ziel beider Instrumente ist es Maßnahmen zu ergreifen, die die identifizierten Risiken ausschließen oder zumindest reduzieren.

4.4 Dokumentationspflichten / Accountability

Das neue Gesetz bringt an verschiedenen Stellen zum Ausdruck, dass die Maßnahmen zur Einhaltung des Gesetzes dokumentiert werden müssen. So gibt § 7 Abs. 2 KDG beispielsweise vor, dass der Verantwortliche für die Einhaltung der Grundsätze des § 7 Abs. 1 KDG nicht nur verantwortlich ist, sondern diese Einhaltung auch nachweisen können muss. Auch wenn das bisherige Recht diese Verpflichtung in diesem Umfang nicht kannte, so dürfte die Anforderung der entsprechenden Dokumentation nicht für alle kirchlichen Stellen neu gewesen sein. Viele Einrichtungen werden entsprechende Dokumentationen auch schon bisher im Rahmen des Qualitätsmanagements, der IT-Sicherheit oder anderer Compliance-Vorgaben vorgehalten haben. Spätestens aber für den Fall, dass die Datenschutzaufsicht nach der Umsetzung notwendiger Schutzmaßnahmen gefragt hätte, wäre eine Dokumentation dieser Maßnahmen zur Vorlage bei der Aufsicht auch nach altem Recht notwendig gewesen.

4.5 Betroffenenrechte und Informationspflichten

Die DSGVO und ihr folgend das KDG haben die Betroffenenrechte breiter ausgestaltet und die Informationspflichten bei der Datenverarbeitung erstmals ausführlich festgeschrieben. Hintergrund der Neufassung beider Regelungsbereiche war das zunehmende Informations-Ungleichgewicht zwischen dem Datenverarbeiter und dem Betroffenen. Hier haben die Gesetzgeber versucht, mit den Betroffenenrechten und den Informationspflichten die Waagschalen wieder etwas mehr ins Gleichgewicht zu bringen. Die Diskussionen der letzten Monate haben gezeigt, dass man auch diese gute Idee im Detail sicher noch verbessern kann. Eine eventuelle gesetzliche Novellierung auf EU-Ebene könnte der Frage nachgehen, wo die Mitteilung an den Betroffenen in der Praxis wirklich einen Mehrwert für den Betroffenen bietet und wo sie nur eine Formalie ist, mit der kein Zugewinn an Information und damit ein Ausgleich der beiden Waagschalen im obigen Sinne erreicht wird.

Es ist also nicht alles neu, was als Aufgabe im KDG beschrieben ist. Durch die gestiegene Sensibilität für das Thema Datenschutz bei den Nutzern kirchlicher Einrichtungen sowie bei den Einrichtungen selbst geraten aber eventuell einige Aufgaben jetzt erst ins Blickfeld der Einrichtungen, die vorher nur den Datenschutzexperten geläufig waren und wirken deshalb neu.

5. Ein Blick über den (kirchlichen) Tellerrand

Wenn wir als kirchliche Datenschutzaufsicht im konkreten Fall zu einer Frage mit den kirchlichen Stellen über den richtigen Umgang mit Daten diskutieren und eine praktikable und praxisnahe Lösung suchen, ist der Handlungsrahmen begrenzt, in dem wir kircheneigene Lösungen finden können. Auf Basis der von Art. 91 Abs. 1 DSGVO geforderten Vergleichbarkeit der datenschutzrechtlichen Regelungen können die kirchlichen Datenschutzaufsichten und die kirchlichen Einrichtungen bei der Auslegung des KDG und anderer kirchlicher Gesetze mit datenschutzrechtlichen Regelungen nicht erheblich von dem abweichen, was außerhalb der Kirche gilt, wenn es dafür keine kirchliche Besonderheit gibt, die eine solche Abweichung auch wirklich rechtfertigen würde.

An vielen Stellen erleben die kirchlichen Datenschutzaufsichten die Diskussionen über ihre Beschlüsse oder Äußerungen von sich zu einzelnen datenschutzrechtlichen Fragestellungen wie z.B. dem Verbot der dienstlichen Nutzung bestimmter Messenger so, als wenn sich die kirchlichen Datenschutzaufsichten diese Vorgaben nur für die kirchlichen Einrichtungen ausgedacht hätten. Auch hier hilft der Blick über den Tellerrand. Mit den Beschlüssen zu den Facebook-Fanpages und den Messengern erwarten die kirchlichen Datenschutzaufsichten nicht mehr als das, was die Landesdatenschützer für ihren Bereich ebenfalls diskutiert und beschlossen haben. Die Diskussion über die dienstliche Nutzung bestimmter Messenger gibt es im außerkirchlichen Bereich ebenso und etliche große Konzerne verbieten ihren Mitarbeitern auch deren dienstlichen Einsatz.

6. Umfassende Datensammlung

In dem Zusammenhang wird von den kirchlichen Stellen immer wieder vorgetragen, die Nutzung gerade dieser Dienste sei unumgänglich. Vielleicht hilft es an dieser Stelle nochmal darauf zu schauen, was denn mit den Daten passieren kann, die die großen Konzerne sammeln.

Wenn bei einem großen Messenger das Telefonbuch eines Smartphones an das Unternehmen übermittelt wird, dann kann dieses Unternehmen dem Nutzer nicht nur neue Kontakte vorschlagen, sondern es kann diese Kontakte auch in das Beziehungsnetzwerk einfügen, dass es aus den bisher bekannten Kontakten der anderen Nutzer hat. Davon betroffen sind dann auch die Kontakte, welche diesen Messenger gar nicht nutzen. Wenn zwei Freunde von mir meine Rufnummer im Telefonbuch gespeichert haben, dann erfährt der Messenger, dass ich mit beiden verbunden bin und über mich könnte ein Eintrag in dem Beziehungsnetzwerk angelegt werden, obwohl ich selbst den Messenger gar nicht nutze. Bei den Nutzern des Dienstes könnte die Beobachtung natürlich noch viel weiter gehen, da hier auf Grund der Nutzung ein viel detaillierteres Bild der Person gebildet werden kann.

„Ich habe ja nichts zu verbergen“ ist eine Antwort, die wir an dieser Stelle dann immer wieder zu hören bekommen. Aber diese Datensammlungen können eben Auswirkungen haben, die über die Nutzung des konkreten Dienstes hinausgehen. So ergeben sich in diesem Zusammenhang Fragen,

die weit über die datenschutzrechtlichen Themen hinausgehen und in den politischen oder ethischen Bereich hineinreichen.

Auch wenn die Kommunikation bei einem der großen Messengerdienste mittlerweile verschlüsselt abläuft und dieser Dienst nach eigenen Aussagen keinen Zugriff auf die Inhalte der Kommunikation hat, so kann dieser Dienst immer noch auf die Metadaten der Kommunikation zugreifen. Im Beispiel weiß der Messengerdienst zwar nicht mehr, was ich meinen Kontakten schreibe, aber er weiß mit wem ich wie häufig in Kontakt trete. Und diese Metadaten der Kommunikation verraten schon mehr, als es auf den ersten Blick ersichtlich ist.

So berichtete die Zeitschrift t3n[1] schon 2014 von einer Studie der Standford University, die auf Basis des Gerätelogs und der Telefonhistorie eines Smartphones belastbare Aussagen zu privaten Informationen, beispielsweise zu Liebschaften (durch häufige Telefonate auch zu späteren Uhrzeiten), zur Religionszugehörigkeit (Kontakt zu Seiten oder Personen, die der Religion eindeutig zuzuordnen sind) oder zu gesundheitlichen Problemen (Kontakte zu einschlägigen Fachärzten oder Portalen) machen konnte. Als anschauliches Beispiel zitiert die Zeitschrift den Fall einer Frau, die erst ihre Frauenärztin anruft, dann ihren Mann und anschließend eine Abtreibungsklinik kontaktiert. Hier kann aus den Metadaten der Gespräche wohl ohne große Probleme der grobe Inhalt der Kommunikation abgeleitet werden.

Vielleicht wird dies noch greifbarer, wenn die Datensammlung unserer Online-Nutzung in die analoge Welt übertragen wird, um zu verdeutlichen, was dort passiert.

Wie würden Sie reagieren, wenn bei Ihnen zu Hause eine Person immer wieder in alle Ihre Schränke schaut um zu erkennen, welche Kleidung Sie bevorzugen, welche Hygieneartikel und Kosmetik Sie benutzen und welche Lebensmittel Sie einkaufen. Nach Verlassen Ihres Hauses oder Ihrer Wohnung läuft diese Person immer hinter Ihnen her und beobachtet Ihre Handlungen. Während Sie durch die Einkaufsstraße schlendern, schreibt

1 „Wer bist du wirklich? Stanford-Studie beweist Brisanz von Metadaten" vom 14. März 2014 auf https://t3n.de/news/metadaten-brisant-stanford-studie-534512/ abgerufen am 26.05.2019.

die Person mit, welche Gegenstände Sie sich in den Schaufenstern anschauen, stoppt die Zeit mit, die Sie vor dem Schaufenster verweilen oder die Sie in einem Geschäft verbringen und analysiert, was Sie mit anderen Personen besprechen. Zwischendurch fragt die Person Sie nach Ihrem Auto oder dem Ticket des öffentlichen Nahverkehrs, das Sie nutzen. Der Bäcker, bei dem Sie ein Brötchen kaufen, fragt Sie erstmal, was Sie gestern so gemacht haben und möchte wissen, wo Sie als nächstes hingehen. Außerdem möchte er noch wissen, welche Freunde Sie haben und fragt nach deren Telefonnummern.

Mit der Zeit merken Sie, dass Ihre Begleitperson immer gezielter nachfragt und viele Ihrer Antworten schon vorausahnt. Beim weiteren Gang durch die Fußgängerzone merken Sie nun, dass sich die Inhalte der Schaufenster ändern, wenn Sie vor die Fensterscheibe treten und es sind immer mehr Sachen sichtbar, für die Sie sich an anderer Stelle interessiert haben[2]. Dieses Szenario ließe sich noch beliebig fortführen.

Dabei werden beim Tracking und der Profilerstellung heute Technologien eingesetzt, die weit über die immer diskutierten Cookies hinausgehen und die uns mit großer Wahrscheinlichkeit identifizieren können, auch wenn wir gerade nicht in einem Sozialen Netzwerk angemeldet sind und darüber identifiziert werden könnten. Anders als Überwachungsmaßnahmen durch Staaten werden solche Datensammlungen privater Unternehmen von den Nutzern hingenommen und die Nutzer helfen durch die intensive Nutzung der Dienste auch noch bei der Datensammlung mit[3].

7. Anfragen und Beschwerden an das Katholische Datenschutzzentrum

Die steigende Sensibilität in Bezug auf die eigenen Daten haben auch bei den kirchlichen Datenschutzaufsichten dazu geführt, dass sich die Eingaben im letzten Jahr deutlich erhöht haben. Die Beratungsanfragen sind mit der Verabschiedung des neuen Gesetzes Ende 2017 massiv gestiegen. Aber auch die Beschwerden haben sich deutlich erhöht und diese Eingaben steigen weiter. Die im kirchlichen Datenschutz jetzt erstmals formal

2 Beispiel in abgewandelter Form entnommen aus: Stefan Aust / Thomas Ammann, Digitale Diktatur, Bonn 2015, Aus der Einleitung „Willkommen in der digitalen Diktatur".

3 Vgl. Vortrag von Fr. Nocun zum Umfang der Datensammlung im Internet (S. 103).

geregelte Meldeflicht von Datenschutzverletzungen hat ebenfalls zu einer Vielzahl von Meldungen geführt.

8. Positive Entwicklungen im kirchlichen Datenschutz

Aus den letzten zwei Jahren gibt es aber auch viele positive Entwicklungen für den kirchlichen Datenschutz zu berichten. So können wir feststellen, dass den betrieblichen Datenschutzbeauftragten im Durchschnitt mehr Zeit für die Erledigung der gesetzlichen Aufgaben gegeben wird. Auch der Ausbildungsstand der betrieblichen Datenschützer wird immer besser. Hier haben die Einrichtungen bzw. die (Erz-)Diözesen für die Einrichtungen in personelle Kapazitäten investiert und die Fachkunde der Personen weiter verbessert.

Ebenfalls positiv können wir als Datenschützer feststellen, dass die Organisation der IT-Sicherheit in den (Erz-)Diözesen an vielen Stellen institutionalisiert worden und mehr in den Fokus der Verantwortlichen gerückt ist. Dies ist aus Sicht der Datenschutzaufsichten sehr zu begrüßen, da der Datenschutz, der ja auch auf die Umsetzung der technischen Schutzmaßnahmen angewiesen ist, nur mit einer funktionierenden, systematischen Umsetzung der IT-Sicherheit in einer Einrichtung funktionieren kann.

9. Offene Punkte und neue Herausforderungen

Aber es gibt auch noch offene Punkte, über deren Umsetzung nachgedacht werden sollte.

Das KDG hat noch Ecken und Kanten, an denen man teilweise noch arbeiten kann und auch sollte. Da sich der kirchliche Gesetzgeber hierbei aber im Rahmen der Vorgaben des europäischen Gesetzgebers bewegen muss, ist schon jetzt ersichtlich, dass nicht alle Wünsche nach neuen oder geänderten Regelungen im KDG so umgesetzt werden können.

Auch in der Anwendung des Gesetzes gibt es noch Verbesserungsbedarf. Nach einem Jahr KDG kann nicht schon alles perfekt laufen. Die katholischen Datenschutzaufsichten werden im Rahmen ihrer Aufgaben mit den kirchlichen Stellen zusammen die Umsetzung des Gesetzes weiter

vorantreiben. Dazu führt das Katholische Datenschutzzentrum ab dem zweiten Halbjahr 2019 auch wieder verstärkt Prüfungen durch. In diesem Zusammenhang ist bei den Meldungen von Datenschutzverletzungen auffällig, dass bestimmte Bereiche von Einrichtungen deutlich weniger bis keine Datenschutzverletzungen melden als andere. Auch dies werden wir uns in den nächsten Monaten im Rahmen unserer Prüfungen genauer anschauen.

Neben den offenen Punkten bei der Umsetzung der bestehenden Gesetze warten aber auch schon die nächsten Aufgaben auf die Datenschutzaufsichten und die Einrichtungen. Mit dem Inkrafttreten der Durchführungsverordnung zum KDG zum 01. März 2019 sind Konkretisierungen zur Umsetzung des KDG von den Einrichtungen zu beachten. Hier sei nur beispielhaft die Absicherung elektronischer Kommunikation genannt, die in § 25 KDG-DVO geregelt wird. Auch durch die Folgen des Brexits können sich für kirchliche Einrichtungen Handlungszwänge ergeben, je nach endgültiger Ausgestaltung des Austritts Großbritanniens aus der EU.

10. Ein eigenständiger kirchlicher Datenschutz – eine richtige Entscheidung

Auch wenn es an der kirchlichen Umsetzung der DSGVO vereinzelt kritische Anmerkungen gibt, ist ein eigenständiger kirchlicher Datenschutz gut und wichtig. Die Kirche nutzt ihre verfassungsrechtlich garantierte Möglichkeit, die eigenen Angelegenheiten selbst zu regeln. Ein Recht, dass auf europäischer Ebene in Art. 91 DSGVO anerkannt und geschützt wird. Das eigene Gesetz bietet der Kirche die Möglichkeit, einige kirchenspezifische Fallgestaltungen gesetzlich zu regeln, die in der DSGVO nicht geregelt sind, ohne dabei das Datenschutzniveau der DSGVO zu unterschreiten. Die eigene kirchliche Datenschutzaufsicht hat einen tieferen Einblick in die zu beaufsichtigen Einrichtungen und kann so die Umsetzung und Einhaltung des Gesetzes besser garantieren, ohne dass dabei die von der DSGVO für die Datenschutzaufsichten geforderte Unabhängigkeit gefährdet wird. Die Entscheidung der DSGVO in Art. 91 für einen eigenen, an die DSGVO angelehnten kirchlichen Datenschutz und eine eigene kirchliche Datenschutzaufsicht ist daher der richtige Weg, um kirchliche Interessen zu berücksichtigen ohne dabei den europaweit gewollten einheitlichen Schutz der personenbezogenen Daten aufzugeben.

Alle Beteiligten sollten auch zukünftig den Datenschutz gemeinsam voranbringen. Ohne Panikmache. Praxisgerecht und im Sinne der Menschen, mit deren Daten die Einrichtungen umgehen und die das Kirchliche Datenschutzgesetz schützen will. Die kirchlichen Datenschutzaufsichten werden ihren Teil dazu beitragen.

Die Datenschutzgerichte der katholischen Kirche – erste Erfahrungen und Perspektiven

Prof. Dr. Gernot Sydow, M.A.*

1. Strukturen der kirchlichen Datenschutzgerichtsbarkeit

2018 hat die katholische Kirche in Deutschland ihr Datenschutzrecht grundlegend reformiert und an die Vorgaben der Datenschutz-Grundverordnung angepasst. Dazu hat die Kirche unabhängige Datenschutzaufsichten geschaffen, deren Funktion für den kirchlichen Bereich den Funktionen der Landesbeauftragten für Datenschutz für den staatlichen und den privaten bzw. privatwirtschaftlichen Bereich entspricht. Um eine adäquate personelle Besetzung zu ermöglichen, sind diese fünf kirchlichen Datenschutzaufsichten in der katholischen Kirche als überdiözesane Einrichtungen mit Zuständigkeiten für den Bereich mehrerer Diözesen errichtet worden. Die Rechtsformen für die Trägerschaft variieren je nach Bundesland, in der die jeweilige Datenschutzaufsicht ihren Sitz hat.[1] Damit sind die europarechtlich erforderliche Unabhängigkeit der Datenschutzaufsichten und zugleich eine klare Funktionstrennung gegenüber den betrieblichen Datenschutzbeauftragten kirchlicher Einrichtungen gewährleistet.

