Software and Computational Systems Lab
Institute of Informatics
Faculty of Mathematics, Informatics, and Statistics
Ludwig-Maximilians-Universität München, Germany

Ausarbeitung
im Fach
Juristisches IT-Projektmanagement

zum Thema

# Die EU-DSGVO ab 25. Mai 2018 - was ändert sich für wen?

von
Anja Mainz

vorgelegt bei
Dr. Frank Sarre

21. Januar 2018

# Inhaltsverzeichnis

Am 25.Mai 2018 tritt die neue EU-Datenschutzverordnung, kurz EU-DSGV in Kraft und trotzdem schreibt der Verein “bitkom” in einem Artikel vom Juni 2017, dass laut einer, von ihm durchgeführten Befragung von “228 IT- und Digitalunternehmen” [18] 19% angäben, sich mit der Thematik noch nicht einmal auseinander gesetzt zu haben. Dazu kommen 42% Prozent der Unternehmen, welche sich zwar mit dem Thema beschäftigen, jedoch noch nicht mit Maßnahmen begonnen hätten. Nur 34 % der befragten Unternehmen hätten zu diesem Zeitpunkt schon mit ersten Maßnahmen begonnen (ebd.).
Das Problem an diesen Zahlen wird ersichtlich, wenn man betrachtet, was Müller schreibt: “Die Datenschutz-Grundverordnung (DS-GVO) trat gemäß ihrem Art. 99 Abs. 1 am 24. Mai 2016 in Kraft und wird gemäß Art. 99 Abs. 2 DS-GVO ab 25. Mai 2018 unmittelbar in jedem Mitgliedsstaat gelten.” [9]. Das bedeutet, den Firmen waren zwei Jahre eingeräumt worden, um sich auf Vorgaben und Änderungen im Gesetz einzustellen. Da es doch einige Änderungen gab - wie weiter unten ersichtlich wird - ist es problematisch, dass die Zeit bisher offensichtlich wenig genutzt wurde. In dieser Arbeit soll dargestellt werden, welche Änderungen die EU-DSGVO mit sich bringt, was sich also ab Mai 2018 für diejenigen ändert, deren Daten genutzt werden, aber auch, welche neuen Ansprüche an Firmen gestellt werden.

# 1 Geschichte des Datenschutzes in Deutschland und Europa

Das älteste Datenschutzgesetz der Welt findet sich tatsächlich in Deutschland, genauer ist es das Hessische Datenschutzgesetz [7] von 1970 (vgl. dazu z.B. [6], S. 99). Auf Bundesebene gab es etwas später auch ein Gesetz: “Das Bundesdatenschutzgesetz vom 27. Januar 1977, geändert durch [das] Gesetz vom 18. August 1980” [10], wozu es am 20.12.1990 noch eine besser an das Grundgesetz angepasste Ausfertigung gab [BDSG].
Auf europäischer Ebene hingegen ist die Richtlinie DSRL 95/46/EG aus dem Jahr 1995 bislang Kernstück zum Schutz personenbezogener Daten (vgl. [9]). Zu ihrer eigenen Umsetzung in den Mitgliedsstaaten ist dort nachzulesen: “Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie binnen drei Jahren nach ihrer Annahme nachzukommen.” ([95/46/EG], Art.32 (1)). Entgegen dieser Vorgabe setzte Deutschland die Anpassungen an die Richtlinie jedoch erst 2001 mit dem “Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze” [GAEB] um.
Verschiedene wissenschaftliche Betrachtungen haben aufgezeigt, dass in der Vergangenheit die Möglichkeiten Daten zu speichern kontinuierlich deutlich zugenommen haben (vgl. z.B. [13]). Somit war absehbar, dass die gesetzlichen Regelungen im Laufe der Zeit der Nachbesserung bedürfen würden. Unabhängig von technischer Weiterentwicklung, gab es andere Problematiken: “Um die vielen nationalen Umsetzungen der EU-Datenschutzrichtlinie 95/46/EG [zu] berücksichtigen und auf die eigenen Geschäftsprozesse übertragen zu können,[mussten] meist internationale Anwaltskanzleien beauftragt werden” [20], was insbesondere für kleine Unternehmen finanziell schwer zu bewältigen war. Gleichzeitig seien Sanktionen bei Verstößen für große Unternehmen meist nicht abschreckend genug und waren durch Datenverarbeitung außerhalb der EU leicht zu umgehen, so Weber (vgl. ebd.). Die DSGVO sollte also bestenfalls zu einer Harmonisierung des Datenschutzrechts innerhalb der EU führen und gleichzeitig sich auch auf Datenverarbeitung persönlicher Daten von EU Bürgern im Ausland beziehen.
So leitete die Europäische Komission Ende 2010 einen Reformprozess ein, ”um das Datenschutzrecht in der Europäischen Union auf eine neue Grundlage zu stellen” [9]. Dieser führte zu “ein[em] Vorschlag zu einer Grundverordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr” seitens der EU-Komission am 25.01.2012 (ebd.) und zur Verabschiedung der Europäischen Datenschutz-Grundverordnung am 25.05.2016 ([4]). Ähnlich wie 1995 müssen die Mitgliedsstaaten nun Anpassungen der eigenen Gesetze vornehmen, “um Rechtsunsicherheiten bei den Normadressaten zu verhindern. Tun sie dies nicht und behalten nationale Regelungen bei, die dem Unionsrecht widersprechen, verstoßen sie damit gegen ihre Verpflichtungen” ([8], S.3).
Abgesehen davon erlauben die Öffnungsklauseln der DSGVO den Mitgliedsstaaten explizit den Erlass

nationaler Regelungen (ebd.). Den eben genannten Verpflichtungen kam Deutschland diesmal zeitnah nach: Am 1. Februar 2017 wurde der Entwurf eines neuen Bundesdatenschutzgesetzes von der Bundesregierung eingebracht (vgl. [14]), im April 2017 wurde es vom Bundestag verabschiedet, im Mai 2017 hat es die Zustimmung des Bundesrats erhalten [2]. In diesem Zuge wurde auch die oben genannte Möglichkeit genutzt "nationale Spezifizierungen für ausgewiesene Bereiche für die Öffnungsklauseln vorzunehmen[:] [...] am 30.06.2017 erfolgte [die] Verabschiedung des Datenschutz Anpassungs- und Umsetzungsgesetzes" [4]. Wichtig zu erkennen ist der Unterschied, dass die Richtlinie 1995 lediglich als solche gedacht war, so dass bisher (und bis Mai 2018), im Zweifelsfall das BDSG gültig war. Die DSGVO steht im Gegensatz dazu über nationalstaatlichen Regelungen (vgl. [4], [21]).