Rechtsstreitigkeiten aus dem Bereich des kirchlichen Datenschutzrechts sind der kirchlichen Datenschutzgerichtsbarkeit zugewiesen. Rechtsgrundlage bildet die Kirchliche Datenschutzgerichtsordnung (KDSGO). Sie ist von der Deutschen Bischofskonferenz aufgrund eines besonderen Mandats des Apostolischen Stuhles gemäß can. 455 § 1 CIC erlassen

* Bei dem Beitrag handelt es sich um die Schriftfassung des Vortrags, den der Verfasser am 28. Mai 2019 in Siegburg gehalten hat und der wesentlich auf einer Publikation des Verfassers über „Perspektiven der kirchlichen Gerichtsbarkeit – Die Datenschutzgerichte der katholischen Kirche als (über-) spezialisierte kirchliche Verwaltungsgerichtsbarkeit" (Kirche und Recht 2019, S. 1 – 8) beruht.

1 Beispiel: Das Katholische Datenschutzzentrum in Dortmund ist als rechtlich selbständige kirchliche Einrichtung in der Rechtsform einer Körperschaft des öffentlichen Rechts mit Zuständigkeit für die Erzdiözesen Köln und Paderborn und den Diözesen Aachen, Essen und Münster errichtet.

worden,[2] bildet also eines der wenigen Beispiele einer Gesetzgebung auf Ebene der Bischofskonferenz, während das materielle Datenschutzrecht des Kirchlichen Datenschutzgesetzes (KDG) auf einer Parallelgesetzgebung aller deutschen Diözesanbischöfe beruht.

Durch ein Errichtungsdekret der Bischöfe aller Bistümer im Bereich der Deutschen Bischofskonferenz, auf das § 1 I KDSGO Bezug nimmt, haben die Bischöfe mit Genehmigung der Apostolischen Signatur ein Interdiözesanes Datenschutzgericht als erste Instanz mit Sitz in Köln errichtet.[3] Dem Interdiözesanen Datenschutzgericht sind alle nach dieser Ordnung wahrzunehmenden Zuständigkeiten übertragen. Die Deutsche Bischofskonferenz hat mit Genehmigung der Apostolischen Signatur ein Datenschutzgericht der Deutschen Bischofskonferenz als zweite Instanz mit Sitz in Bonn geschaffen.[4]

Die Kirchlichen Gerichte in Datenschutzangelegenheiten sind zuständig für die Überprüfung von Entscheidungen der Datenschutzaufsichten der katholischen Kirche in Deutschland sowie für gerichtliche Rechtsbehelfe der betroffenen Person gegen den Verantwortlichen oder den kirchlichen Auftragsverarbeiter. Ein besonderes Verfahren zur Überprüfung der Rechtmäßigkeit von kirchlichen Rechtsnormen (Normenkontrollverfahren) ist nicht für statthaft erklärt worden.[5]

2. Erste Erfahrungen: Tätigkeit der Datenschutzgerichte im ersten Jahr

2018 gingen beim Interdiözesanen Datenschutzgericht drei Verfahren ein, bis Mai 2019 kamen zwei weitere dazu. Dabei handelt es sich um vier Klagen von Privatpersonen gegen das Verhalten kirchlicher Stellen. Zudem ging die Klage einer kirchlichen Einrichtung gegen eine Verfügung der Datenschutzaufsicht ein, welche die Untersagung einer bestimmten

2 Approbiert durch Beschluss der Vollversammlung der Deutschen Bischofskonferenz vom 20.02.2018, rekognosziert durch Dekret der Apostolischen Signatur vom 03.05.2018 und sodann promulgiert durch Schreiben des Vorsitzenden der Deutschen Bischofskonferenz vom 14.05.2018.

3 Vgl. can. 1423 § 1 CIC.

4 Vgl. can. 1439 § 1 CIC.

5 § 2 I KDSGO.

Datenverarbeitung betraf. Bußgeldklagen sind bisher nicht anhängig. Zu einem Verfahren in der zweiten Instanz, vor dem Datenschutzgericht der Deutschen Bischofskonferenz, ist es noch nicht gekommen.

Die Antragsteller der bisher anhängigen Verfahren wenden sich beispielsweise gegen die Weitergabe von Daten durch Kindertagesstätten an Jugendämter aufgrund einer befürchteten Kindeswohlgefährdung. In einem Verfahren dieser Art erging am 15. Mai 2019 der erste Beschluss des Interdiözesanen Datenschutzgerichts.[6] Der zugrundeliegende Sachverhalt betraf die aus Sicht des Antragstellers unzulässige Weitergabe von Sozialdaten durch die Kita-Leitung an das Jugendamt. Das Gericht stellte fest, dass keine Datenschutzverletzungen vorliegen, und wies die Anträge als unbegründet zurück. Vielmehr war die Weitergabe der Sozialdaten gem. § 8a IV 2, § 65 I 1 Nr. 5 SGB VIII, § 69 I Nr. 1, 2. Alt. SGB X aufgrund einer im streitgegenständlichen Zeitpunkt vorliegenden Kindeswohlgefährdung gerechtfertigt.

3. Richterinnen und Richter in der kirchlichen Datenschutzgerichtsbarkeit

Im Hinblick auf die zu erwartenden geringen Eingangszahlen üben alle Richterinnen und Richter ihr Amt als Nebenamt aus. Die Mitglieder des Interdiözesanen Datenschutzgerichts und des Datenschutzgerichts der Deutschen Bischofskonferenz müssen katholisch sein und sollen über Erfahrung in einem juristischen Beruf sowie in Datenschutzfragen verfügen. Anderweitige Tätigkeiten in abhängiger Beschäftigung dürfen das Vertrauen in die Unabhängigkeit und Unparteilichkeit des Richters nicht gefährden. Die Vorsitzenden und ihre Stellvertreter müssen die Befähigung zum Richteramt nach dem Deutschen Richtergesetz, die weiteren Richter einen akademischen Grad im kanonischen Recht oder die Befähigung zum Richteramt nach dem Deutschen Richtergesetz besitzen.[7]

6 Beschl.v. 15.Mai 2019 IDSG 01/2018.

7 § 3 IV KDSGO; die personelle Besetzung beider Gerichte wird diesen Anforderungen gerecht und ist veröffentlicht: https://dbk.de/de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/besetzung/ und https://dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-2-instanz/besetzung/.

Die Richter der kirchlichen Datenschutzgerichte werden jeweils für eine Amtszeit von fünf Jahren auf Vorschlag des Ständigen Rates der Deutschen Bischofskonferenz vom Vorsitzenden der Deutschen Bischofskonferenz ernannt. Die mehrmalige Wiederernennung ist zulässig.[8]

Das Interdiözesane Datenschutzgericht besteht aus sechs Personen, dem Vorsitzenden, dem stellvertretenden Vorsitzenden und vier beisitzenden Richtern. Es besteht aus zwei Spruchkörpern und entscheidet in der Besetzung mit dem Vorsitzenden oder dem stellvertretenden Vorsitzenden und zwei beisitzenden Richtern, wobei ein Mitglied des Spruchkörpers einen akademischen Grad im kanonischen Recht besitzen muss.[9]

Das in zweiter Instanz tätige Datenschutzgericht der Deutschen Bischofskonferenz besteht aus dem Vorsitzenden, dem stellvertretenden Vorsitzenden und acht beisitzenden Richtern. Seine Entscheidungen trifft es in der Besetzung mit dem Vorsitzenden oder dem stellvertretenden Vorsitzenden und vier beisitzenden Richtern, wobei zwei Mitglieder des Spruchkörpers einen akademischen Grad im kanonischen Recht besitzen müssen.[10]

Die Vorsitzenden und stellvertretenden Vorsitzenden zeichnen sich durch langjährige Erfahrungen und oft einer herausgehobenen Position in der staatlichen Gerichtsbarkeit aus. Die beisitzenden Richter sind zur Hälfte weltlich-rechtlich und zur anderen Hälfte kirchenrechtlich qualifiziert. Unter den Richtern in der ersten und zweiten Instanz befinden sich fünf Professoren, man mag es daher – ähnlich dem Bundesverfassungsgericht – als „Professorengericht" bezeichnen. Denn es gibt kaum Kirchenrechtler, die nicht im kirchlichen Dienst stehen; so bleiben die Lehrstuhlinhaber an staatlichen Universitäten.

Die Geschäftsstellen des Interdiözesanen Datenschutzgerichts und des Datenschutzgerichts der Deutschen Bischofskonferenz sind beim Verband der Diözesen Deutschlands (VDD) eingerichtet[11] und befinden sich im Sekretariat der Deutschen Bischofskonferenz in Bonn.

8 § 6 I KDSGO.
9 § 5 I KDSGO.
10 § 5 II KDSGO.
11 § 3 VII KDSGO.

4. Europarechtliche Grundlagen der kirchlichen Regelungsautonomie für das Datenschutzrecht

Die Datenschutz-Grundverordnung (DSGVO) eröffnet Religionsgemeinschaften einen Freiraum für eine eigenständige Datenschutzgesetzgebung, eine eigenständige Datenschutzaufsicht und eine eigene Rechtsprechung in Datenschutzfragen. Die einschlägige Norm des Art. 91 DSGVO kann schon aus Paritätsgründen keine reine Bestandsschutzregelung sein. Sie muss allen Religionsgemeinschaften offenstehen, die ein eigenes, den Schutzstandards der DSGVO entsprechendes Datenschutzrecht schaffen und fortentwickeln wollen.[12]

Aus deutscher Perspektive ist dies ein vertrautes Regelungskonzept: Die deutsche Rechtsordnung erstreckt die staatliche Gesetzgebung an verschiedensten Stellen ausdrücklich nicht auf Religionsgemeinschaften, sondern achtet das Selbstbestimmungs- und Selbstorganisationsrecht der Religionsgemeinschaften aus Art. 140 GG i.Vm. Art. 137 III WRV dadurch, dass kirchliche Institutionen und kirchliches Handeln einer kirchlichen Gesetzgebung unterworfen werden können. Ausprägung dieser Achtung auf der Ebene der einfachen Gesetze ist u.a. § 118 II BetrVG, nach dem das Betriebsverfassungsrecht keine Anwendung auf Religionsgemeinschaften und ihre karitativen und erzieherischen Einrichtungen unbeschadet deren Rechtsform findet. Auch sonst ist die deutsche Rechtsordnung autonomiefreundlich, beispielsweise indem die Rechtsprechung des BVerfG für den Bereich des Individualarbeitsrechts die Möglichkeit zur Festlegung spezifisch kirchlicher Loyalitätsanforderungen anerkannt hatte.[13]

12 Str. im Hinblick auf Teile des Wortlauts der Norm („bestehende Vorschriften", „zum Zeitpunkt des Inkrafttretens dieser Verordnung", „weiter angewandt"); deren restriktive Interpretation würde sich indes in einen offensichtlichen Widerspruch zu Art. 91 I, 2. Hs DSGVO setzen, wonach ja gerade ein Fortentwicklungsgebot für kirchliche Datenschutzregelungen besteht; im Übrigen ist das Paritätsargument kaum zu widerlegen. Wie hier Hense, in: Sydow (Hg.), Europäische Datenschutz-Grundverordnung – Handkommentar, 2. Aufl. 2018, Art. 91 Rn. 13 ff. Hingegen sieht Seifert, in: Simitis et al. (Hg.), Datenschutzrecht, 2019, Art. 91 Rn. 19, nur noch „Nachjustierungen" nach Inkrafttreten der DSGVO als zulässig an; noch deutlicher Herbst, in: Kühling/Buchner (Hg.), DSGVO/BDSG, 2. Aufl. 2018, Art. 91 Rn. 13, der explizit von einer „Bestandsschutzregelung" spricht.

13 So erstmals ausführlich BVerfG, Beschl. v. 4.6.85 – 2 BvR 1703/83 u.a., BVerfGE 70, 138.

Das europäische Unionsrecht achtet zwar ausdrücklich den Status der Kirchen und Religionsgemeinschaften, den sie nach den mitgliedstaatlichen Rechtsordnungen haben.[14] Gleichwohl zieht das Unionsrecht die Grenzen für eigenständige kirchliche Regelungskonzepte tendenziell enger, im Individualarbeitsrecht unter Berufung auf das Antidiskriminierungsrecht.[15] Explizite Normen, die Freiräume für eine eigenständige Gesetzgebung von Religionsgemeinschaften schaffen, waren im Unionsrecht bislang nicht vorhanden. Angesichts der Regelungsbereiche des Unionsrechts hatte es bisher auch kaum Sachbereiche gegeben, in denen ein entsprechendes Regelungskonzept nahegelegen hätte. Vor diesem Hintergrund ist es sehr bemerkenswert, dass der europäische Gesetzgeber mit Art. 91 DSGVO eine solche Norm für das Datenschutzrecht geschaffen hat.

Diese Entscheidung des europäischen Gesetzgebers zur Anerkennung kirchlicher Autonomie kann nicht einfach als Ergebnis erfolgreicher Lobbyarbeit deutscher Kirchenvertreter verstanden werden. Denn auch in zahlreichen anderen EU-Mitgliedstaaten machen Religionsgemeinschaften von Art. 91 DSGVO Gebrauch: für den Bereich der katholischen Kirche die Bischofskonferenzen in Polen, Italien, Spanien, Portugal, Österreich und der Slowakei sowie die Erzbischöfe von Malta und Luxemburg, so dass mit der einzigen Ausnahme Frankreichs in allen EU-Mitgliedstaaten mit größeren katholischen Bevölkerungsanteilen entsprechende kirchliche

14 Art. 17 I AEUV.

15 Siehe dazu etwa die beiden in jüngerer Zeit ergangenen Entscheidungen EuGH, Urt. v. 17.4.18 – C-414/16 (Egenberger), ECLI:EU:C:2018:257 sowie EuGH, Urt. v. 11.9.18 – C-68/17 (Chefarzt), ECLI:EU:C:2018:696, in denen es jeweils um die Rechtfertigung einer Ungleichbehandlung wegen der Religion geht, die unter bestimmten Voraussetzungen von Art. 4 II RL 2000/78/EG zugelassen wird. Gemeinsame Besprechung beider Entscheidungen bei Suttorp/Braun, KuR 2018, 269 ff. Zur Rechtssache Egenberger ferner Joussen, EuZA 2018, 421 ff. Zur Rechtssache Chefarzt ferner Thüsing/Mathy, BB 2018, 2805 ff.

Regelungen bestehen.[16] Art. 91 DSGVO kann daher nicht einer speziellen Rücksichtnahme auf ein angeblich besonders gelagertes Staat-Kirche-Verhältnis in Deutschland entspringen, sondern enthält offensichtlich für die große Mehrheit der EU-Staaten eine adäquate Regelungsoption.

Die Akzeptanz kirchlicher Autonomie durch das Europarecht ist nicht grenzenlos, sondern steht materiell unter der Bedingung, dass die kirchlichen Normen und Institutionen an die Standards der DSGVO angeglichen werden. Art. 91 DSGVO formuliert explizit als Bedingung für eine eigenständige kirchliche Datenschutzgesetzgebung, dass sie den Schutzstandards der DSGVO entsprechen muss bzw. bis zum Inkrafttreten der DSGVO diesen Standards anzupassen war. Soweit die deutsche Rechtsordnung, beispielsweise im kollektiven Arbeitsrecht oder im Stiftungsrecht, Regelungsfreiräume für autonome kirchliche Regelungen schafft, setzt sie implizit voraus, dass die kirchlichen Regelungen für den jeweiligen Schutzzweck ein vergleichbares Niveau gewährleisten. Die betriebliche Mitbestimmung kann im Einzelnen anders geregelt sein als unter der Geltung des BetrVG, die Strukturen kirchlicher Mitarbeitervertretungen können den kirchlichen Organisationsstrukturen entsprechend gestaltet werden – doch die betrieblichen Mitwirkungsbefugnisse kirchlicher Mitarbeiter können nicht grundsätzlich anders ausfallen als diejenigen von

16 Italien: Decreto Generale – Disposizioni per la tutela del diritto alla buona fama e alla riservatezza, das durch „operative Hinweise" ergänzt worden ist (Trattamento dei dati personali, tutela della privacy ed enti ecclesiastici: prime indicazioni operative per le diocesi); Luxemburg: Normes internes de l'Archevêché de Luxembourg en matière de protection des données, die durch Ausführungsbestimmungen ergänzt werden (dt. Fassung: Ausführungsbestimmungen zu den internen Richtlinien des Erzbistums Luxemburg bezüglich des Datenschutzes auf Grundlage der Datenschutz-Grundverordnung der Europäischen Union); Malta: The Archdiocese of Malta – General Decree on the protection of data; Niederlande: Algemeen Reglement Bescherming Persoonsgegevens Parochies 2018; Österreich: Decretum generale über den Datenschutz in der katholischen Kirche in Österreich und ihren Einrichtungen (Kirchliche Datenschutzverordnung); Polen: Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim; Portugal: Instrução sobre o direito de cada pessoa a proteger a própria intimidade; Slowakei: Zabezpečenie ochrany osobných údajov Rímskokatolíckou cirkvou v Slovenskej republike; Spanien: Decreto general de la Conferencia Episcopal Española sobre la protección de datos de la Iglesia Católica en España. Für die evangelischen Kirchen ist in den überwiegend protestantisch geprägten EU-Mitgliedstaaten ähnliches zu vermuten, nur fehlt eine leicht zugängliche Übersicht; verwiesen sei hier nur auf das für die Evangelische Kirche in Deutschland geltende EKD-Datenschutzgesetz (DSG-EKD).

Mitarbeitern säkularer Unternehmen und Betriebe, ohne dass § 118 II BetrVG seine Legitimation verlieren würde.

Wenn der staatliche deutsche Gesetzgeber kirchliche Eigenregelungen ermöglicht, vertraut er also darauf, dass die Kirchen in ihren Regelungen von sich aus adäquate rechtsstaatliche Standards verwirklichen. Die Grundlagen dieses Vertrauens erodieren indes seit einiger Zeit, einerseits weil eine kirchliche Prägung staatlicher Funktionsträger nicht mehr die Regel ist, andererseits aber auch, weil der kirchliche Umgang mit Missbrauchsfällen oder Finanzskandalen in den letzten Jahren nicht immer den Eindruck erweckt hatte, dass die katholische Kirche zur Etablierung adäquater rechtsstaatlicher Standards und Verfahrens willens oder in der Lage sei. Soweit die Kirchen beklagen, von der Öffentlichkeit oder staatlichen Stellen mit zunehmendem Misstrauen beäugt zu werden, handelt es sich weitgehend um ein selbstverschuldetes Problem. Es wird nach einem solchen Vertrauensverlust erheblicher Anstrengungen bedürfen, bis die – durchaus vorhandenen – Schritte in die richtige Richtung die allgemeine öffentliche Einschätzung der Kirche wieder wenden werden.

Gerade vor diesem Hintergrund war es eine richtige Entscheidung, die von Art. 91 DSGVO eröffneten Möglichkeiten zu nutzen, auch wenn der damit verbundene organisatorische und finanzielle Aufwand für die Etablierung neuer kirchlicher Aufsichtsstellen und neuer Gerichte innerkirchlich nicht unumstritten war. Die Kirche kann nun im Bereich des Datenschutzes unter Beweis stellen, dass eine Vergleichbarkeit kirchlicher und staatlicher Schutzstandards erreichbar ist, ohne dass dazu Unterschiede zwischen säkularen und religiösen Einrichtungen nivelliert und kirchliche Institutionen unmodifiziert staatlichen Regelungen unterworfen werden müssten.

Es kann dabei indes nicht darum gehen, kirchliche Eigenständigkeit um der Eigenständigkeit willen zu demonstrieren. Vielmehr bedürfen Abweichungen von konkreten Regelungen des staatlichen oder europäischen Rechts einer nachvollziehbaren, auf die religiöse Prägung rückführbaren Begründung. Fehlt es daran, spricht alles dafür, die kirchlichen Regelungen nicht nur in ihrem Schutzniveau, sondern auch in ihren Einzelheiten dem staatlichen bzw. europäischen Recht anzupassen. Soweit das normativ durch wörtliche Übernahme von DSGVO-Normen in das kirchliche Datenschutzrecht geschehen ist, spricht zudem methodisch alles für eine Parallelitätsvermutung bei der Auslegung dieser Normen: Präjudizien

staatlicher Ober- und Höchstgerichte werden für die kirchlichen Datenschutzgerichte zwar nicht formal bindend, aber doch im hohen Maße beachtlich sein. Auch die kirchliche Arbeitsgerichtsbarkeit orientiert sich seit ihrer Errichtung völlig zu Recht an der Rechtsprechung der staatlichen Gerichte, soweit die auszulegenden Normen wortlautidentisch sind.

Zugleich setzt dies die Personen, die mit verantwortlichen Aufgaben in den kirchlichen Datenschutzaufsichten und den beiden Datenschutzgerichten der katholischen Kirche betraut sind, unter eine doppelte Erwartung aus staatlicher und aus kirchlicher Perspektive, ihre Ämter in sachlicher Unabhängigkeit und mit hoher fachlicher Expertise wahrzunehmen.

5. Bestandsaufnahme: Ausdifferenzierung – oder Zersplitterung? – der kirchlichen Gerichtsbarkeiten

Das Gerichtssystem der katholischen Kirche im Bereich der Deutschen Bischofskonferenz erreicht mit der Datenschutzgerichtsbarkeit eine Komplexität, die fragen lässt, ob die katholische Kirche nicht einen institutionellen Irrweg beschreitet. Zugespitzt formuliert: Die Kirche schafft seit einigen Jahren für jedes neue Problem eine neue Gerichtsbarkeit. Wann immer es in den letzten Jahren opportun oder geboten erschien, in einem bestimmten Sachbereich gerichtliche Rechtsschutzmöglichkeiten zu eröffnen, ist dafür eine neue Institution geschaffen worden. In der Regel handelt es sich nicht nur um ein einzelnes neues Gericht, sondern eine eigenständige neue, binnendifferenzierte Gerichtsbarkeit aus mehreren Gerichten in zumindest zwei Instanzen. Zu den Offizialaten sind so mittlerweile je nach Bistum schon vier weitere Fachgerichtsbarkeiten hinzugetreten: Gibt es Kirchenbeamte, muss eine kirchliche Disziplinargerichtsbarkeit her. Muss das kollektive Arbeitsrecht der Kirche an staatliche Standards angeglichen werden, schafft die Kirche eine Kirchliche Arbeitsgerichtsbarkeit. Sollen die Wahlen zu kirchlichen Gremien vor allem in den Pfarreien ernst genommen werden, werden Wahlprüfungskammern errichtet. Ermöglicht die DSGVO ein eigenes kirchliches Datenschutzrecht, entstehen kirchliche Datenschutzgerichte. Die Errichtung einer kirchlichen Strafgerichtsbarkeit könnte in absehbarer Zeit der nächste Schritt in dieser Entwicklung hin zu immer weiteren, ausdifferenzierten Gerichtsbarkeiten sein.

Auch für die regionale Verortung dieser Gerichte und ihre Zuordnung zu den Diözesen ist kaum eine Möglichkeit ausgelassen: Die Offizialate sind überwiegend diözesane, teils aber auch interdiözesane Gerichte, mit einer zweiten Instanz auf der Ebene der Kirchenprovinzen. Beamtendisziplinarkammern bestehen jeweils isoliert in den Bistümern, die vereinzelt Kirchenbeamte ernennen. Die Kirchlichen Arbeitsgerichte sind interdiözesane Gerichte, wobei die Jurisdiktionsbezirke nicht mit den Kirchenprovinzen korrespondieren, sondern sich an den Bundesländern orientieren. Die zweite Instanz besteht auf Ebene der Deutschen Bischofskonferenz. Die Datenschutzgerichtsbarkeit umfasst nur zwei Gerichte, ein interdiözesanes Gericht für alle deutschen Bistümer als erste Instanz und das Datenschutzgericht der Deutschen Bischofskonferenz als zweite Instanz. Hinzu kommen vereinzelte Personalunionen, etwa durch Ernennung derselben Person zum Offizial durch zwei Bischöfe unter Aufrechterhaltung der institutionellen Eigenständigkeit der beiden Offizialate als diözesaner Gerichte.

Die Geschäftsbelastung oder die schlichte Anzahl von Verfahren vor den kirchlichen Gerichten können nicht als Argument für diese Vielgestaltigkeit des Gerichtssystems in Anspruch genommen werden. Allein die Offizialate (in Ehesachen) und die Kirchlichen Arbeitsgerichte (in Fragen des kollektiven Arbeitsrechts) verhandeln jedes Jahr eine nennenswerte Zahl anhängiger Verfahren. Die beamtenrechtlichen kirchlichen Disziplinargerichte sind angesichts der geringen Zahl von Kirchenbeamten weitgehend funktionslos und haben lediglich eine Reservefunktion für anders nicht lösbare schwerwiegende Konfliktfälle; Wahlprüfungsverfahren finden nur periodisch und punktuell im Zusammenhang mit der Wahl pfarrlicher Vertretungsgremien statt; in der kirchlichen Datenschutzgerichtsbarkeit sind im ersten Dreivierteljahr seit ihrer Errichtung nur drei Verfahren anhängig geworden.

Daran ist nicht zu kritisieren, dass für Streitigkeiten in immer mehr Fällen der Rechtsweg und damit der Zugang zu einem kirchlichen Gericht eröffnet wird. Dieser Entwicklungspfad ist überzeugend. Er schafft gewaltenteilende Strukturen, dient der geordneten Klärung und Entscheidung von Konflikten und trägt so zur Legitimation kirchlichen Handelns bei. Es ist aber kritisch zu fragen, ob die Zersplitterung kirchlicher Gerichtsinstitutionen der richtige Weg ist. Wo soll das hinführen: zu fünf weiteren kirchlichen Fachgerichtsbarkeiten in den kommenden Jahren? Das sollte man

nicht für schlichtweg undenkbar halten, denn vor dreißig Jahren hätte niemand die heutige Ausdifferenzierung der kirchlichen Gerichtsbarkeiten vorhersagen können.

Es ist noch so gut wie gar nicht reflektiert, was diese Zersplitterung der kirchlichen Gerichtsbarkeit für die Einheit des Kirchenrechts und der Kirchenrechtsprechung bedeutet. Eine Einrichtung, die dem Gemeinsamen Senat der obersten Bundesgerichte[17] vergleichbar wäre und die in ähnlicher Weise die Rechtsprechung unterschiedlicher Gerichtszweige zusammenführen könnte, existiert in der Kirche nicht. Stattdessen gibt es punktuelle Irritationen durch römische Gerichtsinstanzen, etwa 2010 durch das Urteil des Delegationsgerichts der Apostolischen Signatur zum kirchlichen Arbeitsrecht.[18]

6. Perspektive: Kirchliche Verwaltungsgerichtsbarkeit

Die ratio für die Errichtung immer weiterer kirchlicher Gerichtsbarkeiten kann nicht darin liegen, dass die Verfahrenszahlen nur so bewältigt werden könnten. Ganz im Gegenteil: Angesichts sehr überschaubarer Verfahrenszahlen ist der institutionelle Aufwand, um die Gerichte zu errichten, Rechtsgrundlagen für sie zu schaffen, sie mit Richtern zu besetzen und eine Geschäftsstelle vorzuhalten, teilweise höher als der konkrete Aufwand für die Durchführung der anhängigen Verfahren. Nur für die Offizialate und die Kirchlichen Arbeitsgerichte dürfte diese Grundlast in einem angemessenen Verhältnis zur Verfahrenszahl stehen.

Es lässt sich auch kaum behaupten, dass die Ausdifferenzierung des materiellen oder des Verfahrensrechts eine fachliche Spezialisierung erzwingen würde, die sich nur in eigenständigen Gerichtsbarkeiten erreichen ließe. Das Argument einer Eigenständigkeit von Verfahren und Entscheidungsmaßstäben dürfte für die Eheverfahren der Offizialate und die arbeitsgerichtlichen Streitigkeiten der Kirchlichen Arbeitsgerichte Plausibilität haben, nicht aber für die verschiedenen verwaltungsrechtlichen Streitigkeiten, für die die Kirche mittlerweile unter verschiedenen Namen Fach-

17 Art. 95 III GG.

18 Urt. v. 31.03.10 – 42676/09 VT (Az. KAGH M 13/08 u. M 01/10); abgedruckt in ZMV 2010, 145 ff.; dazu kritisch Eder, ZMV 2010, 149 ff.; Ihli, ZMV 2010, 151 f.; Joussen, ZMV 2010, 152; Fey, ZMV 2010, 152 f.

gerichtsbarkeiten errichtet hat. Die staatliche Verwaltungsgerichtsbarkeit verhandelt jedenfalls vergleichbare Streitigkeiten und noch ein weitaus größeres Verfahrensspektrum im Rahmen einer einzelnen Gerichtsbarkeit, allenfalls spezialisiert und ausdifferenziert in verschiedenen Kammern oder Senate, also durch Spezialisierung der Spruchkörper innerhalb einer organisatorisch einheitlichen Gerichtsbarkeit. Die organisatorischen Vorteile einer solchen einheitlichen Gerichtsstruktur liegen auf der Hand, insbesondere wenn die Zahl der Verfahren in den einzelnen Sachbereichen sehr überschaubar ist.

Die Diskussion über die Errichtung einer kirchlichen Verwaltungsgerichtsbarkeit wird üblicherweise unter anderen Gesichtspunkten als hier geführt, nämlich als Diskussion über die Schaffung von Rechtsschutzmöglichkeiten, über die Verhinderung von Machtmissbrauch und über eine Erhöhung der Legitimation kirchlichen Handelns. Der Vorsitzende der Deutschen Bischofskonferenz Kardinal Marx hat zum Abschluss der Frühjahrsvollversammlung der Deutschen Bischofskonferenz im März 2019 erklärt: „Was getan werden muss, um den nötigen Machtabbau zu erreichen und eine gerechtere und rechtlich verbindliche Ordnung aufzubauen, wird der synodale Weg klären. Der Aufbau von Verwaltungsgerichten gehört dazu."[19] Das ist eine überzeugende Perspektive, mit der implizit auch die Gegenpositionen gegen eine kirchliche Verwaltungsgerichtsbarkeit zurückgewiesen werden, die entweder den Nutzen einer solchen Gerichtsbarkeit in Abrede stellen oder sich auf ekklesiologische Scheinargumente zurückziehen, nach denen fundamentale, wenn nicht unüberwindbare theologische Hindernisse für eine kirchliche Verwaltungsgerichtsbarkeit bestehen sollen.

Diese Diskussion ist um eine zusätzliche Perspektive und ein zusätzliches Argument zu erweitern: Funktional sind kirchliche Verwaltungsgerichte in der katholischen Kirche in Deutschland bereits vorhanden, wenn auch unter anderen Bezeichnungen und in einer unsystematischen Weise mit zersplitterten Kompetenzen. Bei Lichte betrachtet kann es daher gar nicht um die Schaffung einer gänzlich neuen Gerichtsbarkeit gehen, sondern um eine überzeugende Gesamtstruktur, in der die vielfältig gewachsenen

19 Pressebericht des Vorsitzenden der Deutschen Bischofskonferenz vom 14. 03. 2019, S. 7 (https://dbk.de/fileadmin/redaktion/diverse_downloads/presse_2019/2019-040-Pressebericht-FVV-Lingen.pdf).

Rechtsprechungsstrukturen zusammengefasst werden und aufgehen müssen. Die Frage nach gerichtlichen Kontrollkompetenzen ist in dieser Perspektive dann keine Frage nach Errichtung einer gänzlich neuen Institution, sondern primär nach der Eröffnung des Gerichtszugangs für weitere Sachbereiche.

Die heutigen Diskussionslinien innerhalb der Kirche sind nicht ohne Parallelen zu den Diskussionen über die Schaffung einer Verwaltungsgerichtsbarkeit in den deutschen Territorien des 19. Jahrhunderts. Auch damals war es ein längerer Erkenntnisprozess, dass die Unterwerfung der monarchischen Exekutive unter eine unabhängige Gerichtskontrolle nicht dysfunktional ist, sondern dass sie im Gegenteil zur Legitimation des Verwaltungshandelns erheblich beitragen kann.[20] Die Fürsten schwankten zwischen der Sorge um die eigene Machtvollkommenheit und der Einsicht in Überzeugungskraft rechtsstaatlicher Reformforderungen. Das Enumerationsprinzip, nach dem die gerichtlichen Zuständigkeiten für jeden Sachbereich einzeln zugewiesen werden mussten und sich nicht im Wege der Generalklausel und damit letztlich schon aus der Errichtung der Verwaltungsgerichtsbarkeit als solcher ergaben, bot die Möglichkeit einer Kompromisslinie.

Die Verwaltungsgerichtsbarkeit der evangelischen Kirche ist nach diesem Muster aufgebaut: nach dem Muster einer institutionell einheitlichen Gerichtsbarkeit, deren Zuständigkeiten enumerativ bestimmt werden. Sie beschränken sich im Fall der evangelischen Verwaltungsgerichtsbarkeit auf Fragen des Pfarrerdienstrechts und auf die gerichtliche Überprüfung von Aufsichtsverfügungen der Landeskirchenämter.[21] Das sind durchaus zwei wesentliche, insgesamt aber doch alles andere als umfassende Zuständigkeiten. Die bloße Existenz der Institution innerhalb der evangelischen Kirche trägt also offenbar schon zur verbreiteten Annahme hoher rechtsstaatlicher Standards bei.

Es ist Zeit, den institutionellen Irrweg zu beenden, nach dem die katholische Kirche für jede Sachfrage eine neue Gerichtsbarkeit errichtet. Ein überzeugendes Sachargument für diese Überdifferenziertheit ist nicht zu

20 Ausführlich zu diesen zeitgenössischen Diskussionen Gernot Sydow, Die Verwaltungsgerichtsbarkeit des ausgehenden 19. Jahrhunderts, S. 12 ff.

21 Siehe hierzu die Bestimmung zur Eröffnung des Kirchlichen Verwaltungsrechtswegs in § 15 VwGG.EKD, insb. Abs. 1 Nr. 1 und 2.

finden. Die gegenwärtige Zersplitterung insbesondere der verwaltungsrechtlichen Fachgerichtsbarkeiten in der katholischen Kirche ist nicht nur organisatorisch von Nachteil, sondern vergibt die Möglichkeit, die eigenen Strukturen in eine breite Öffentlichkeit hinein als plausibel darzustellen. Der Nutzen ihrer Fortentwicklung zu einer kirchlichen Verwaltungsgerichtsbarkeit liegt auf der Hand.

Datenschutzmanagement mit dem Standard-Datenschutzmodell – (auch) ein Hilfsmittel zur Umsetzung des kirchlichen Datenschutzes

Gabriel Schulz

1. Datenschutz in der katholischen Kirche

Die Datenschutzvorschriften im Bereich der katholischen Kirche (Gesetz über den Kirchlichen Datenschutz – KDG) wurden gemäß Art. 91 Abs. 1 DS-GVO in enger Anlehnung an die Europäische Datenschutz-Grundverordnung (DS-GVO) entwickelt. Dies ist eine wichtige Voraussetzung für die Anwendung des Standard-Datenschutzmodells (SDM) bei der Umsetzung des KDG. Denn das SDM kann dadurch die Managementprozesse für den Datenschutz in der katholischen Kirche in vergleichbarer Weise unterstützen wie beim Datenschutz im staatlichen Bereich.