# 2 Wichtige Begriffe

Ein Begriff, welcher in mehr oder minder jedem Artikel der DSGVO genannt wird sind sog. "Personenbezogene Daten". Der Originalwortlaut zu diesem Begriff ist:

"Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind" ([DSGVO], Art.4, Abs.1).

Intuitiver gesprochen also alles, was sich auf eine Person bezieht wie Name, Religion, Fingerabdruck, oder ähnliches. Für Unternehmen interessant sind in diesem Zusammenhang jedoch mehr Name, Anschrift, E-Mail oder IP-Adresse. Die DATA Software AG verweist neben diesen Daten auch allgemeiner auf Kundendaten, die z.B. in einem CRM-System verarbeitet werden oder Daten, welche nur für Marketingzwecke verwendet oder auch als "Beifang" aufgezeichnet werden (vgl. [1]).

Der "Betroffene" oder die "betroffene Person" meint im Rahmen dieser Arbeit die Person, auf welche sich personenbezogenen Daten beziehen, welche aufgenommen und verarbeitet werden.

# 3 Das neue DSGVO - eine Übersicht

Die DSGVO beinhaltet 99 Artikel, sowie 173 Erwägungsgründe - alle vorzustellen würde den Rahmen der vorliegenden Arbeit sprengen. Aus diesem Grund stelle ich im Folgenden die (für Unternehmen und die Forschung) wichtigsten Artikel des DSGVO vor, insbesondere solche, die eine Neuerung bedeuten. Die zuvor erwähnten "Öffnungsklauseln" sind nicht als eigene, mit dieser Bezeichnung versehene Absätze in der DSGVO zu verstehen, sondern meinen Formulierungen innerhalb verschiedener Artikel wie "zur Erfüllung rechtlicher Verpflichtungen", welche somit nationalstaatliche Rechte miteinbeziehen und erlauben.

## 3.1 Allgemeine Bestimmungen

### Artikel 3 - Geltungsbereich der DSGVO

Schon hier findet sich eine wichtige Neuerung im Gesetzestext: Aktuell gilt das EU-Datenschutzrecht nur dann, wenn derjenige der die Daten aufnimmt, entweder seinen Sitz in einem EU-Land hat oder „der Anbieter ohne EU-Niederlassung personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt." [19]. Artikel 3 der DSGVO erweitert jedoch den den Wirkungsbereich: Die DSGVO gilt wie bisher, wenn die Niederlassung in der EU liegt, jedoch auch, wenn nur die Waren oder Dienstleistungen in der EU angeboten werden - egal wo die Datenverarbeitung statt findet und wo der Sitz der Verantwortlichen ist! - und dies unabhängig von finanziellen Leistungen des Betroffenen (somit gilt die DSGVO auf dem

Papier auch für Facebook). Wybitul bemerkt, dass dies für global tätige Unternehmen bedeutet, dass sie sämtliche Vorgaben der Verordnung ggf. auch im Ausland erfüllen müssten (vgl.[21]). Allerdings gibt die Verbraucherzentrale zur Umsetzung dieses Artikels zu bedenken: “Damit sich europäische Datenschutzstandards auch durchsetzen lassen, sind entsprechende internationale Abkommen erforderlich.” [19].

### Neueinführung biometrischer und genetischer Daten in Artikel 4

Artikel 4 beschäftigt sich mit wichtigen Begriffsbestimmungen: Die oben genannten“personenbezogene Daten”, “Pseudonymisierung”, sowie noch einige andere Begriffe, die für das korrekte Verständnis der DSGVO wichtig sind. Eine neue Begriffsdefinition sind zum Beispiel die “biometrischen Daten” sowie “genetische Daten”. Beide Begriffe tauchen bisher weder in der Richtlinie von 1995 noch im BDSG auf. Jetzt, in der DSGVO werden sie jedoch als personenbezogene Daten bezeichnet, was bedeutet, dass biometrische Daten denselben strengen, neuen Auflagen unterliegen werden wie andere personenbezogene Daten. Dies ist insbesondere für Wissenschaft und Medizin von großer Bedeutung.

## 3.2 Grundsätze

### Thema Verantwortlichkeit in den Artikeln 4 & 5

Ein weiterer Begriff aus Artikel 4 ist “Verantwortlicher”. Dieser wird, vereinfacht gesagt, als Instanz definiert, welche “über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet” ([DSGVO], Art. 4, Abs. 7). Hier kann man ein Beispiel für eine Öffnungsklausel betrachten: Der Verantwortliche muss eventuell Daten zu gesetzlichen Zwecken aufnehmen - die DSGVO führt hierbei gleichberechtigt das “Unionsrecht oder das Recht der Mitgliedstaaten” an.
In Artikel 5 wird dieser Instanz die Verantwortlichkeit für einen bestimmten Umgang mit personenbezogenen Daten auferlegt, wobei die Einhaltung nachgewiesen werden muss. Dieser “bestimmte Umgang” wird in Absatz 1 beschrieben: Die Verarbeitung muss transparent und rechtmäßig erfolgen, für einen eindeutigen, angemessenen Zweck bestimmt sein, die Daten müssen richtig sein, dürfen keine Identifikation außerhalb des vorgesehenen Zweckes ermöglichen und müssen sicher aufbewahrt werden.
Die eben erwähnte Nachweispflicht ist neu. Schaar betont in ihrer Arbeit, dass hier eine deutliche Veränderung zum BDSG von 1990 vorliegt, da es dort in §4g lediglich heißt: “Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin”. Sie bemerkt zu Recht, dass Datenschutzbauftragte nun die Einhaltung von Vorschriften auch kontrollieren und sicherstellen müssten, sowie die Datenschutzfolgeabschätzung (siehe 3.4) überwachen und weitere Anforderungen erfüllen müssten (vgl. [16]).

### Definition der Zweckbindung in Artikel 5

Was ich im vorigen Absatz abgekürzt als ‘eindeutiger und angemessener Zweck’ beschrieben habe, meint die so genannte Zweckbindung. Diese existierte zwar schon vor dem DSGVO, jedoch in einer schmaleren Definition (vgl. [16]): In der Richtlinie von 1995 heißt es “Die Verarbeitung personenbezogener Daten [...] hat de[m] angestrebten Zweck zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Die Zwecke müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein” ([95/46/EG] , Erwägungsgrund 28). Im DSGVO wird nun ausdrücklich erlaubt, dass “im öffentlichen Interesse liegende Archivzwecke, [...] wissenschaftliche oder historische Forschungszwecke [und] statistische Zwecke [...] nicht als unvereinbar mit den ursprünglichen Zwecken [gelten]” ([DSGVO], Art. 5, Abs.1). Somit wird der Forschung hier ein größerer Handlungsspielraum eingeräumt.

### Welche Daten dürfen verarbeitet werden, welche nicht? Über die Artikel 6 - 9

Artikel 6 bestimmt, dass eine Datenverarbeitung rechtmäßig ist, wenn die Einwilligung des Betroffenen vorliegt, die Daten für eine Vertragserfüllung mit dem Betroffenen oder für die Erfüllung rechtlicher Pflichten notwendig sind, bei lebenswichtigen Belangen, für das öffentliche Interesse, sowie zur Wahrung von berechtigten Interessen. Letzteres ist, wie Possekel und Schiemann schreiben, "neu formuliert" und hat in dieser vagen Formulierung das Problem, dass unklar bleibe wie weit "berechtigtes Interesse" genau trägt [12]. Wybitul schreibt, dass das Verarbeiten von Daten für andere Zwecke als den ursprünglich bei der Datenaufnahme angenommenen, für viele Arbeitgeber von Interesse sei (vgl. [21]) - mit dieser Thematik beschäftigt sich Abs. 4: wichtig ist unter anderem eine Betrachtung möglicher Folgen für den Betroffenen sowie evtl. eine Pseudonymisierung (Definition der Pseudonymisierung unter 3.5). Keinesfalls tritt jedoch deshalb die Zweckbindung aus Art. 5 außer Kraft! Aus diesem Grund rät Wybitul dazu die (möglichen) Zwecke der geplanten Verarbeitung personenbezogener Daten von Beschäftigten gleich bei deren Erhebung umfassend und vollständig festzulegen (ebd.).
Artikel 7 beschreibt die Bedingungen für die eben genannte Einwilligung des Betroffenen. In der Richtlinie von 1995 gab es zu diesem Thema keine weiteren Ausführungen (lediglich eine Definition des Begriffes "Einwilligung" als zwanglos, zweckgebunden und in Wissen der Tatsache, dass personenbezogene Daten verarbeitet werden in Art. 2h). Das BDSG fügt diesen Punkten hinzu, die Einwilligung bedürfe außer in besonderen Umständen der Schriftform und fordert für sog. "besondere Daten" eine Einwilligung ausdrücklich für diese Daten ([BDSG],§4a). Die DSGVO definiert eine Einwilligung in ähnlicher Weise ([DSGVO], Art.4, Abs.11), fügt in Art. 7 jedoch hinzu, dass der Verantwortliche nachweisen können muss, dass der Betroffene eingewilligt hat, fordert eine verständliche Sprache, spricht dem Betroffenen ein Widerrufsrecht zu so wie ein Recht darauf über dieses aufgeklärt zu werden und fügt explizit hinzu, dass ein Vertragsschluss nicht davon abhängig gemacht werden darf, dass der Betroffene eine Einwilligung in die Verarbeitung personenbezogener Daten gibt - G DATA bringt hier das gute Beispiel, dass das Einwilligen zur werblichen Verwendung der Daten nicht zwingend sein darf, um eine Bestellung abschließen zu können ([1]). An dieser Stelle ist also eine klare Verschärfung des Gesetzes zu erkennen.
Artikel 8 legt fest, dass die Verarbeitung personenbezogener Daten bei Kindern grundsätzlich erst ab dem sechzehnten Lebensjahr oder mit Einwilligung der Eltern möglich ist (auch hier ist eine Öffnungsklausel, so dass nationalstaatliche Regelungen das Alter des Kindes auf höchstens dreizehn Jahre herunter setzen können).
Artikel 9 verbietet die Verarbeitung "besonderer Kategorien personenbezogener Daten" - zu diesen zählen alle Daten, aus denen rassische oder ethnische Herkunft, politische, religiöse oder weltanschauliche Überzeugungen, sexuelle Orientierung oder Gewerkschaftsangehörigkeit hervorgehen, so wie explizit genetische und biometrische Daten. Die letzteren beiden wurden ja schon in 3.1 erwähnt, die Bezeichnung als besondere personenbezogene Daten, erhöht ihren Schutz nun noch einmal. Bis auf die Einbeziehung genetischer und biometrischer Daten, war diese Regelung auch schon im BDSG §13 getroffen worden. Im BDSG und jetzt auch in der DSGVO wird für medizinische und wissenschaftliche Zwecke unter Auflagen trotzdem eine Verarbeitung erlaubt.