Die Organisation des Datenschutzes im KDG entspricht der der DS-GVO sehr weitgehend (Abb.1).

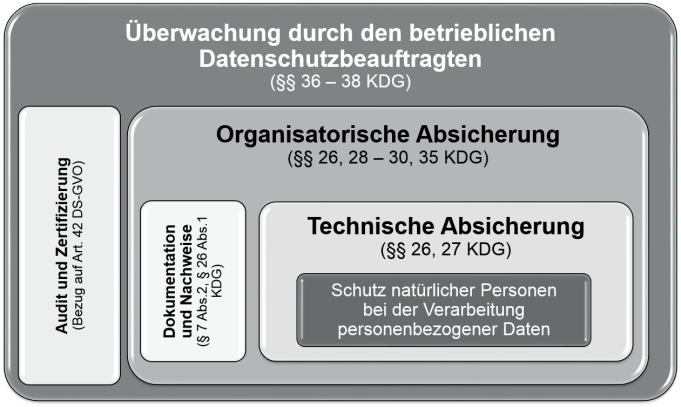


Abbildung 1: Schutzkonzept des KDG

Schon der Präambel des KDG ist zu entnehmen, dass es im Kern darum geht, die Grundrechte und Grundfreiheiten natürlicher Personen und

insbesondere deren Recht auf Schutz personenbezogener Daten bei der Verarbeitung dieser Daten zu schützen. Ein zentrales Mittel zur Gewährleistung dieses Schutzes sind technische und organisatorische Maßnahmen (§ 26 KDG), die bereits bei der Planung der Verarbeitungstätigkeiten (§ 27 KDG - Technikgestaltung und Voreinstellungen) zu treffen sind. Es müssen solche technischen und organisatorischen Maßnahmen getroffen werden, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Das Erreichen dieses Schutzniveaus muss nachgewiesen werden können (Rechenschaftspflicht).

2. Das Standard-Datenschutzmodell

Die Auswahl geeigneter Maßnahmen und der Nachweis der Wirksamkeit sind nicht trivial. Hier ist konzeptionelles Herangehen gefordert. Obwohl sich weder in der DS-GVO noch im KDG der Begriff „Konzept" findet, ist für jede Verarbeitungstätigkeit ein umfassendes Datenschutz- und IT-Sicherheitskonzept erforderlich, um der gesetzlich geforderten Rechenschaftspflicht (§ 26 Abs. 1 KDG) nachkommen zu können. Das SDM unterstützt die Erstellung derartiger Konzepte, indem es technische und organisatorische Maßnahmen auf der Basis von Gewährleistungszielen systematisiert und somit die Auswahl geeigneter Maßnahmen erleichtert. Die Gewährleistungsziele bündeln und strukturieren die datenschutzrechtlichen Anforderungen und können durch mit ihnen verknüpfte, skalierbare Maßnahmen operationalisiert werden. Auf diese Weise wird ein wirksamer Schutz Betroffener gewährleistet und die Minderung von Risiken für die Rechte und Freiheiten natürlicher Personen prüfbar sichergestellt.

Das SDM benennt sieben Gewährleistungsziele des Datenschutzes, welche für die Anwendung des SDM von elementarer Bedeutung sind: Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit und Datenminimierung. In diesen Gewährleistungszielen finden sich die seit vielen Jahren in der Praxis bewährten Schutzziele der Informationssicherheit wieder. Die Ziele Verfügbarkeit, Integrität und Vertraulichkeit dienten bisher vorrangig der Gewährleistung der Informationssicherheit in Behörden und Unternehmen, also der Absicherung und dem Schutz der Daten einer Organisation.

Abbildung 2 beschreibt die Beziehung der verschiedenen Schutzziele zueinander.

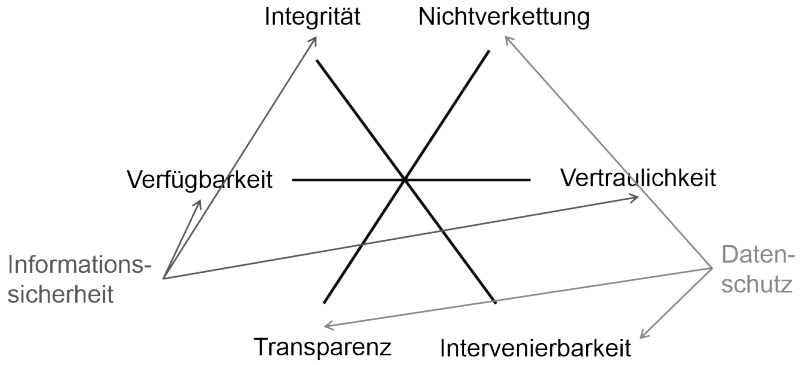


Abbildung 2: Systematisierung der Gewährleistungsziele des SDM

Datenschutz interpretiert Schutzziele jedoch nicht aus der Perspektive der Organisation, sondern aus der Perspektive der Betroffenen und betrifft die Gesamtheit der datenschutzrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten. Das SDM betrachtet daher die Gewährleistungsziele in ihrer Gesamtheit und erfüllt somit auch die Funktion, die bekannten Schutzziele der Informationssicherheit und die datenschutzrechtlichen Anforderungen für die Verarbeitung personenbezogener Daten als Gewährleistungsziele zusammenzuführen.

Um die Forderungen des KDG vollständig abbilden zu können, sind alle Gewährleistungsziele erforderlich. Abbildung 3 soll den Zusammenhang dieser Gewährleistungsziele verdeutlichen.

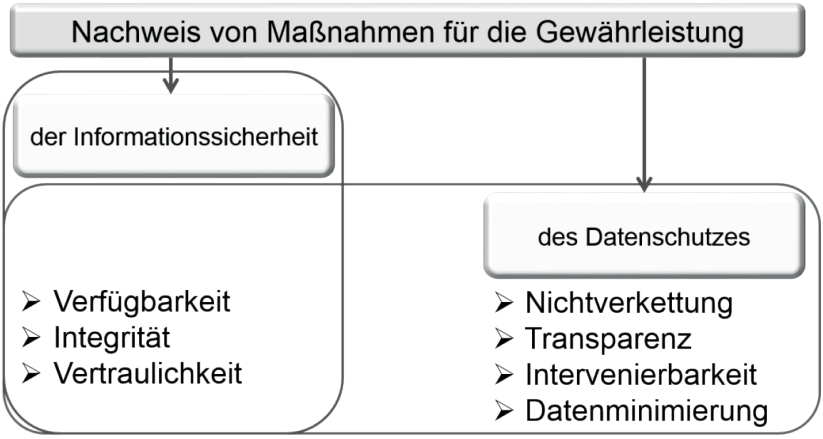


Abbildung 3: Zusammenhang der Gewährleistungsziele der Informationssicherheit und des Datenschutzes

3. Datenschutz und BSI-Grundschutz

Für die Auswahl der Maßnahmen im Bereich der Informationssicherheit hat sich die Grundschutzmethodik des Bundesamtes für die Sicherheit der Informationstechnik (BSI) bewährt. Die modernisierte Grundschutzmethodik erleichtert die Auswahl geeigneter Maßnahmen durch eine differenzierte Herangehensweise. Auch kleineren Organisationen kann die Grundschutzmethodik empfohlen werden, weil mit der so genannten Basisabsicherung recht schnell ein grundlegender Schutz vor den wesentlichen Bedrohungen für die Informationssicherheit erreicht werden kann.

Die Umsetzung der Grundschutzmethodik dient aber ganz wesentlich auch den Zielen des Datenschutzes, denn Informationssicherheit ist grundlegende Voraussetzung für die Gewährleistung eines angemessenen Datenschutzes. Grundschutz ist bezogen auf den Datenschutz allerdings nur „die halbe Miete". Neben den Maßnahmen zur Gewährleistung der Informationssicherheit sind auch Maßnahmen erforderlich, die vorrangig der Umsetzung von Betroffenenrechten dienen. Der BSI-Grundschutz bietet diese Maßnahmen nicht an, stellt jedoch eine sinnvolle Verbindung zwischen Informationssicherheit und Datenschutz her. Im Abschnitt 8.2 (Schutzbedarfsfeststellung) des BSI-Standards 200-2 wird darauf hingewiesen, dass auch im Datenschutz der Schutzbedarf fest-

gelegt werden muss, um angemessene technische und organisatorische Schutzmaßnahmen bestimmen und konfigurieren zu können. Dort wird auch festgestellt, dass das SDM eine ganze Reihe an Kriterien bietet, um das Risiko eines Grundrechtseingriffs zu bestimmen. Der Baustein CON.2 (Datenschutz) des BSI-Kompendiums fordert, dass geprüft werden muss, ob das SDM angewendet wird (CON.2.A1 - Umsetzung Standard-Datenschutzmodell).

4. Der Datenschutzmanagement-Prozess

Um die Anforderungen der Informationssicherheit und des Datenschutzes effektiv und vollständig umsetzen zu können, ist ein zyklischer Managementprozess erforderlich. Das SDM empfiehlt, diesen Managementprozess in Anlehnung an den bewährten PDCA-Zyklus auszugestalten. Der aus den vier Phasen Plan, Do, Check und Act bestehende Zyklus hat sich bspw. als kontinuierlicher Verbesserungsprozess beim Qualitätsmanagement seit vielen Jahren bewährt und ist grundlegender Bestandteil der Normenfamilien DIN EN ISO 9000, ISO 14000, ISO/IEC 20000 und insbesondere auch der ISO/IEC 27001. Der PDCA-Zyklus wird daher auch im BSI-Standard 200-1 (Managementsysteme für Informationssicherheit - ISMS) umgesetzt.

Datenschutzmanagement bezeichnet einen kontrollierten und gesteuerten Prozess über den gesamten Lebenszyklus einer oder mehrerer Verarbeitungstätigkeiten mit dem Ziel, die gesetzlichen und betrieblichen Anforderungen des Datenschutzes umzusetzen. Für die Anwendung des PDCA-Zyklus als Datenschutzmanagement-Prozess (DSM-Prozess) definiert das SDM dessen vier Phasen wie folgt:

- PLAN → Planen / Spezifizieren
- DO → Implementieren / Protokollieren
- CHECK → Kontrollieren / Prüfen / Beurteilen
- ACT → Verbessern

Abbildung 4 zeigt den DSM-Prozess als modifizierte Form des PDCA-Zyklus.

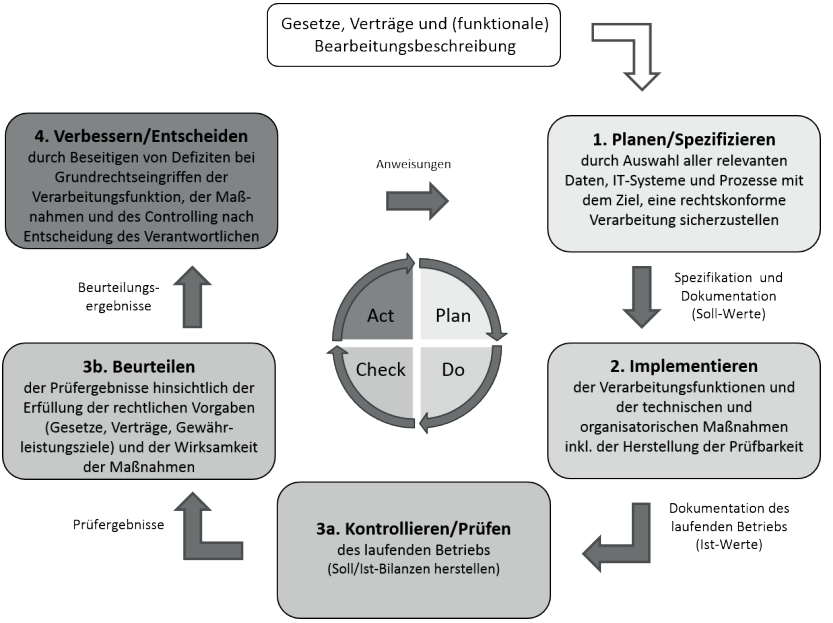


Abbildung 4: Der Datenschutzmanagement-Prozess

Vor dem Einstieg in den DSM-Prozess sind zunächst die rechtlichen Rahmenbedingungen der betreffenden Verarbeitungstätigkeit zu klären, deren datenschutzrechtliche Zulässigkeit zu prüfen und die Ergebnisse zu dokumentieren.

4.1 DSM-Phase 1 – Planen/Spezifizieren

Die erste Phase des DSM-Prozesses (Planen/Spezifizieren) dient der Auswahl aller relevanten Daten, IT-Systeme und Prozesse mit dem Ziel, eine rechtskonforme Verarbeitung sicherzustellen. Diese Phase des DSM-Prozesses beinhaltet die Teilphasen Planung, Spezifikation und Dokumentation.

Bei der Planung von Verarbeitungstätigkeiten sind folgende Aspekte zu betrachten:

- Beschreibung der Datenverarbeitung,
- Identifikation und Dokumentation aller beteiligten Akteure,
- Identifikation und Dokumentation der Rechtsgrundlagen,
- Durchspielen von Use-Cases, um Risikoquellen erkennen zu können (Angreifermodell),
- Bestimmung des Risikos für die Rechte und Freiheiten Betroffener,
- Erarbeitung einer Dokumentation mit funktionalen Anforderungen,
- Bestimmung technischer und organisatorischer Maßnahmen,
- Erstellung und förmliche Abnahme des Lastenheftes,
- Erstellung von Test- und Pilotierungskonzepten und
- Erarbeitung der Freigabeprozedur / des Freigabeprozesses.

Bei der Spezifikation einer Verarbeitungstätigkeit sind folgende Ebenen zu betrachten und darzustellen:

- die Gestaltung der Prozesse (Fachlichkeit), die den fachrechtlichen und datenschutzrechtlichen Anforderungen genügen müssen,
- die Nutzung einer Fachapplikation durch die Sachbearbeitung,
- die Technik der Datenverarbeitung, der Prozesse und Dienste und der IT-Systeme und IT-Infrastrukturen,
- die Schnittstellen von Prozessen und IT-Systemen sowie
- die jeweilige Administration der vorgenannten Ebenen.

Ziel der Dokumentation ist die Sicherung der Transparenz

- von Datenbeständen,
- von Transformationen zwischen Daten,
- der benutzten Systemkomponenten, deren Funktionen und Schnittstellen,
- der Prozesse innerhalb von IT-Systemen und Organisationen und über IT-Systemgrenzen und Organisationsgrenzen hinweg und
- der Nachvollziehbarkeit von Entscheidungen und Verarbeitungshandeln.

Bei der Erstellung der Dokumentation sind die folgenden formalen Anforderungen zu berücksichtigen:

- Strukturierung der Gesamtdokumentation,

- Dokumentation darüber, welcher Teil der Dokumentation der Verarbeitung als Papierausdruck und welcher Teil elektronisch vorliegt,
- Angemessenheit,
- Vollständigkeit,
- Revisionsfestigkeit,
- Aktualität und
- Fortschreibung.

Im Ergebnis der Planungsphase des DSM-Prozesses liegen alle funktionalen Sollwerte der Verarbeitungstätigkeit vor. Damit sind die Voraussetzungen gegeben, um später durch Vergleich mit den in der zweiten DSM-Phase gewonnenen funktionalen Ist-Werten die betreffende Verarbeitungstätigkeit kontrollieren und prüfen zu können.

4.2 DSM-Phase 2 – Implementieren

Die zweite Phase des DSM-Prozesses (Implementieren) beschreibt die eigentliche Entwicklung der Verarbeitungstätigkeit und die Implementierung der in der Planungs- und Spezifizierungsphase ermittelten technischen und organisatorischen Maßnahmen. Diese Phase kann im Wesentlichen die folgenden Aspekte beinhalten:

- Softwareentwicklung,
- Hardwareauswahl und -bereitstellung,
- Umsetzung der technischen und organisatorischen Maßnahmen und
- Starten aller Protokollierungsfunktionen.

Von besonderer Bedeutung für der Generierung von Ist-Werten sind alle Protokollierungsaktivitäten. Schon im Verlauf der Planung und Spezifizierung ist daher festzulegen, was protokolliert werden soll. Die folgenden Komponenten sind zu berücksichtigen:

- Zeitkomponente (Wann?),
- Instanz, die eine Aktivität auslöst (Wer?),
- Aktivität bzw. Ereignis, das durch die Instanz ausgelöst wurde (Was?),
- Speicherinstanz (Quelle und Ziel), die diese Protokolldaten speichert (Protokollierung durch wen?).

4.3 DSM-Phase 3a – Kontrollieren/Prüfen

In der Phase 3a des DSM-Prozesses (Kontrollieren/Prüfen) werden die in der Planungs- und Spezifikationsphase festgelegten funktionalen Sollwerte mit den während des laufenden Betriebs anfallenden funktionalen Ist-Werten verglichen. Erst zu diesem Zeitpunkt ist der Verantwortliche in der Lage, seine Verarbeitungstätigkeit zu kontrollieren und zu prüfen. Die Ergebnisse des Soll-Ist-Vergleichs dienen dann als Input für die Phase 3b des DSM-Prozesses. Abbildung 5 verdeutlicht den Vorgang des Kontrollierens und Prüfens einer Verarbeitungstätigkeit.

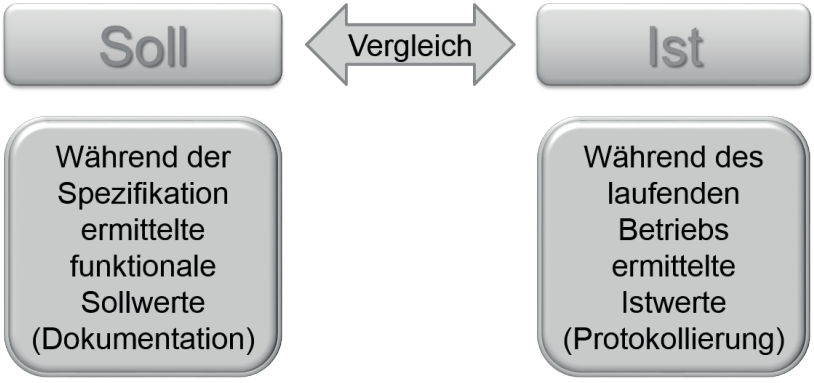


Abbildung 5: Phase 3a (Kontrollieren/Prüfen) des DSM-Zyklus

4.4 DSM-Phase 3b – Beurteilen

In der Phase 3b des DSM-Prozesses (Beurteilen) kann nun das Prüfergebnis aus Phase 3a datenschutzrechtlich beurteilt werden. Das Beurteilen der Prüfergebnisse erfolgt hinsichtlich der Erfüllung der rechtlichen Vorgaben (Gesetze, Verträge, Gewährleistungsziele) und der Wirksamkeit der ausgewählten und implementierten technischen und organisatorischen Maßnahmen. Die Abbildung 6 veranschaulicht den Vorgang der Beurteilung.

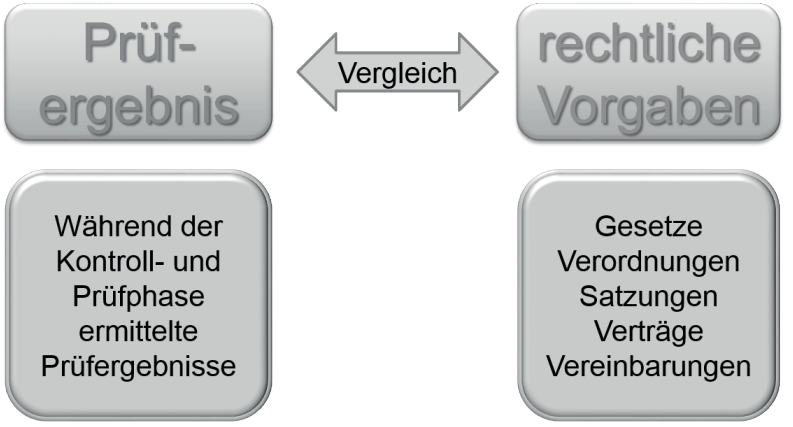


Abbildung 6: Phase 3b (Beurteilen) des DSM-Zyklus

Eine Verarbeitungstätigkeit kann beurteilt werden, indem das Prüfergebnis aus Phase 3a mit den rechtlichen Vorgaben verglichen wird, die bereits vor dem Start des DSM-Zyklus geprüft wurden. Erst im Ergebnis der Beurteilungsphase kann eine Aussage darüber getroffen werden, ob die Verarbeitung rechtskonform ist. Im DSM-Prozess wird die Beurteilung bewusst als extra Phase ausgewiesen. Das SDM kann Verantwortliche bei der rechtlichen Prüfung einer Verarbeitungstätigkeit unterstützen. Die Ergebnisse der Phase 3b bilden die Grundlage zur Behebung von Defiziten in der Phase 4 (Verbessern). Die folgenden formalen Indikatoren weisen auf fehlende Rechtskonformität hin:

- eine Verarbeitung wurde nicht nachweislich hinreichend geplant und spezifiziert,
- es liegen keine hinreichende Dokumentation und keine Protokolldaten zu Zwecken der Kontrolle und Prüfung vor,
- es erfolgt keine methodischen Prüfung oder Beurteilung einer Verarbeitung,
- der laufende Betrieb einer Verarbeitung unterliegt keiner fortwährenden Kontrolle und Prüfung,
- festgestellte Mängel führen nicht zu Aktivitäten, die eine Verbesserung bewirken.

Wenn der Verantwortliche die Phase 3 des DSM-Prozesses vollständig abgearbeitet hat ist er in der Lage, die Rechtskonformität der Verarbeitungstätigkeit zu beurteilen.

4.5 DSM-Phase 4 – Verbessern

In Phase 4 des DSM-Prozesses (Verbessern) muss der Verantwortliche entscheiden, ob Details der Verarbeitung verbessert werden müssen, weil er bspw. Defizite bei Grundrechtseingriffen der Verarbeitungsfunktion, Mängel bei der Umsetzung der geforderten technischen und organisatorischen Maßnahmen oder ein unzureichendes Controlling festgestellt hat. Stellt der Verantwortliche mangelnde Rechtskonformität fest, muss er Änderungen der Verarbeitungstätigkeit anweisen. Diese Anweisungen führen in der Regel zu einem erneuten Durchlaufen des gesamten DSM-Prozesses, weil Änderungen der Verarbeitungstätigkeit nur im Rahmen einer erneuten Planung und Spezifizierung möglich sind.

Spätestens hier wird der Prozesscharakter des Datenschutzmanagements deutlich. Der DSM-Zyklus muss so oft durchlaufen werden, bis die Beurteilungsphase eine rechtskonforme Verarbeitungstätigkeit bescheinigt. Der Regelfall wird sein, dass vor dem Starten des Wirkbetriebs der DSM-Zyklus mehrfach durchlaufen wird, das erste Mal bspw. im Rahmen des Testbetriebs, das zweite Mal im Rahmen des Pilotbetriebs und das dritte Mal im Rahmen des Wirkbetriebs.

Aber selbst nach der Feststellung der Datenschutzkonformität kann der DSM-Prozess nicht beendet werden. Der Verantwortliche ist verpflichtet, die Verarbeitungstätigkeit laufend zu beobachten um festzustellen, ob sich irgendwelche Rahmenbedingungen geändert haben. So könnten sich bspw. die gesetzlichen Vorgaben ändern was dazu führen muss, den DSM-Prozess erneut zu durchlaufen. Es können sich aber auch technische Details der Verarbeitungstätigkeit ändern. Eine neue Betriebssystemversion auf den Clients des Verfahrens oder eine neue Version der Datenbank auf dem Datenbankserver des Verfahrens müssen ebenso dazu führen, dass der DSM-Prozess erneut durchlaufen werden muss. Jede Änderung

der Verarbeitungstätigkeit muss zu einer erneuten datenschutzrechtlichen Beurteilung (Phase 3b) führen um feststellen zu können, ob die Verarbeitungstätigkeit nach der betreffenden Änderung noch rechtskonform ist.

5. Das Datenschutzmanagement-System

Datenschutzmanagement ist für jede Verarbeitungstätigkeit einzurichten. Organisationsweit ist zudem erforderlich, ein übergreifendes Datenschutzmanagement-System (DSMS) einzurichten. Dabei sind folgende Aspekte zu berücksichtigen:

- Benennung eines Verantwortlichen für das DSMS (Projektmanager),
- Klärung der Rolle des Datenschutzbeauftragten (in kleineren Organisationen oft Personenidentität),
- Abgrenzung zur IT-Revision und zum IT-Sicherheitsbeauftragten,
- Erarbeitung, Spezifizierung und Dokumentation der Prozesse des DSMS,
- Heranzeihen des Verzeichnisses der Verarbeitungstätigkeiten als zentrales Dokument und
- Sichern der erforderlichen Ressourcen (Personal, Instrumente, Zeit, Budget).

6. Literatur

Die Details des DSM-Prozesses sind ausführlich beschrieben im Standard-Datenschutzmodell und insbesondere in den ersten Baustein-Entwürfen des Referenzmaßnahmen-Katalogs des SDM. Auf die folgenden Literaturquellen wird daher verwiesen:

- SDM-Methode Version 1.1 https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf

- Bausteine des Referenz-Maßnahmenkatalogs (noch nicht von der DSK verabschiedet):
  - Datenschutzmanagement (https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutz modell/Bausteine/SDM-1.1_80_Datenschutzmanagement_V1.0_uagsdmbs_final.pdf/
  - Planung und Spezifikation (https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_41_Planung_Spezifikation_V1.0_uagsdmbs_final.pdf
  - Dokumentation (https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_42_Dokumentation_V1.0_uagsdmbs_final.pdf
  - Protokollierung (https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_43_Protokollierung_V1.0_uagsdmbs_final.pdf

Die bisher veröffentlichten Bausteine wurden von den Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein und der Evangelischen Kirche Deutschlands zur Erprobung der SDM-Methode erarbeitet und veröffentlicht. Diese Bausteine sind keine Publikationen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. Es ist davon auszugehen, dass die Texte noch weiter entwickelt werden, bevor sie von der Datenschutzkonferenz herausgegeben werden.[1]

1 Der Beitrag beschreibt den Wissensstand, der zum Zeitpunkt des Sympoisums im Mai 2019 aktuell war. Mittlerweile liegt das Standard-Datenschutzmodell in der Version 2.0b vor.

Risiko als zentrales Maß zur Auswahl und Bewertung von Maßnahmen in der DS-GVO

Dr.-Ing. Rene Meis

1. Geeignete Maßnahmen im Sinne der DS-GVO

Beim technisch-organisatorischen Datenschutz geht es darum, die Anforderungen des Datenschutzrechts mit geeigneten technischen und organisatorischen Maßnahmen umzusetzen. Diese Maßnahmen können technisch (bspw. Verschlüsselungsmechanismen oder automatische Löschroutinen) oder nicht-technisch (bspw. Abläufe zur Bearbeitung von Anfragen von Personen deren Daten verarbeitet werden) sein. Der für die Verarbeitung personenbezogener Daten Verantwortliche muss sich die Frage stellen: „Welche technischen und organisatorischen Maßnahmen muss ich treffen, um personenbezogene Daten datenschutzkonform zu verarbeiten?"

Die Datenschutz-Grundverordnung (DS-GVO) gibt in den Artikeln 24, 25 und 32 Vorgaben dafür, nach welchen Maßstäben technische und organisatorische Maßnahmen getroffen werden müssen. Zunächst sind die Eigenschaften der Verarbeitung personenbezogener Daten an sich zu berücksichtigen:

- **Art** der Verarbeitung (Welche Daten und Personen sind betroffen?)
- **Umfang** der Verarbeitung (Wie viele Daten und Personen sind betroffen?)
- **Umstände** der Verarbeitung (Mit welchen Mitteln wird verarbeitet?)
- **Zwecke** der Verarbeitung (Warum findet die Verarbeitung statt? Welche Interessen werden mit der Verarbeitung verfolgt?)

Dann ist durch den Verantwortlichen zu beurteilen welche Risiken die Verarbeitung personenbezogener Daten für die Rechte und Freiheiten natürlicher Personen birgt.

Schließlich muss der Verantwortliche den Stand der Technik zur Auswahl geeigneter Maßnahmen berücksichtigen, ist in der Regel aber nicht dazu

verpflichtet, über den Stand der Technik hinaus Maßnahmen zu treffen. Schließlich kann der Verantwortliche auch die Implementierungskosten der Maßnahmen als Faktor zur Auswahl heranziehen.

Unter den sieben aufgeführten Faktoren, die bei der Auswahl und somit auch bei der Bewertung von technischen und organisatorischen Maßnahmen berücksichtigt werden müssen, kann das Risiko als zentrales Maß angesehen werden. Zum einen, da zur Bestimmung des Risikos die vier obengenannten Eigenschaften der Verarbeitung (Art, Umfang, Umstände und Zwecke) berücksichtigt werden müssen (vgl. Erwägungsgrund 76 DS-GVO) und zum anderen, da die Abwägungen zwischen zu treffenden Maßnahmen bezüglich des Stands der Technik und der Implementierungskosten immer unter Berücksichtigung des verbleibenden Risikos (Restrisiko) erfolgen müssen.

2. Risikoindikatoren in der DS-GVO

Um eine erste Einschätzung bezüglich der Risiken für die Rechte und Freiheiten natürlicher Personen, die von einer Verarbeitung personenbezogener Daten ausgeht, vorzunehmen, werden in Erwägungsgrund 75 der DS-GVO beispielhaft Indikatoren bezüglich möglicher Schäden, der verarbeiteten Daten, der Art, Umstände und Zwecke der Verarbeitung sowie deren Umfang angeführt. Sollte für eine Verarbeitung einer der im Folgenden aufgelisteten Risikoindikatoren zutreffen, so geht von der Verarbeitung wahrscheinlich ein Risiko aus.

Die folgenden Schäden, die im Rahmen einer Verarbeitung personenbezogener Daten auftreten können, führt die DS-GVO beispielhaft als Risikoindikatoren auf:

- Diskriminierung
- Identitätsdiebstahl
- Finanzieller Verlust
- Rufschädigung
- Verletzung des Berufsgeheimnisses
- Aufhebung der Pseudonymisierung
- erhebliche wirtschaftliche oder gesellschaftliche Nachteile

- Verlust der Kontrolle über personenbezogene Daten
- Einschränkung von Rechten und Freiheiten

Die Verarbeitung folgender Daten wird zudem als Risikoindikator angeführt:

- Besondere Kategorien personenbezogener Daten (vgl. Art. 9 DS-GVO)
- Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (vgl. Art. 10 DS-GVO)
- Personenbezogene Daten von Schutzbedürftigen, insbesondere von Kindern (vgl. Erwägungsgrund 38 DS-GVO)

Die folgenden Eigenschaften einer Verarbeitung personenbezogener Daten werden ebenfalls als Risikoindikatoren angesehen:

- Bewertung persönlicher Aspekte
- Einsatz neuer Technologien
- systematische Überwachung
- automatisierte Entscheidungen
- Abgleich oder Zusammenführen von Datensätzen
- Verarbeitung großer Menge von Daten
- Verarbeitung betrifft große Anzahl von Personen

Diese Indikatoren wurden auch von der Artikel 29 Datenschutzgruppe in die Leitlinie WP248 rev.01[1] aufgenommen, um die Frage zu beantworten, ob eine Verarbeitung personenbezogener Daten wahrscheinlich ein hohes Risiko birgt und daher der Verantwortliche eine Datenschutz-Folgenabschätzung (DSFA) durchführen muss. Die Artikel 29 Datenschutzgruppe kommt zu dem Schluss, dass beim Vorliegen von mindestens zwei der angeführten Risikofaktoren von der Verarbeitung wahrscheinlich ein hohes Risiko ausgeht.

Somit kann auf Basis der Risikoindikatoren eine erste Einschätzung bezüglich des Risikos vorgenommen werden. Auf diese erste Einschätzung muss dann eine genauere Betrachtung der möglichen Risiken folgen.

1 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (zuletzt aufgerufen am 20. August 2019).

3. Risikobetrachtung

Die beiden zentralen Schritte einer Risikobetrachtung sind die Identifizierung von Risiken und deren Bewertung.

3.1 Risikoidentifizierung

Zur Risikoidentifizierung müssen im Allgemeinen folgende Fragen beantwortet werden:

- Was soll geschützt werden? (Assets)
- Der Eintritt welcher Ereignisse verletzt die Assets? (Schadensereignisse)
- Wie kann es zu den Schadensereignissen kommen? (Bedrohungsszenarien)

Im Sinne der DS-GVO sind die Assets die Rechte und Freiheiten natürlicher Personen. Daraus folgt insbesondere, dass personenbezogene Daten besonders geschützt werden müssen, jedoch reicht der alleinige Schutz von Daten nicht aus, da Risiken bspw. auch aus einer intransparenten Verarbeitung personenbezogener Daten resultieren können. Schadensereignisse, die die Rechte und Freiheiten natürlicher Personen betreffen, können Datenschutzverletzungen (bspw. Verstöße gegen die Grundsätze aus Artikel 5 DS-GVO) sein oder auch Grundrechtseingriffe, wie eine Einschränkung der Meinungsfreiheit nach Artikel 11 der Charta der Grundrechte der Europäischen Union. Ein Bedrohungsszenario kann sich aus der Verarbeitung personenbezogener Daten selbst ergeben, aus technischen Fehlern, aus unabsichtlichen menschlichen Fehlern oder aus gezieltem menschlichem Handeln (z. B. Hackerangriffe). In Tabelle 1 werden die Risikoelemente Asset, Schadensereignis und Bedrohungsszenario anhand von Beispielen verdeutlicht.

	Bedrohungsszenario	Schadensereignis	Asset
Risiko 1	Großflächige Videoüberwachung eines öffentlichen Platzes, an dem regelmäßig Demonstrationen stattfinden.	Bürger fürchten negative Auswirkungen durch Teilnahme an Demonstration und nehmen daher nicht teil.	Recht auf Meinungsfreiheit
Risiko 2	Automatisierter Prozess zum Löschen von Serverlogs wird nicht ausgeführt.	Personenbezogene Daten werden länger gespeichert als erforderlich.	Grundsatz der Speicherbegrenzung
Risiko 3	Ein Mitarbeiter meldet eine aufgetretene Datenpanne nicht an den Verantwortlichen.	Betroffene Personen und Aufsichtsbehörden werden nicht über den Vorfall informiert.	Grundsätze der Transparenz und Rechenschaftspflicht
Risiko 4	Ein Hacker greift über eine Sicherheitslücke einer Unternehmensdatenbank Adressdaten von Kunden ab.	Unbefugter Dritte hat Zugang zu den Adressdaten der Kunden erhalten.	Grundsatz der Vertraulichkeit

Tabelle 1 – Illustration der Risikoelemente anhand von Beispielen

3.2 Risikobewertung

Die identifizierten Risiken müssen nun vom Verantwortlichen bewertet werden. Diese Bewertung erfolgt entlang zweier Dimensionen - der Schwere des Schadens und der Eintrittswahrscheinlichkeit. Dazu müssen die folgenden zwei Fragen beantwortet werden:

- Wie sehr verletzt das Schadensereignis das Asset? (Schwere)
- Wie wahrscheinlich ist es, dass die Bedrohungsszenarien eintreten und zum Schadensereignis führen? (Eintrittswahrscheinlichkeit)

Die Bewertung der Schwere und Eintrittswahrscheinlichkeit erfolgt quantitativ (Ereignis tritt 3-mal im Jahr ein, finanzieller Schaden für Betroffene zwischen 1.000 € und 5.000 €) oder qualitativ (Ereignis tritt selten ein, gravierender Eingriff in das Recht auf Meinungsfreiheit). Die Bewertung des Risikos insgesamt erfolgt über eine Risikofunktion, die auf Basis der festgestellten Schwere und Eintrittswahrscheinlichkeit das Risiko

kategorisiert. Häufig wird dazu eine Matrix mit qualitativen Abstufungen für Schwere und Eintrittswahrscheinlichkeit als Zeilen und Spalten verwendet. Die Zellen der Matrix ordnen den jeweiligen Kombinationen der beiden Dimensionen einen Risikowert zu.