## 3.3 Rechte der Betroffenen

### Die sog. Transparenzpflicht in Artikel 12

Wybitul bezeichnet die in diesem und den folgenden Artikeln formulierten Regelungen als die vielleicht wesentlichste Veränderung gegenüber dem BDSG, da Informationspflichten massiv gesteigert wären (vgl. [21]): Sämtliche, gesetzlich vorgeschriebene Mitteilungen (z.B. die Information darüber, dass Daten gespeichert werden (vgl. 3.3)) müssen "in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" ([DSGVO], Art.12 §1) gehalten, sowie kostenlos

sein (Ausnahme nur bei exzessiver Nutzung mit Nachweispflicht beim Verantwortlichen). Des weiteren ist der Verantwortliche verpflichtet, den Betroffenen die Ausübung der Rechte, die sie gemäß dieses Artikels besitzen, zu erleichtern (außer er kann nachweisen, dass er die betroffene Person nicht identifizieren kann). Zum Verfügung stellen der Information bleiben dem Verantwortlichen ein bis höchstens in besonderen Fällen drei Monate. Bei Ignorieren des Antrags ist der Verantwortliche verpflichtet, dem Betroffenen die Gründe zu nennen und ihn über Beschwerdemöglichkeiten zu unterrichten.

Die EU-Richtlinie von 1995 schreibt dazu: "Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen [...] frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten [...] eine Mitteilung in verständlicher Form über die Daten , die Gegenstand der Verarbeitung sind, [zu erhalten]" ([95/46/EG], Abschnitt V, Artikel 12). Neu ist also die klare Frist zur Lieferung der Daten im Gegensatz zur vorherigen sehr pauschalen Formulierung, sowie die klare Forderung nach Vergütungsfreiheit.

### Artikel 13 & 14 - Die Informationspflicht

Die betroffene Person muss direkt zum Zeitpunkt der Erhebung der Daten über die Kontaktdaten der Verantwortlichen, den Grund der Datenaufnahme, die rechtliche Grundlage, bei „Interessenabwägung" über ebendieses Interesse, die Dauer der Datenspeicherung, die Betroffenenrechte, etc. informiert werden. Ist der Betroffene nicht bei der Datenerhebung vor Ort, so müssen ihm trotzdem ähnliche Informationen mitgeteilt werden.
Diese Informationspflicht gab es in abgeschwächter Form im BDSG §4 und in 95/46/EG Art. 10. Neu sind bei der Informationspflicht, dass Rechtsgrundlage für die Verarbeitung angegeben werden muss, sowie die Dauer der Speicherung und die Information über das Recht dazu eine Einwilligung zu widerrufen und über das Recht auf Auskunft, Berichtigung und Löschung.

### Artikel 15 - 17: Das Recht auf Auskunft, Berichtigung und Löschung

In Artikel 15 geht es darum, dass ein Betroffener das Recht hat eine Bestätigung zu erhalten, ob personenbezogene Daten verarbeitet werden, so wie auf weitere Informationen wie den Zweck oder die Dauer der Datenverarbeitung. Bisher war dieses Recht in der Richtlinie 95/46/EG in Artikel 12 vorgesehen und in §19 des BDSG von 1990 geregelt. Im DSGVO ist zusätzlich formuliert, dass der Betroffene Recht auf eine kostenlose Kopie hat, sofern es Rechte und Freiheiten anderer Personen nicht beeinträchtigt, und das Recht auf die Information über die Übermittlung personenbezogener Daten an ein Drittland. Wybitul sieht in diesem Recht auf eine Kopie eine potentiell schlechtere Situation für Arbeitgeber vor Gericht. Er nimmt an, Arbeitnehmeranwälte würden dieses Recht in Zukunft zu Beginn von Verfahren regelmäßig nutzen. So könnten diese "zum einen umfassende Informationen erhalten und zum anderen auf Beweisverwertungsverbote hoffen, wenn der Arbeitgeber hierauf nur unvollständig informiert" [21].
Artikel 16: Der Betroffene hat das Recht auf Berichtigung und Vervollständigung seiner Daten. Dieses Recht findet sich ähnlich in der Richtlinie 95/46/EG Artikel 12 b),c) und im BDSG §20.
Artikel 17: Dieser Artikel beschreibt das "Recht auf Vergessenwerden", welches eine Person besitzt, sobald der ursprüngliche Erhebungszweck wegfällt, der Betroffene die Einwilligung widerruft, Widerspruch einlegt, wenn die Daten unrechtmäßig verarbeitet wurde, sowie weitere Gründe, welche wiederum eingeschränkt werden können wie z.B. durch das Recht auf freie Meinungsäußerung. Eine Löschung war auch zuvor schon möglich ([BDSG] §20), wenn auch weniger streng formuliert.

Artikel 12 bis 17 bedeuten einen hohen Aufwand für Unternehmen - z.B. falls "tausendfach der Nachweis über die Löschung von Daten gefordert wird oder viele Tausend Kunden gleichzeitig die über sie gespeicherten Informationen sehen wollen" [12] ist hohe Skalierbarkeit vonnöten, etc.

### Artikel 20 - Recht auf Datenübertragbarkeit

Artikel 20 beschreibt ein neues Recht: Der Betroffene darf seine Daten in einem maschinenlesbaren Format einfordern, es so auch weitergeben und hat sogar ein Recht darauf, dass ein Verantwortlicher die Daten an einen anderne Verantwortlichen überträgt. Das kann zum Beispiel bedeuten, dass Arbeitgeber Daten weitergeben müssen etc. und wird Firmen sicherlich Aufwand und entsprechend Geld kosten.

### Artikel 21 - das Widerspruchsrecht

Während das allgemeine "Recht auf Vergessenwerden" aus Artikel 17 im Allgemeinen laut Wybitul keine erhebliche Änderung zum bisherigen Recht darstellt, seien die Ausnahmen von der generellen Löschpflicht (Art. 17, Abs.3) künftig eng gefasst (vgl. [21]). Tatsächlich hat der Betroffene dank Art. 21 jederzeit das Recht Widerspruch gegen die Verarbeitung personenbezogener Daten einzulegen und der Verantwortliche hat daraufhin diese Daten zu löschen, es sei denn er kann "zwingende schutzwürdige Gründe für die Verarbeitung nachweisen" ([DSGVO], Art.21, Abs.1). Die Nachweispflicht liegt also beim Verantwortlichen.