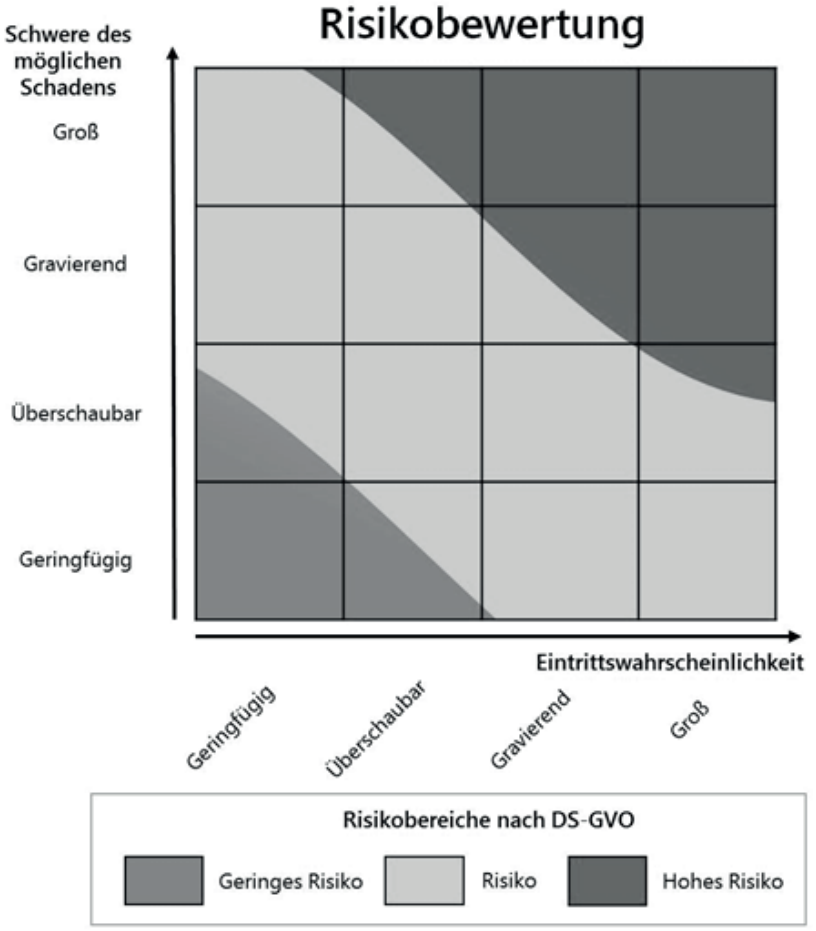


Abbildung 1 - Risikomatrix aus dem Kurzpapier Nr. 18

Die in Abbildung 1 gezeigte Matrix stammt aus dem Kurzpapier Nr. 18 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zum Thema „Risiko für die Rechte und Freiheiten natürlicher Personen“[2]. Für die Schwere des Schadens und seine Eintrittswahrscheinlichkeit werden in der Matrix jeweils vier Abstufungen genutzt. Die Färbung der Matrix gibt an, ob die jeweilige Kombination aus Schwere und Eintrittswahrscheinlichkeit ein geringes, normales oder hohes Risiko darstellt.

Grundsätzlich ist zu beachten, dass Definitionen der qualitativen Abstufungen für die Eintrittswahrscheinlichkeit (bspw. überschaubar: Ereignis tritt 1-mal in 10 Jahren ein) sowie für die Schwere von möglichen Schäden für jedes Asset bereitgestellt werden müssen (bspw. gravierend: viele Bürger verzichten auf ihr Recht auf Meinungsfreiheit aus Angst vor negativen Auswirkungen). Dies ist insbesondere erforderlich, um die durchgeführte Risikobewertung auch für die zuständigen Aufsichtsbehörden nachvollziehbar zu dokumentieren.

3.3 Risikomodellierung

Grundsätzlich können Bedrohungsszenarien zu verschiedenen Schadensereignissen führen (z. B. kann der Ausfall eines Datensicherungssystems zu inkonsistenten und inkorrekten Datenständen führen sowie zum vollständigen Verlust von Daten). Andererseits können Schadensereignisse durch verschiedene Bedrohungsszenarien verursacht werden (z. B. können personenbezogene Daten durch einen unbeabsichtigten Fehler einer Person Dritten unbefugt zugänglich gemacht werden oder durch einen Hackerangriff). Ebenso können Schadensereignisse mehrere Rechte und Freiheiten natürlicher Personen (Assets) schädigen und Rechte und Freiheiten können durch verschiedene Schadensereignisse geschädigt werden. Diese Beziehungen werden in Abbildung 2 in der CORAS-Notation[3] illustriert.

2 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (zuletzt aufgerufen am 20. August 2019) Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Datenlizenz Deutschland – Namensnennung – Version 2.0 (www.govdata.de/dl-de/by-2-0).

3 http://coras.sourceforge.net/index.html (zuletzt aufgerufen am 20. August 2019).

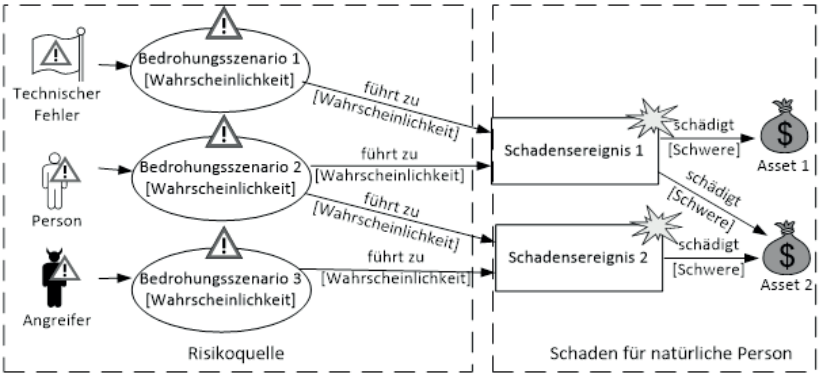


Abbildung 2 - Mögliche Modellierung von Risiken und Abhängigkeiten zwischen diesen

In dieser Notation bestimmt sich die Wahrscheinlichkeit, dass ein Schadensereignis eintritt, über die Wahrscheinlichkeit, dass die assoziierten Bedrohungsszenarien an sich eintreten und der Eintritt der Bedrohungsszenarien tatsächlich zu dem Schadensereignis führt. Falls mehrere Bedrohungsszenarien zu einem Schadensereignis führen können, muss ein geeignetes Kalkül zur Bestimmung der Eintrittswahrscheinlichkeit des Schadensereignisses ausgewählt werden, bspw. Auswahl der maximalen Eintrittswahrscheinlichkeit. In der CORAS-Notation aus Abbildung 2 ergibt sich aus jeder Schädigung eines Assets durch ein Schadensereignis ein Risiko. Somit ergeben sich durch das Schadensereignis 1 in Abbildung 2 zwei Risiken. Diese Risiken haben beide die Eintrittswahrscheinlichkeit des Schadensereignis 1 und als Schwere die jeweilige Schwere, mit der das Schadensereignis 1 das jeweilige Asset schädigt.

4. Auswahl geeigneter Maßnahmen

Für die identifizierten und bewerteten Risiken müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um die Risiken adäquat zu reduzieren und damit ein angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten zu erreichen. Der risiko-orientierte Ansatz der DS-GVO hilft dem Verantwortlichen zu priorisieren, an welchen Stellen und in welchem Umfang technische und organisatorische Maßnahmen ergriffen werden müssen. So muss ein besonderes Augen-

merk auf die Behebung oder Abmilderung von hohen Risiken gelegt werden, wobei für geringfügige Risiken gegebenenfalls keine weiteren Maßnahmen ergriffen werden müssen.

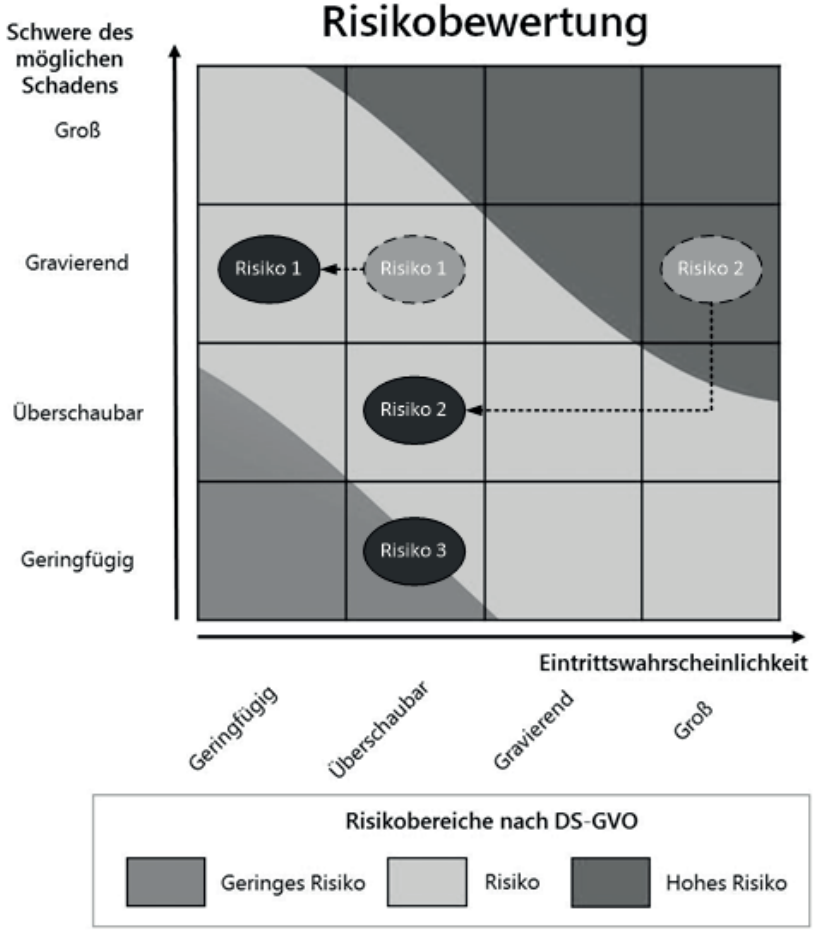


Abbildung 3 - Illustration der Risikoreduktion durch getroffene Maßnahmen

Grundsätzlich können Maßnahmen zu einer Reduzierung der Eintrittswahrscheinlichkeit eines Risikos führen oder zur Reduzierung der Schwere

des Risikos. Beispiele für Maßnahmen, die die Eintrittswahrscheinlichkeit reduzieren sind:

- Anonymisierung und Pseudonymisierung (Personenbezug für Unbefugte nicht herstellbar)
- Verschlüsselung, Rechte- und Rollenkonzepte (Zugriff für Unbefugte nicht möglich)
- Penetrationstests, Zertifizierungen (Ausschluss von technischen Fehlern)
- Mitarbeiter-Schulungen (Reduktion von unabsichtlichen menschlichen Fehlern)

Beispiele für Maßnahmen, die die Schwere eines Risikos reduzieren oder abmildern, sind:

- Prozesse zur Feststellung und Behandlung von Datenschutzverletzungen
- Prozesse zur Benachrichtigung von Betroffenen über Datenschutzverletzungen
- Eingriffsmöglichkeiten in die Verarbeitung personenbezogener Daten (z. B. Ausschluss von Daten von der Verarbeitung, Löschung von Daten)

Die Reduktion von Risiken ist in Abbildung 3 beispielhaft illustriert. Die Eintrittswahrscheinlichkeit des Risikos 1 wird in Abbildung 3 durch getroffene Maßnahmen um eine Stufe reduziert. Für das Risiko 2 hat sich durch die Auswahl von Maßnahmen sowohl die Eintrittswahrscheinlichkeit, als auch die Schwere reduziert. Für das Risiko 3 wurden keine Maßnahmen getroffen bzw. die getroffenen Maßnahmen haben die Zuordnung der Eintrittswahrscheinlichkeit und der Schwere des Risikos in die Abstufungen nicht verändert.

Nach der Auswahl der Maßnahmen ist eine erneute Risikobetrachtung erforderlich. Dabei muss zum einen betrachtet werden, ob alle Risiken adäquat adressiert wurden und ein angemessenes Schutzniveau erreicht wurde, und zum anderen, ob von den gewählten technischen und organisatorischen Maßnahmen selbst Risiken für die Rechte und Freiheiten natürlicher Personen ausgehen und welche Risiken bezüglich des Ausfalls oder der Unwirksamkeit der technischen und organisatorischen Maßnah-

men bestehen. Dieser iterative Prozess wird solange durchgeführt, bis durch die Auswahl von technischen und organisatorischen Maßnahmen ein angemessenes Schutzniveau - es bestehen bspw. nur noch geringe Restrisiken - erreicht wurde.

5. Fazit

Bei der Auswahl von technischen und organisatorischen Maßnahmen nach der DS-GVO ist für jede Verarbeitung personenbezogener Daten der Stand der Technik zu berücksichtigen. Das Ziel des Verantwortlichen sollte es sein, durch die Auswahl geeigneter technischer und organisatorischer Maßnahmen Datenschutzverletzungen in seiner Verantwortung soweit möglich zu verhindern und ihre Folgen abzumildern. Der risiko-orientierte Ansatz der DS-GVO unterstützt Verantwortliche dabei, indem die Behandlung möglicher Datenschutzverletzungen auf Basis der Höhe der festgestellten Risiken priorisiert werden können. Schließlich muss der Verantwortliche die verbliebenen Restrisiken verantworten und argumentieren können, dass er durch die ergriffenen technischen und organisatorischen Maßnahmen ein angemessenes Schutzniveau für die betroffenen Personen erreicht hat. Dazu müssen Verantwortliche die durchgeführte Risikobetrachtung nachvollziehbar dokumentieren, um ihren Rechenschafts- und Nachweispflichten gemäß der DS-GVO nachzukommen.

Eine Besonderheit der Risikobetrachtung nach der DS-GVO ist, dass sich die Schwere einer Datenschutzverletzung (bzw. eines Schadensereignisses) über ihre Folgen für die Rechte und Freiheiten natürlicher Personen bestimmt. Damit müssen zusätzlich zu physischen und materiellen Schäden auch immaterielle Schäden betrachtet werden, wie bspw. Diskriminierungen oder Einschränkungen der Meinungsfreiheit.

Verpflichtende Sicherheitskonzepte in Einrichtungen der Evangelischen Kirche in Deutschland

Michael Tolk

1. Wieso ist IT-Sicherheit bei der Ev. Kirche verpflichtend?

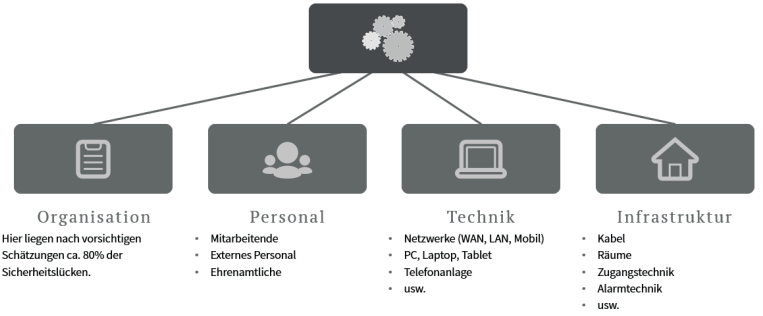
Seit Mai 2015 gibt es die IT-Sicherheitsverordnung (ITSVO). Diese findet unmittelbar Anwendung in allen kirchlichen Stellen der Ev. Kirche in Deutschland. Sie verpflichtet alle evangelischen kirchlichen Einrichtungen zur Umsetzung der IT-Sicherheit ein IT-Sicherheitskonzept zu erstellen und dieses auch kontinuierlich fortzuschreiben. Ein IT-Sicherheitskonzept ist nie fertig! Es gibt immer Änderungen, die in ein bestehendes Konzept eingearbeitet werden müssen, um es aktuell zu halten; sei es ein Update auf ein neues Betriebssystem oder auch der Austausch von Endgeräten.

Des Weiteren sieht die ITSVO vor, dass der für die Umsetzung des IT-Sicherheitskonzeptes erforderliche Sicherheitsstandard sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) zur Informationssicherheit und zum IT-Grundschutz zu orientieren hat. Hier ist bewusst kein Zwang auf eine Verpflichtung nach IT-Grundschutz gelegt worden, um den kirchlichen Einrichtungen eine Wahl zu lassen, ob sie alternative Wege gehen möchten, um IT-Sicherheit umzusetzen. So haben kirchliche Einrichtungen die Möglichkeit, sich z.B. nach ISO 27001 zertifizieren zu lassen, um den Anforderungen der ITSVO zu entsprechen.

Leider schreibt die ITSVO nicht vor, eine beauftragte Person für IT-Sicherheit zu bestellen, wie es das Datenschutzgesetz für die örtlich Beauftragten fordert. Bei der Erstellung und der kontinuierlichen Fortschreibung des IT-Sicherheitskonzeptes und bei der Entscheidung zur Auswahl über IT-Systeme, mit denen personenbezogene Daten verarbeitet werden, sind die örtlich Beauftragten für den Datenschutz zwingend zu beteiligen. Wird kein Mitarbeitender als beauftragte Person für IT-Sicherheit von der kirchlichen Stelle benannt, so trägt die Leitung der kirchlichen Stelle die Verantwortung für IT-Sicherheit und deren Umsetzung.

Die Empfehlung, sich bei der Umsetzung des IT-Sicherheitskonzeptes am Grundschutz des BSI zu orientieren, rührt daher, dass sich der § 27 DSG-EKD direkt auf die Grundwerte der IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) bezieht. Zudem beinhaltet er weiter die Datensicherungspflicht, sowie die Verwendung eines Managementsystems für Informationssicherheit (Information Security Management System / ISMS) zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verbreitung.

2. Wie wird IT-Sicherheit nach BSI-Grundschutz umgesetzt?

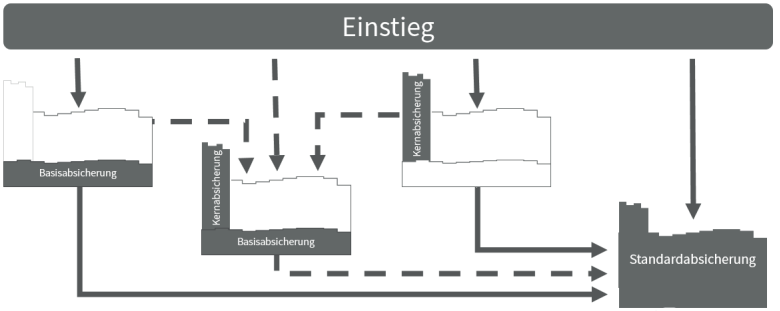


Der Grundschutz hat mehrere Facetten, die es zu betrachten gilt. Neben der Organisation, wo nach vorsichtigen Schätzungen ca. 80% der Sicherheitslücken einer kirchlichen Stelle liegen, wird auch das Personal, welches die Daten verarbeitet, die Technik, auf der die Daten verarbeitet werden, und die Infrastruktur des Gebäudes betrachtet.

Der Grundschutz wird in fünf Bereiche aufgeteilt. Die ersten vier Bereiche sind die BSI Standards. Diese werden ergänzt durch das IT-Grundschutz-Kompendium, welches die Standard-Sicherheitsmaßnahmen aus den bereits genannten Facetten Organisation, Personal, Infrastruktur und Technik enthält. Der Standard 200-1 definiert die Anforderungen an ein ISMS. Der Standard 200-2 beschreibt Schritt für Schritt die IT-Grundschutz-Vorgehensweise, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Der Stan-

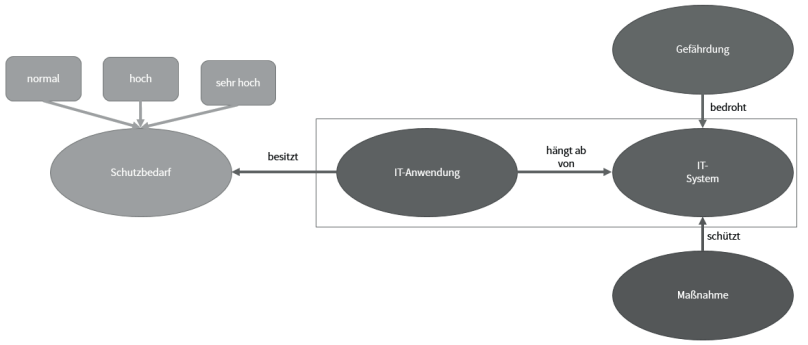
dard 200-3 befasst sich mit der Risikoanalyse und beschreibt, wie ein Risikoentscheidungsprozess, welcher mit dem neuen Datenschutzgesetz erstmalig nun auch im Datenschutz Berücksichtigung finden muss, implementiert werden kann. Der Standard 100-4 ist noch nicht auf den neuen Grundschutz angepasst und erläutert das Notfallmanagement, mit dem in einer kirchlichen Stelle die Kontinuität des Geschäftsbetriebes sichergestellt werden soll.

Der IT-Grundschutz kennt drei Einstiegsmöglichkeiten zur Erstellung eines IT-Sicherheitskonzeptes. Die Basis-Absicherung ist ein vereinfachter Einstieg und soll die grundlegenden Geschäftsprozesse und Ressourcen sichern. Ziel der Basis-Absicherung ist es, die größten Risiken schnell zu senken. Im Anschluss können dann die weiteren Schritte überlegt werden, um die tatsächlichen Sicherheitsanforderungen im Detail zu analysieren. Die Kernabsicherung soll herausragende, besonders schützenswerte Geschäftsprozesse und Ressourcen schützen. Sie fokussiert sich auf einen kleinen, aber sehr wichtigen Geschäftsbereich der kirchlichen Stelle. Dieser Einstieg eignet sich für Einrichtungen, die bereits ihre Geschäftsprozesse identifiziert haben. Die Standardabsicherung ist eine umfassende und tiefergehende Absicherung und sollte grundsätzlich angestrebt werden, um alle Bereiche einer kirchlichen Stelle angemessen und umfassend zu schützen.



Um die Anforderungen des Grundschutzes in der Praxis umzusetzen, sind acht Schritte notwendig:

1. **Festlegen eines Informationsverbundes**: Hier wird der Geltungsbereich der kirchlichen Stelle definiert. Betrachte ich z.B. die Behörde des Beauftragten für den Datenschutz der EKD (BfD EKD) gesamt oder definiere ich jede Außenstelle des BfD EKD als separat zu betrachtenden Informationsverbund. Neben den zu ermittelnden kritischen Verfahren und Fachaufgaben werden hier auch die Schnittstellen zu externen Partnern beschrieben.
2. **IT-Strukturanalyse**: Hier erfolgt die eigentliche Erfassung aller relevanten Komponenten innerhalb des zu betrachtenden Informationsverbundes. Neben den IT-Anwendungen werden hier auch die IT-Systeme erfasst. Unter den IT-Systemen sind nicht nur die Computer zu verstehen, sondern es sind auch aktive Netzwerkkomponenten, Drucker und TK-Anlagen etc. zu berücksichtigen. Insbesondere IT-Systeme, die nicht in einem Netzplan enthalten sind, sind hier zu erfassen. Gleichartige Objekte werden zusammengefasst, damit nicht jedes Objekt separat betrachtet werden muss.
3. **Schutzbedarfsfeststellung**: Der Schutzbedarf richtet sich nach den Stufen normal, hoch und sehr hoch und muss für jedes Objekt separat, jeweils für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit festgelegt werden. Je höher die Schutzbedarfsstufe gewählt wird, je mehr Maßnahmen müssen später zum Schutz des Objektes umgesetzt werden. Bei der Festlegung des Schutzbedarfes steht die IT-Anwendung, die auf einem IT-System läuft, im Mittelpunkt. Jede Anwendung bekommt einen Schutzbedarf zugewiesen und ist einer Kategorie zuzuordnen. Das Ziel von Bedrohungen ist immer das IT-System, auf dem eine Anwendung läuft.



Um den Schutzbedarf zuzuordnen gilt es, folgende drei Punkte zu berücksichtigen:

a. **Das Maximalprinzip**: Wenn auf einem IT-System mehrere Anwendungen betrieben werden, bestimmt die Anwendung mit dem höchsten Schutzbedarf auch den Schutzbedarf des IT-Systems.

b. **Der Kummulationseffekt**: Werden z.B. bei einer kleinen kirchlichen Stelle alle Anwendungen, auch wenn jede für sich einen niedrigen Schutzbedarf haben sollte, auf einem IT-System verarbeitet, entsteht bei Ausfall dieses IT-Systems ein insgesamt größerer Gesamtschaden für die kirchliche Stelle. Der Schutzbedarf des IT-Systems muss daher höher bewertet werden.

c. **Der Verteilungseffekt**: Eine IT-Anwendung überträgt ihren höheren Schutzbedarf nicht auf ein IT-System, wenn dort nur unwesentliche Teile der IT-Anwendung laufen. Werden z.B. die Daten aus einer Personalsoftware in einer physikalisch getrennten Datenbank auf einem separaten IT-System verarbeitet, bekommt das IT-System, auf dem die Anwendung läuft und mit dem die Daten verarbeitet werden, keinen höheren Schutzbedarf zugewiesen.

4. **Modellierung**: Bei der Modellierung werden den Ressourcen, die in der Strukturanalyse festgelegt wurden, Bausteine aus dem IT-Grundschutzkatalog zugeordnet. Die Bausteine beinhalten Maßnahmen, die von den zuvor vergebenen Schutzklassen abhängig sind. Je höher

der Schutzbedarf gewählt wurde, desto mehr Maßnahmen müssen umgesetzt werden, um IT-Sicherheit zu gewährleisten. Bei Verwendung eines ISMS-Tools kann bei jeder Maßnahme der Umsetzungsgrad definiert werden. Zusätzlich gibt es die Möglichkeit, den Maßnahmen bestimmte Personen in der kirchlichen Stelle zuzuordnen, die für deren Umsetzung dann verantwortlich sind.

5. **IT-Grundschutz-Check (Teil 1)**: Der erste Teil des Grundschutz-Checks dient dazu, organisatorische Vorbereitungen zu treffen; insbesondere sollen relevante Ansprechpartner für den Soll-Ist-Vergleich ausgewählt werden. Der Soll-Ist-Vergleich wird mittels eines Interviews und stichprobenartiger Kontrollen durchgeführt. Ziel ist es, den Umsetzungsgrad der Maßnahmen festzustellen (rot: noch nicht erledigt / gelb: teilweise erledigt / grün: ist erledigt). Die erzielten Ergebnisse des Soll-Ist-Vergleichs sind einschließlich der erhobenen Begründungen zu dokumentieren.

6. **Risikoanalyse**: Ist die verantwortliche Stelle der Ansicht, dass die Maßnahmen aus der Modellierung für bestimmte Zielobjekte nicht ausreichend sind, dient die Risikoanalyse dazu, die Gefährdungen für diese Zielobjekte festzustellen und zu bewerten. In der Regel erfolgt die Analyse in drei Schritten:

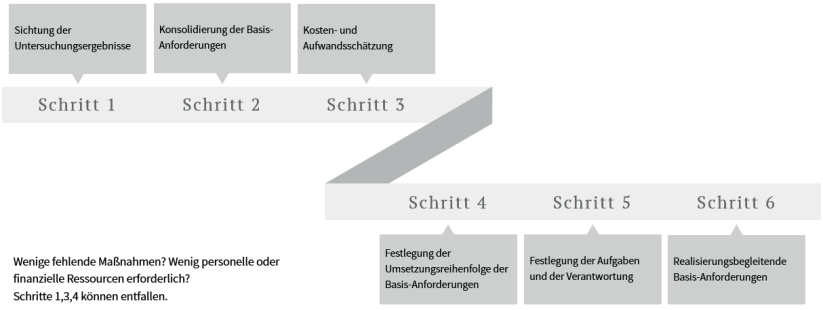
    a. **Erstellung einer Gefährdungsübersicht**: In Schritt eins wird eine Liste von allen möglichen elementaren Gefährdungen erstellt. Zudem werden zusätzliche Gefährdungen ermittelt, die sich aufgrund eines Einsatzszenarios ergeben und über die elementaren Gefährdungen hinausgehen.

    b. **Risikoeinstufung**: In Schritt zwei erfolgt die Einschätzung, wie häufig die Eintrittswahrscheinlichkeit ist und wie hoch der Schaden für die kirchliche Einrichtung sein kann. Für die Ermittlung der notwendigen Maßnahmen ist es hilfreich, die Risiken in diesem Schritt ebenfalls in Kategorien zu gliedern.

c. **Risikobehandlung**: In Schritt drei wird überlegt, wie das Risiko zu vermeiden ist. Gelingt dies, so sind keine weiteren Maßnahmen erforderlich. Sollte es aber nicht gelingen, das Risiko zu vermeiden, so werden hier Sicherheitsmaßnahmen definiert, um das Risiko so gut es geht zu reduzieren. Diese Maßnahmen sind individuell von der kirchlichen Stelle zu definieren, sie sind kein Bestandteil des IT-Grundschutz-Kompendiums.

7. **IT-Grundschutz-Check (Teil 2)**: In Teil zwei des Grundschutz-Checks wird nochmal festgehalten, welche Maßnahmen aus den Bausteinen noch nicht erfüllt oder nur zum Teil umgesetzt sind. Zusätzlich werden weiterführende Maßnahmen, die durch die Risikoanalyse festgestellt wurden, mit aufgenommen. Das Ergebnis ist ein finaler Maßnahmenkatalog, der die verpflichtend umzusetzenden Maßnahmen für die kirchliche Stelle enthält.

8. **Realisierung der Maßnahmen**: Hier vollzieht sich der Wandel von der Theorie zur Praxis. Es wird festgehalten, in welcher Reihenfolge die Maßnahmen umgesetzt werden sollen und wer für die Umsetzung verantwortlich ist. Eine Hilfestellung bei der Umsetzungsreihenfolge ist die Kosten- und Aufwandsschätzung. Maßnahmen, die einen geringen Aufwand haben und geringe Kosten bei ihrer Realisierung verursachen, können leichter umgesetzt werden.



3. Welche Konzepte resultieren noch aus einem IT-Sicherheitskonzept?

Natürlich gibt es nicht nur das eine IT-Sicherheitskonzept für eine kirchliche Einrichtung, sondern mehrere Teilkonzepte, die gemeinsam ein Gesamtkonzept ergeben. Neben dem Virenschutzkonzept, welches sich mit den Bedrohungen von außen und der Abwehr dieser Bedrohungen durch bestimmte Gegenmaßnahmen befasst, gibt es auch das Kryptokonzept, welches u.a. die Verschlüsselungsverfahren beschreibt, die eingesetzt werden, um sensible Daten vor unberechtigtem Zugriff zu schützen. Des Weiteren gibt es noch Konzepte zur sicheren Internetnutzung und für die Webangebote der kirchlichen Stelle. Wichtig sind auch das Datensicherungs- und das Notfallkonzept. Diese sind beide relevant, wenn es bei einer kirchlichen Stelle zu einem Schaden kommt, sei es durch einen technischen Mangel eines IT-Systems oder z.B. durch einen Virenbefall basierend auf einem Verschlüsselungstrojaner.

Als Anweisungen für die Mitarbeitenden resultieren aus einem IT-Sicherheitskonzept neben Leitlinien und Richtlinien der kirchlichen Stelle auch Merkblätter, Regelungen oder Hausverfügungen, die neben der Sensibilisierung der Mitarbeitenden wichtige Werkzeuge sind, um IT-Sicherheit praktisch umzusetzen.

4. Gibt es Unterschiede bei der Umsetzung von IT-Sicherheit innerhalb der EKD?

Eine Arbeitsgruppe aus Juristen und IT-Fachleuten hat auf Ebene der EKD ein Musterkonzept für kirchliche Einrichtungen erarbeitet. Dieses Muster ist aber nicht als Vorlage zu verstehen, sondern als Leitfaden bei der Erstellung eines eigenen Konzeptes. Die Arbeitsgruppe sah Handlungsbedarf bei der Erarbeitung einer Vorgabe zur Umsetzung von IT-Sicherheit in kleinen Einrichtungen. Hier hat die Arbeitsgruppe einen Fragenkatalog mit 26 Fragen entworfen, der ausreichend ist, um IT-Sicherheit in kleinen Organisationen zu gewährleisten. Zusätzlich zu dem Fragenkatalog gibt es in dem insgesamt zwölf Seiten umfassenden Dokument einen erläuternden Text zu zehn inhaltlichen Bereichen wie z.B. der Internetnutzung, dem Netzwerk oder auch der Verwendung von mobilen Datenträgern. Um keine Missverständnisse aufkommen zu lassen, hat die Arbeitsgruppe im

Muster-IT-Sicherheitskonzept definiert, was kleine Organisationen sind: „Kleine und kleinste Einrichtungen verfügen über kein geschultes IT-Personal, nur eine minimale Infrastruktur und eine überwiegend dezentrale Datenhaltung, z.T. zentrale Anwendungen. Zudem existiert z.T. keine ausreichende Abgrenzung zu privaten Bereichen. In der Regel gibt es keinen IT-Standard und auch keine Server." Somit ist klar, dass die Arbeitsgruppe als kleine Organisationen lediglich die Pfarrbüros definiert. Alle anderen Organisationen fasst die Arbeitsgruppe unter folgende Definition: „Mittlere und große Einrichtungen verfügen über eigenes, geschultes IT-Personal oder Externe sowie eine professionelle IT-Infrastruktur mit eigenen Servern. Zudem existieren in der Regel bereits unterschiedlich ausgeprägte IT-Standards. Es gibt z.T. auch Dienstleistungen, die durch Outsourcing betrieben werden." Hierunter sind die Kreis- und Landeskirchenämter zu fassen, die somit verpflichtet sind, ein ISMS für die Erstellung ihres IT-Sicherheitskonzeptes zu verwenden.

Tracking durch die Versicherung: Zu Risiken und Nebenwirkungen

Katharina Nocun

Versicherungen erheben immer mehr Daten: zurückgelegte Schritte, geputzte Zähne, sogar Gentests. Auf den ersten Blick sind viele Angaben freiwillig, doch langfristig droht Datensparsamkeit zum Luxusgut zu werden. Diese schleichende Diskriminierung braucht gesetzliche Grenzen.