## 3.4 Verantwortlicher und Auftragsverarbeiter

### Artikel 24 - Vorschrift für geeignete technische und organisatorische Maßnahmen

Der Verantwortliche muss technische und organisatorische Maßnahmen umsetzen, um eine Datenverarbeitung gemäß DSGVO sicher stellen zu können. Diese Forderung gab es schon in Erwägungsgrund 46 der Richtilinie 95/46/EG, sowie in §9 des BDSG - Neu ist auch hier die Nachweispflicht, die die DSGVO dem Verantwortlichen auferlegt.

### Auftragsverarbeitung in den Artikeln 24 und 26

Bisher war es dank dem BDSG möglich, dass es die so genannte Funktionsübertragung gab. Das bedeutet, dass es möglich war, dass ein Auftraggeber einem Dienstleister einen Teil des Umgangs mit den Daten übergeben konnte, in dem Sinne, dass dieser Nutzungsrechte an den Daten hat, selbst Daten aufnehmen kann, jedoch auch selbst für den Schutz der Rechte der Betroffenen zuständig ist (vgl.z.B.[11]). Das ist jetzt nach der neuen DSGVO nicht mehr möglich, da der Verantwortliche für den Schutz der Daten verantwortlich ist (vgl. 3.4) - laut Art. 26 legen der oder die Verantwortliche jedoch den Zweck und die Mittel zur Verarbeitung fest, was eine Funktionsübertragung unmöglich macht.

### Artikel 25 - Vorgaben für datenschutzfreundliche Voreinstellungen

Dieser Artikel ist in seinem Inhalt völlig neu und wird den Firmen viel Arbeit abverlangen: Der Verantwortliche muss sowohl wenn die Mittel für die Verarbeitung der Daten festgelegt werden als auch bei der eigentlichen Verarbeitung "geeignete technische und organisatorische Maßnahmen" treffen, um Datenschutzgrundsätze umzusetzen und die Rechte der Betroffenen zu schützen. Per Voreinstellungen dürfen jeweils nur personenbezogene Daten, deren Verarbeitung auch wirklich für den Zweck nötig sind, verarbeitet werden. Dies bezieht sich auf Menge, Speicherzeit, Zugänglichkeit, etc. Insbesondere muss die Voreinstellung dafür sorgen, dass die Daten nicht ohne Eingreifen der Person einer größeren Zahl Personen zugänglich gemacht wird. Graßhof bringt ein gutes Beispiel: "Wenn ich einen neuen Anwender innerhalb der Benutzerverwaltung anlege und ihm noch keine Rolle zuordne, so soll der Benutzer auch noch keine Daten sehen dürfen. Erst mit Zuordnung der Rolle darf er auf die seine Rolle entsprechenden Daten zugreifen. Häufig sind Systeme so aufgebaut, dass man ohne Rollenzuordnung plötzlich alle Rechte besitzt und viel mehr Daten sieht als man dürfte" [5]. In so einem Fall müsste eine Firma also entweder völlig neu entwickeln oder versuchen auszubessern. Ersteres droht teuer zu werden, zweiteres birgt die Gefahr etwas zu übersehen oder sich komplizierter zu gestalten als gedacht.

### Artikel 30 - Verzeichnis von Verarbeitungstätigkeiten

Dazu ein so genanntes Verzeichnis von Verarbeitungstätigkeiten schriftlich zu führen, wird ab Mai 2018 der Verantwortliche bzw. der Auftragsverarbeiter verpflichtet sein. Da diese Auflage völlig neu ist, wird jeder Verantwortlichen, ob in der Wissenschaft oder in einem Unternehmen, sich damit befassen müssen (zumindest in größeren Unternehmen - die Regelung gilt erst ab 250 beschäftigten Mitarbeitern). Aus diesem Grund, führe ich im Folgenden kurz auf, was verzeichnet sein muss:
Der Verantwortliche hat ein Verzeichnis aller Verarbeitungstätigkeiten zu führen, welches enthält:

- Name und Kontaktdaten des Verantwortlichen
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, die in der Vergangenheit oder Zukunft die Daten erhalten haben oder erhalten werden
- falls möglich Fristen für Löschung der Datenkategorien und/oder Beschreibung der Schutzmaßnahmen (siehe nächster Abschnitt)

Der Auftragsverarbeiter hat ein Verzeichnis zu allen Kategorien von Verarbeitungstätigkeiten zu führen, welches enthält:

- Name und Kontaktdaten des Auftragsverarbeiters
- Kategorien von Verarbeitungen
- ggf. Übermittlungen von Daten an ein Drittland/ eine internationale Organisation
- falls möglich Beschreibung der Schutzmaßnahmen (siehe nächster Abschnitt)

### Artikel 32 - Sicherheit der Verarbeitung

Dieser Artikel ist für Unternehmen von hoher Relevanz. Er verpflichtet den Verantwortlichen und den Auftraggeber dazu durch technische und organisatorische Maßnahmen ein “angemessenes Schutzniveau” bei der Verarbeitung zu gewährleisten. Dies bedeutet zum Beispiel, dass die Verschlüsselung personenbezogener Daten (und hier ist nun wiederum wichtig, was als personenbezogene Daten definiert wurde, wie die zuvor erwähnten genetischen und biometrischen Daten) jetzt zur Pflicht wird. Allgemein gesprochen nennt der Artikel als Maßnahmen Pseudonymisierung, Verschlüsselung, Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit (sowie eine rasche Wiederherstellung derselben nach einem Zwischenfall), Belastbarkeit, etc. Im BDSG von 1990 gab es lediglich §9a, welcher Anbietern von Datenverarbeitungssysthemen zugesteht ihr Konzept durch unabhängige Gutachter prüfen zu lassen, dies jedoch nicht vorschreibt. Auch die DSGVO weist darauf hin, dass Zertifizierungsverfahren herangezogen werden können, um die Erfüllung von Art.32 Abs.1 nachzuweisen. Zusätzlich schreibt sie “ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung” vor. Hier werden es zukünftig Unternehmen, die sich jetzt schon nach der ISO 27001 zertifizieren lassen, wahrscheinlich leichter in der Umstellung haben.