Wer sich nicht sicher ist, ob gesetzliche Krankenversicherungen eine gute Sache sind, sollte sich einmal in den USA die Kundenbewertung von Tiermedikamenten bei Amazon durchlesen. Dort schreibt beispielsweise Christine, die Entwurmungspaste für Pferde mit Apfelgeschmack habe bei ihr und ihrem Ehemann ausgezeichnet gegen Krätze geholfen. „German Shepherd Mama" lobt ein Fisch-Antibiotikum mit folgendem Erfahrungsbericht: „Mein ‚Fisch' hatte Zahnschmerzen. Nachdem ich ihm fünf Tage lang morgens eine Pille verabreicht hatte, waren die Zahnschmerzen weg." 28 Menschen finden den Bericht hilfreich. Aus Sicht der Bewohner eines Landes mit gesetzlicher Krankenversicherung erscheint das skurril. Doch in einem der reichsten Länder der Welt können sich viele Menschen eine gute Krankenversicherung nicht leisten. Günstige Tiermedikamente werden so zur letzten Chance.

1. Kostbares Gut Gesundheitsdaten

Wenn Krankenversicherungen Kunden ablehnen und den Preis je nach Risiko frei gestalten dürfen, werden Gesundheitsdaten zum kostbaren Gut. Flexible datengetriebene Tarife nötigen immer mehr Menschen dazu, der Versicherung tägliche Updates zu schicken. Kunden des US-Versicherers John Hancock, die am „Vitality"-Programm teilnehmen, bekommen eine Apple Watch zum Schnäppchenpreis von nur 25 US-Dollar angeboten. Im Gegenzug erklären sich die Versicherten dazu bereit, die damit erfassten Fitnessdaten zwei Jahre lang an ihre Versicherung weiterzuleiten. Die tägliche Leistung wird mit Punkten belohnt. 15.000 oder mehr täglich zurückgelegte Schritte erhöhen das Konto um 30 Punkte. Wer es

nicht schafft, monatlich mindestens 500 Vitality Points nachzuweisen, muss für seine Apple Watch nachzahlen. Bei guten Werten sinkt dafür die Gesamtprämie der Versicherung.

Selbstverständlich gibt es Klauseln, die Kunden von derartigen Bonusprogrammen das Verleihen der Fitness-Wearables an Dritte verbieten. Über die Erholungsraten beim Puls lassen sich Menschen recht gut unterscheiden. Sonst könnte man ja einfach die Kinder zum Joggen schicken. Für den Versicherer John Hancock sind solche Fitness-Anreizsysteme nichts Neues. Den Einkauf gesunder Nahrungsmittel belohnt die Versicherung schon lange.

2. Neue datengetriebene Versicherungstarife

Nicht nur die körperliche Fitness ist Gegenstand neuer datengetriebener Tarife. Die Zahnzusatzversicherung kommt beim US-Anbieter Beam mit einer neuen elektronischen Zahnbürste. Die monatliche Zahlung im entsprechenden Tarif richtet sich danach, wie regelmäßig sich der Versicherte die Zähne putzt. Auch für europäische Versicherungen sind solche Systeme hochinteressant.

In der Reality-Sendung „Die Höhle der Löwen" des deutschen Privatsenders Vox suchen Start-up-Gründer regelmäßig vor einem Millionenpublikum nach Investoren. Bei der Präsentation der elektronischen Zahnbürste happy-brush sieht es zunächst ganz danach aus, als würden die Gründer ohne Finanzspritze abziehen müssen. Am Ende sammelten sie vor allem deshalb 500.000 Euro beim Unternehmer Carsten Maschmeyer ein, weil er die Idee einer intelligenten Schnittstelle zum Austausch von Putzdaten mit Krankenversicherungen vielversprechend fand.

3. Ständige Prüfungssituation für Versicherte

Vor Abschluss einer privaten Krankenversicherung oder einer Zahnzusatzversicherung wird meist die Offenlegung der bisherigen Krankengeschichte verlangt. Lügt der Versicherte dabei, darf sich die Krankenkasse später weigern, Kosten zu übernehmen. Doch die Vergangenheit kann stets nur einen begrenzten Ausblick auf zukünftige Risiken geben. Die

Zwillingsforschung zeigt, dass selbst die Genetik oft nur Wahrscheinlichkeiten aufzeigen kann. Alles spricht dafür, dass der individuelle Lebensstil gewaltige Auswirkungen auf unsere Gesundheit hat. Die Information, ob wir uns in den letzten Jahren bevorzugt von Mehrkornbrot und Gemüse oder ausschließlich von Pizza ernährt haben oder gar rauchen, ist für Versicherungen daher äußerst wertvoll.

Die neuen datengetriebenen Versicherungstarife passen sich beständig an immer neu berechnete Krankheitswahrscheinlichkeiten an. Aus einer Vorab-Prüfung wird so schleichend eine ständige Prüfungssituation. Der Versicherte ist immer in der Pflicht zu beweisen, dass er genug in seine Gesundheit investiert. Tut er das nicht, folgt die Strafe auf dem Fuße – in Form höherer Tarife oder dem Entzug von Bonusleistungen. Früher oder später droht bei einem solchen System eine Beweislastumkehr: Der Versicherte muss beweisen, dass er keine Mitschuld an einer Folgeerkrankung trägt.

4. Verwertungslogik statt Solidaritätsprinzip

Das kann auch objektiv krank machen. Diabetiker wären im ständigen Stress, bloß nicht gestresst zu sein, damit die Zuckerwerte stabil bleiben. Man will sich gar nicht vorstellen, was ein ähnlich gestricktes Prämiensystem für Bluthochdruck-Patienten bedeuten würde. Einen 10-Euro-Gutschein für das Wahrnehmen der jährlichen Vorsorgeuntersuchung beim Zahnarzt auszuloben, ist grundsätzlich nicht verkehrt. Bei hohen Prämien, die nur per Nachweis von Körperdaten verfügbar sind, besteht jedoch die Gefahr, dass aus Freiwilligkeit irgendwann finanzieller Zwang wird. Wer bei seinem Krankenkassentarif richtig sparen will oder muss, bezahlt dann mit Abstrichen bei der Privatsphäre.

Individualisierte Versicherungstarife bedeuten nicht zuletzt, dass Bereiche unseres Lebens der ökonomischen Verwertungslogik unterworfen werden, die bisher frei davon waren. Sie höhlen das Solidaritätsprinzip aus. Ich möchte nicht in einer Welt leben, in der ich aus Angst vor dem langen Arm meiner Krankenversicherung im Internet nur noch per Anonymisierungsdienst Pizza bestellen kann. Wer Angehörige pflegt, schafft es

beim besten Willen nicht jeden Tag ins Fitnessstudio. Bei einem Trauerfall hat so gut wie jeder andere Prioritäten, als sich um seinen Blutdruck zu kümmern.

Was für eine Gesellschaft wären wir, wenn wir eine alleinerziehende Mutter dazu drängen würden, nach Feierabend noch das vorgeschriebene Work-out zu absolvieren, damit die Prämie nicht steigt? Wollen wir wirklich, dass Kinder aus weniger wohlhabenden Familien mit dem Zwang aufwachsen, ihre Zähne vor allem deshalb gründlich zu putzen, weil den Eltern sonst das Geld für den Familienurlaub fehlt?

5. Kfz-Versicherung nach Fahrverhalten

Individualisierte Tarife sind nicht nur bei Krankenversicherungen auf dem Vormarsch. So gibt es etwa bereits Kfz-Versicherungen, die den Tarif anhand des Fahrverhaltens berechnen. Wer vorsichtig fährt, langsam beschleunigt und sachte bremst, bekommt Rabatt. Einige Versicherungen bewerten es negativ, wenn man häufig an Unfallschwerpunkten unterwegs ist. Selbst die Bevölkerungsdichte rund um die Strecke kann mit hineingerechnet werden. Nachtfahrten werden bei einigen Tarifen abgestraft, weil sie statistisch gesehen ein höheres Unfallrisiko bedeuten. Für den einen oder anderen mag das gerecht erscheinen. Würden solche Tarife allerdings zum Standard, könnte sich eine Hebamme, die im Notfall auch einmal nachts über die Landstraße zum Einsatzort eilen muss, womöglich keine Kfz-Versicherung mehr leisten. Auch Schichtarbeiter und Menschen mit hohem Nachtdienstanteil hätten das Nachsehen.

Ob das gesellschaftlich wünschenswert ist, wage ich zu bezweifeln. Den Rabatt zahlen wir außerdem mit unseren Standortdaten. Jede Fahrt zum Supermarkt, jedes etwas zu späte Losfahren zur Arbeit, jedes Abholen der Kinder vom Sport, jeder Besuch bei Freunden – anhand unseres Bewegungsprofils lässt sich unser Tagesablauf je nach Autonutzung recht genau nachvollziehen. Setzen sich solche Tarife durch, wird das Recht, für sich zu behalten, wohin man fährt, zu einem Luxusgut.

6. Emotionale und psychische Gesundheit

Versicherungen haben nicht nur ein Interesse an unseren Körperdaten. Unter dem Label Generali Vitality wird in Deutschland ein Angebot für Berufsunfähigkeits-, Erwerbsunfähigkeits- und Risikolebensversicherungen beworben. Bei gesunder Lebensweise und Übermittlung von Fitnessdaten winkt ein reduzierter Versicherungsbeitrag sowie ein bunter Strauß an Sachprämien. Zusätzlich sorgt sich der Anbieter aber auch um den psychischen Zustand der Kunden: „Die Vitality-Mental-Tests (Online-Fragebögen) helfen dabei, die emotionale und psychische Gesundheit besser einzuschätzen und persönliche Stressfaktoren zu erkennen."

Die Psycho-Tests werden natürlich mit Punkten belohnt. „Generali Vitality hat sich zum Ziel gesetzt, Sie auf Ihrem Weg in ein gesünderes Leben zu begleiten und zu belohnen", heißt es auf der Webseite. Das ist natürlich nur ein Teil der Wahrheit. Viel wichtiger ist, dass Risikokunden so frühzeitig erkennbar werden. Auch wenn die aus den Daten abgeleiteten Vorhersagen im Einzelfall falsch sein können, so sind sie im statistischen Mittel doch erfolgreich. Ausbaden muss das dann vor allem der Versicherte, der nicht ins Raster passt.

7. Privatsphäre als Privileg für Besserverdiener

Der eine oder andere mag einwenden, dass niemand gezwungen sei, bei solchen Systemen mitzumachen. Doch so einfach ist es leider nicht. Würde die Mehrheit die Durchleuchtung zum Standard erheben, dann würde Datenverweigerern bald unterstellt werden, sie hätten „etwas zu verbergen". Die Dynamik des Marktes bei Versicherungen kann ohne staatliches Eingreifen dazu führen, dass datensparsame Kunden auf lange Sicht tariflich genauso wie die Hochrisikogruppe behandelt werden. Das Grundrecht auf Privatsphäre würde damit zu einem Privileg für Besserverdiener. Geringverdiener und Familien mit knappem Budget wären schlichtweg gezwungen, die permanente Überwachung ihres Körpers, Fahrverhaltens und Einkaufs in Kauf zu nehmen.

Ein Experiment, das ich für mein Buch geplant hatte, habe ich mich am Ende doch nicht getraut durchzuführen. Die medizinische Forschung hat in den vergangenen Jahren eine beachtliche Zahl von Genkombinatio-

nen als Ursache für Erbkrankheiten identifizieren können. Gentests sind bereits für unter 200 Euro zu haben. Angelina Jolie ließ sich die Brüste amputieren, weil sie laut Gentest ein hohes Risiko in sich trägt, später an Brustkrebs zu erkranken. Es war ihre freie Entscheidung, sie wurde nicht dazu gedrängt. Ich habe für mich beschlossen, dass ich nicht alles über meinen Körper wissen will. Vielleicht fehlt auch die Dringlichkeit, weil es in meiner Familie keine Häufungen von schweren Krankheiten gibt. Ich weiß nicht, wie ich mit dem Wissen um eine zukünftige schwere Erkrankung umgehen würde.

8. Wir haben nur einen Körper

Vielleicht wird die Freiheit, seine Gene nicht zu kennen, in Zukunft für viele Menschen nicht mehr gelten. Im Jahr 2017 empfahl ein Ausschuss des US-Repräsentantenhauses die Annahme eines Gesetzentwurfs, der in diese Richtung geht. Kommt dieser Entwurf durch, dürfen Unternehmen Angestellte, die bei Wellness-Programmen des Arbeitgebers teilnehmen, zu einem Gentest animieren. Wer sich dem „freiwilligen Programm" entzieht, verpasst womöglich attraktive Prämien und muss für seine Krankenversicherung bis zu 50 Prozent mehr zahlen. Weiter gedacht, droht mit solchen Modellen ein Szenario, in dem schon vor der Geburt vorherbestimmt wäre, ob ein Mensch später Chancen auf einen guten Job und eine bezahlbare Krankenversicherung hat.

Wir müssen sicherstellen, dass Ärzte, Krankenkassen und Arbeitgeber unsere Gesundheitsdaten mit dem Respekt behandeln, den sie verdienen. Wir haben nur einen Körper. Einmal weitergegeben, ist es schwierig, Gesundheitsdaten aus der Welt zu schaffen. So manches datengetriebene Versicherungsmodell entpuppt sich bei näherem Hinsehen als schlechter Deal. Es braucht gesetzliche Grenzen, damit datengetriebene Versicherungsmodelle nicht zu einer schleichenden Diskriminierung führen. Denn die Risiken und Nebenwirkungen solcher Geschäftsmodelle tragen wir am Ende ganz allein.

Katharina Nocun: Die Daten, die ich rief. 347 Seiten, 18 Euro, Bastei Lübbe. ISBN: 978-3-7857-2620-4.

Informationen zu den Referenten

Marcus Baumann-Gretza

Marcus Baumann-Gretza ist Justiziar der Erzdiözese Paderborn und seit dem 01.01.2018 Leiter der Unterkommission Datenschutz- und Melderecht/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands (VDD). Die Unterkommission bereitet die Gesetzesentwürfe für die Beratung und Beschlussfassung in den Organen des VDD vor. Die aus den Diözesanbischöfen bestehende Vollversammlung beschließt die Gesetze in einer Musterfassung, die dann in den jeweiligen Diözesen durch den (Erz-) Bischof in Kraft gesetzt werden.

Prof. Dr. Dieter Kugelmann

Prof. Dr. Dieter Kugelmann ist seit dem 01.10.2015 der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, welcher als Kontrollinstanz für den öffentlichen Bereich sowie als Datenschutzaufsichtsbehörde für die privaten Stellen (Unternehmen) dient. Zuvor war er ordentlicher Universitätsprofessor für Öffentliches Recht, mit Schwerpunkt Polizeirecht einschließlich des internationalen Rechts und des Europarechts an der Deutschen Hochschule der Polizei in Münster. Prof. Dr. Kugelmann hatte im Jahr 2019 den Vorsitz der Datenschutzkonferenz (DSK) inne.

Steffen Pau

Steffen Pau, Jurist, ist seit dem 01.09.2016 Diözesandatenschutzbeauftragter für die fünf nordrhein-westfälischen (Erz-)Diözesen, Leiter des Katholischen Datenschutzzentrums in Dortmund und Verbandsdatenschutzbeauftragter für den Verband der Diözesen Deutschlands. Er war vor seiner Tätigkeit bei der katholischen Kirche über zehn Jahre im Bankenbereich als Datenschutzbeauftragter tätig, ist zertifizierter Datenschutzbeauftragter (GDDcert.) und Datenschutzauditor (TÜV).

Prof. Dr. Gernot Sydow

Prof. Dr. Gernot Sydow, M.A., ist Professor am Institut für internationales und vergleichendes öffentliches Recht der Universität Münster und Vorsitzender des Datenschutzgerichts der Deutschen Bischofskonferenz. Von 2006-2015 war er u.a. Justiziar des Bistum Limburg und im Nebenamt Richter am Kirchlichen Arbeitsgerichtshof Bonn, stellv. Aufsichtsratsvorsitzender eines größeren kirchlichen Schulträgers und Mitglied des Verwaltungsrates des Verbandes der Diözesen Deutschlands.

Gabriel Schulz

Gabriel Schulz ist stellvertretender Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Mecklenburg-Vorpommern und leitet dort den Bereich Technik. Er war bis Ende 2019 Leiter des Arbeitskreises Technik (AK Technik) der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK).

Dr.-Ing. Rene Meis

Dr.-Ing. Rene Meis ist Referent im Referat Technik der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

Michael Tolk

Michael Tolk ist seit Februar 2015 IT-Sachbearbeiter beim Beauftragten für den Datenschutz der EKD. Der Beauftragte für den Datenschutz der EKD nimmt die Datenschutzaufsicht für die Landeskirchen und diakonische Landesverbände mit ihren Mitgliedseinrichtungen wahr, die die Datenschutzaufsicht auf die EKD übertragen haben.

Katharina Nocun

Katharina Nocun ist Netzaktivistin, Bloggerin, ehemalige Politikerin, Bürgerrechtlerin, Publizistin und studierte Ökonomin und Politikwissenschaftlerin (M.Sc.). Sie leitete bundesweite Kampagnen zum Schutz der Bürgerrechte.

Frau Nocun ist seit 2012 regelmäßig als Expertin für Datenschutz und digitale Demokratiebewegungen Gast in zahlreichen Fernsehformaten und veröffentlicht zum Thema Datenschutz Beiträge in zahlreichen Medien. In ihrem Blog kattascha.de setzt sie sich vor allem mit gesellschaftlichen Folgen der Digitalisierung sowie populistischen Bewegungen auseinander. Ihr erstes Buch „Die Daten, die ich rief" erschien 2018 bei Lübbe, 2020 folgte (gemeinsam mit Pia Lamberty) der Bestseller „Fake Facts" (Quadriga).

www.katholisches-datenschutzzentrum.de