### Die Meldung von Datenschutzverletzungen nach den Artikeln 33 & 34

Wird der Schutz personenbezogener Daten verletzt, muss der Verantwortliche außer in Ausnahmefällen innerhalb von 72 Stunden nachdem er davon erfahren hat die zuständige Aufsichtsbehörde informieren, sowie "unverzüglich" die betroffene Person. Außerdem sind solche Verletzungen und ergriffene Maßnahmen zu dokumentieren. Neu ist hier der deutlich weiter als im BDSG gefasste Begriff der "Verletzung des Schutzes personenbezogener Daten" (vgl. [21]). In Artikel 4, Abs. 12 DSGVO wird eine solche Verletzung definiert als "Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden". Im BDSG, Art 42a wurde hier zum Einen anstelle eines klaren Zeitlimits lediglich vorgeschrieben "unverzüglich" Aufsichtsbehörde und Betroffenen zu informieren. Außerdem betraf die Regelung im BDSG bisher nur besondere Arten personenbezogener Daten, nicht dieselben im Allgemeinen.

### Artikel 35 - Datenschutz-Folgenabschätzung

Der Verantwortliche muss bei hohem Risiko bei der Datenverarbeitung personenbezogener Daten vorab eine Risikoabschätzung durchführen, wofür er den Rat des Datenschutzbeauftragten einholt. Im Artikel werden u.a. Fälle aufgelistet, für welche eine Datenschutz-Folgenabschätzung erforderlich ist (z.B. Videoüberwachung) sowie was eine solche Datenschutz-Folgenabschätzung beinhalten sollte:

- Auflistung geplanter Verarbeitungsvorgänge sowie Zweck
- Verhältnismäßigkeit zwischen Zweck und den Verarbeitungsvorgängen
- Risikoeinschätzung für den Betroffenen
- Umgang mit Risiken

Wenn also eine Datenverarbeitung absehbar hohe Risiken für die persönlichen Rechte und Freiheiten des Betroffenen zur Folge hat, muss das Unternehmen diese im Vorfeld umfassend prüfen, dokumentieren und sich eventuell mit der Datenschutzbehörde abstimmen. Diese Regelung ist von der Begrifflichkeit her neu, es gibt jedoch schon etwas Ähnliches: im BDSG von 1990 §4d wird bei besonderen Risiken eine Vorabkontrolle gefordert und auch die europäische Richtlinie beschreibt eine solche in Artikel 20. Schaar weist jedoch darauf hin, dass das Unterscheiden verschiedener Risiken, welches hier betrieben wird, eine Neuerung im Vergleich zur vorherigen gesetzlichen Regelung darstellt (vgl. [16]). Mit Blick auf interne Ermittlungen bei Unternehmen rät Wybitul daran zu denken, dass auch hier im Vorfeld eine Folgenabschätzung zu veranlassen sei (vgl. [21]).

### Artikel 39 - über die Haftung des Datenschutzbeauftragten

In Artikel 39 werden die Aufgaben des Datenschutzbeauftragten (der laut Art. 37 in bestimmten Fällen vom Verantwortlichen ernannt werden muss - hier unterscheiden sich die genannten Fälle in der DSGVO von denen im BDSG von 1990 - und der lt. Erwägungsgrund 97 als Person mit Fachwissen den Verantwortlichen unterstützen soll) aufgeführt. Diese Aufgaben sind deutlich weitgreifender als bisher im BDSG festgehalten (vgl. [BDSG], §4g). Der Datenschutzbeauftragte muss u.a. den Verantwortlichen über seine Pflichten bzgl. der DSGVO und anderer Datenschutzvorschriften sowie Datenschutzstrategien unterrichten und beraten, sich jedoch auch um Schulungen der Mitarbeiter kümmern und insbesondere die Einhaltung der eben genannten Pflichten überwachen. "Diese klar zugewiesene künftige Überwachungspflicht" hält Wybitul gerade in Kombination mit der in 3.5 genannten Sanktionen für ein Zeichen dafür, dass Gerichte und Behörden den Datenschutzbeauftragten zukünftig als Überwachergaranten bewerten werden [21].

## 3.5 Restliche Abschnitte

### Artikel 58 & 83 - Geldbußen und andere Sanktionen

Artikel 83 verhängt empfindliche Geldbußen, falls ein gesetzeswidriges Vorgehen mit personenbezogenen Daten vorliegt. Dabei wird explizit formuliert: "Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird" ([DSGVO], Art. 83, Abs. 9). Wie Schaar schreibt ist hier die Hauptversänderung, auf die sich die Wissenschaft (darauf bezieht sie sich, dies gilt jedoch natürlich genau so für IT-Firmen) einstellen muss, eine deutliche Erhöhung zur bisherigen Regelung nach dem BDSG ist: "Waren es bislang nach dem deutschen Bundesdatenschutzgesetz (BDSG) für Verstöße nach § 43 Bußgelder in Höhe von bis zu 300.000 Euro, sind es nun für direkt Verantwortliche bis zu 10 bzw. 20 Millionen oder zwei bzw. vier Prozent des Jahresumsatzes für Unternehmen" [16]. Die Bußgelder können nicht nur die Unternehmen selbst treffen, sondern auch natürliche Personen - bei diesen "belaufen sich [die Bußgeldrisiken] auf bis zu a 20 Mio. oder a 10 Mio. – je nach der Art des begangenen Verstoßes" [21]. Jedoch drohen Unternehmen bei Verstößen nicht nur Geldbußen: Possekel und Schiemann verweisen auf die Möglichkeit, dass die Aufsichtsbehörde auch befugt sei bei gravierenden Verstößen, die IT-Systeme in den betroffenen Unternehmensbereichen still zu legen (vgl. [12]). Damit beziehen die Autoren sich auf Artikel 58, welcher die Befugnisse der Aufsichtsbehörde beschreibt. Dieser Artikel gibt der Aufsichtsbehörde das Recht auf sämtliche für sie relevante Informationen zuzugreifen, darauf Untersuchungen durchzuführen, auf Verstöße hinzuweisen, zu verwarnen, Geldstrafen zu verhängen und sogar darauf die Datenverarbeitung zu beschränken oder sogar personenbezogene Daten zu löschen.

### Betriebsvereinbarungen und die DSGVO - Artikel 88

Wybitul stellt fest, dass viele der Regelungen der DSGVO sich eher an Datenschutz im Internet oder bei Online-Geschäften orientiere und dadurch an vielen Stellen nicht zu den Besonderheiten des Arbeitsverhältnisses "passe" (vgl. [21]). Passend dazu erlaubt Art. 88 den Mitgliedstaaten Rechtsvorschriften und Kollektivvereinbarungen zum Datenschutz im Beschäftigungskontext, welche der Komission bis zum 25.Mai 2018 mitgeteilt werden müssen. Allerdings unterliegen diese Vereinbarungen bestimmten Auflagen: Die Forderung nach Schutz der menschlichen Würde und Wahrung der Grundrechte unterscheiden sich dabei nicht wirklich von den bisherigen Anforderungen, Wybitul stellt jedoch fest, dass im Bezug auf die vorgeschriebene Transparenz die Vorgaben der DSGVO weit über das bisherige Recht hinaus gehen und dass damit hohe Anforderungen an entsprechende Betriebsvereinbarungen gestellt werden (ebd.).

### Artikel 89 - Anonymisierung und Pseudomisierung zur Verwendung persönlicher Daten in der Forschung

Es gibt eine "ausdrückliche Einführung der „Pseudonymisierung"" ([DSGVO], Erwägungsgrund 28) im neuen DSGVO und in Artikel 89 findet sie Anwendung: Während in der Richtlinie von 1995 eine strikte Anonymisierung vorgeschlagen wurde ([95/46/EG], Erwägungsgrund 26), erlaubt die DSGVO für "im öffentlichen Interesse liegende[] Archivzwecke[]" auch die Pseudomisierung von Daten, solange sichergestellt wird, dass "die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist" ([DSGVO], Art.89, Abs.1). Wie Schaar darstellt ist dies zwar neu im europäischen Recht, im BDSG von 1990 jedoch schon formuliert [16]. So wird dort Anonymisierung deutlich weniger strikt definiert ([BDSG], §3, Abs.6) und auch der Begriff der Pseudomisierung schon eingeführt (ebd. Abs. 6a). Eine Pseudomisierung ist jetzt in der DSGVO definiert als

"Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt

werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden." ([DSGVO], Art.4, Abs.5)

Im Gegensatz dazu gibt es für die Anonymisierung keine eigene Definition in der DSGVO. Schaar führt zum Thema der Anonymisierung weiter aus, dass "genetische Daten an sich nicht anonymisierbar sind", da sie einzigartig seien und selbst bei der Entfernung aller anderen direkt identifizierenden Merkmale seien sie im Prinzip einer Person wieder zuzuordnen [16]. Wie weiter oben bei 3.2 erwähnt dürfen jedoch in bestimmten Fällen (und dazu gehören wissenschaftliche Forschungsprojekte, da der Betroffene zustimmt und der Zweck die Gesundheitsvorsorge ist (ebd.)) trotzdem auch genetische Daten erhoben und verarbeitet werden.

### Erwägungsgrund 1

In diesem Erwägungsgrund, wird der Datenschutz als ein Grundrecht festgelegt. Dieser wichtige Punkt ist in Deutschland seit 30 Jahren gesetzlich geregelt (vgl. [17]). Schmitt formuliert diesen Kontext in ihrer Arbeit, als sei dies auf Europaebene eine Neuerung. Allerdings gibt es seit 2000 die Charta der Grundrechte der Europäischen Union [CdG] und dort ist in Art. 8 der Schutz personenbezogener Daten festgehalten. Diese Charta wiederum ist laut der Bundesregierung rechtlich bindend (vgl. [3]), was Schmitts Implikation widerlegen würde.

### Erwägungsgrund 30

Erstmals befasst sich die gesetzliche Regelung auch mit Online Kennungen, wie IP-Adressen und Cookie-Kennungen. In diesem Erwägungsgrund wird betrachtet, dass solche oftmals natürlichen Personen zugeordnet werden, was wiederum ermöglichen kann, Profile dieser Personen zu erstellen und sie zu identifizieren. Aus diesem Grund unterliegen auch Online Kennungen nun den Bestimmungen der DSGVO. Auch Possekel und Schiemann weisen darauf hin, dass die Nutzung von Cookies durch Unternehmen deutlich strikteren Bestimmungen unterliegen werden, dass auf ihnen basierenden Verarbeitungsprozesse entsprechend dokumentiert werden und prozessual wie vertraglich sicher sein müssen (vgl. [12]).

### Erwägungsgrund 48

Eine positive Neuerung ergibt sich für die Weitergabe personenbezogener Daten zwischen Konzernunternehmen, wie auch Wybitul bemerkt: Erwägungsgrund 48 spricht von einem berechtigten Interesse personenbezogene Daten von Kunden und beschäftigten "innerhalb der Unternehmensgruppe für interne Verwaltungszwecke" zu übermitteln.

## 4 Schlussgedanken

Wie schon in der Einleitung erwähnt, werden einige der neuen Regelungen eine Herausforderung für Unternehmen. Sie müssen nicht nur so spezielle Vorgaben erfüllen wie eine Datenschutz-Folgenabschätzung. G DATA weist auf ein viel allgemeineres Problem hin:

"[V]iele Vorgaben [setzen] voraus, dass Unternehmen wissen, in welchem Umfang und an welchen Stellen sie personenbezogene Daten gespeichert haben. Das kann in einer kleinen Firma mit nur einer zentralen Kundendatenbank noch zutreffen, aber spätestens beim Betrachten von Datenquellen wie Videoüberwachungen in öffentlich zugänglichen Räumen oder auch bei Verarbeitung von Daten in Cloud-Plattformen [...] wird klar,dass viele Firmen viel mehr personenbezogene Daten speichern und verarbeiten ,als ihnen vielleicht bewusst ist und diese auch außerhalb des eigenen direkten Einflussbereichs gespeichert oder verarbeitet werden" [1].

Tatsächlich ist gerade die genannte Videoüberwachung problematisch, da, wie oben erwähnt, biometrische Daten nun als personenbezogene Daten gelten und somit deren Schutz genießen.

Einen weiteren Punkt sprechen Behrend et. al. an, die darauf hinweisen, dass technische Lösungen für Datenschutz in Registern benötigt werden. Man benötigt also auch hier spezielle Softwarelösungen (vgl.

[4]).
Nicht alles wird abschließend mit der neuen DSGVO geklärt. So bleibt zum Beispiel ungeklärt “wie künftig mit einem „Open Access“ bzw. „Scientific Use“ für genetische Daten umgegangen werden kann” [16]. Auch Roßnagel und Nebel vermissen den Umgang mit modernen Informationstechniken [15]. Außerdem monieren sie, dass der Grundsatz der Direkterhebung in der Verordnung nicht verankert sei (ebd.). Fehlende Aspekte sind jedoch nicht die einzigen Kritikpunkte, die genannt werden: Roßnagel bemängelt, die DSGVO sei nur “eine Richtlinie im Gewand einer Verordnung” [14], da sie nur vage formuliert und viel aufgrund der Öffnungsklauseln offen lässt und wieder in die Hand der Mitgliedsstaaten übergibt. Auch Weber sieht die Öffnungsklauseln als eher problematisch, da diese der Idee der Harmonisierung des europäischen Datenschutzrechts widersprechen (vgl. [20]).
Alle diese Kritikpunkte sind berechtigt, haben jedoch das Problem, dass es wahrscheinlich schlicht nicht möglich war, die DSGVO detaillierter und klarer zu gestalten. Schmitt schreibt in ihrem Artikel von 4000 Änderungsanträgen, die nach dem ersten Entwurf der Reform eingingen (vgl. [17]) - wahrscheinlich war eine klarere Regelung schlicht nicht machbar, wenn 28 Mitgliedstaaten ihre eigenen Wünsche zu deren Realisierung haben. Und so offen die DSGVO an einigen Stellen gehalten sein mag - ich bin mir sicher, die Unternehmen empfinden sie aktuell als herausfordernd genug.

## Literatur


[1] G DATA Software AG. „Die neue EU-Datenschutz-Grundverordnung – Was Unternehmen unbedingt wissen müssen“. In: *G DATA Whitepaper* Online verfügbar unter: https://www.gdata.de/fileadmin/web/de/documents/whitepaper/Die_neue_EU _Datenschutz_Grundverordnung_Was _Unternehmen_unbedingt_wissen_muessen.pdf (2017).

[2] Presse und Informationsamt der Bundesregierung. „Datenschutzrecht novelliert“. In: *https:// www.bundesregierung.de/Content/DE/Artikel/2017/02/2017-02-01-datenschutz.html* (2017).

[3] Presse und Informationsamt der Bundesregierung. „Europäische Grundrechtecharta“. In: *https://www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/Europa/Artikel/2014-08-07-europaeische-grundrechtecharta.html* (2018).

[4] Dr. med. C.-A. Behrendt, M. Sc. H. Pridöhl, Dr. K. Schaar, Prof. H. Federrath und Prof. Dr. med. E. S. Debus. „Klinische Register im 21. Jahrhundert; Ein Spagat zwischen Datenschutz und Machbarkeit?“ In: *Chirurg* 11 (2017), S. 944–949. DOI: 10.1007/s00104-017-0542-9.

[5] Wolfgang Graßhof. „Auswirkungen der neuen EU Datenschutzgrundverordnung auf die Softwareentwicklung“. In: Online verfügbar unter https://www.wogra.com/auswirkungen-der-neuen-eu-datenschutzgrundverordnung-auf-die-softwareentwicklung/ (2017).

[6] Winfried Hassemer. „Über die absehbare Zukunft des Datenschutzes“. In: *Kritische Justiz* 29.1 (1996), S. 99–105.

[7] Landtag Hessen. „Gesetz- und Verordnungsblatt für das Land Hessen, Teil 1“. In: *http://starweb.hessen.de/cache/GVBL/1970/00041.pdf* 41 (1970), S. 625–642.

[8] Prof. Dr. Iur. Jürgen Kühling, Prof. Dr. Iur. Mario Martini, Johanna Heberlein, Benjamin Kühl, David Nink, Quirin Weinzierl und Michael Wenzel. „Die Datenschutz-Grundverordnung und das nationale Recht: Erste Überlegungen zum innerstaatlichen Regelungsbedarf“. In: (2016).

[9] J. Müller. „Reformperspektiven des Datenschutzrechts durch eine europäische Datenschutz-Grundverordnung“. In: *Auto-ID-Verfahren im Kontext allgegenwärtiger Datenverarbeitung. DuD-Fachbeiträge* (2018), S. 583–619. ISSN: 978-3-658-19125-2. DOI: 10.1007/978-3-658-19125-2_6.

[10] U. Mielow-Weidmann und P. Weidmann. „Das Bundesdatenschutzgesetz“. In: *Wirtschafts-, Rechts- und Sozialkunde für Sekretärinnen* (1996), S. 287–289. ISSN: 978-3-663-05816-8. DOI: 10.1007/978-3-663-05816-8_19.

[11] Thomas Petri. „Auftragsdatenverarbeitung und ärztliche Schweigepflicht“. In: *Datenschutz und Datensicherheit* 38.12 (2014), S. 862–863. ISSN: 1862-2607. DOI: 10.1007/s11623-014-0333-0.

[12] Martin Possekel und Sven Schiemann. „Risiko Datenschutz“. In: *Controlling & Management Review* 61.8 (2017), S. 58–61. ISSN: 2195-8270. DOI: 10.1007/s12176-017-0098-z.

[13] Martin Hilbert und Priscila López. „The World’s Technological Capacity to Store, Communicate, and Compute Information“. In: *Science* 332.6025 (2011), S. 60–65. DOI: 10.1126/science.1200970.

[14] A. Roßnagel. „Entwurf eines neuen Bundesdatenschutzgesetzes“. In: *Datenschutz und Datensicherheit - DuD* 41 (2017), S. 269–270. ISSN: 1862-2607. DOI: 10.1007/s11623-017-0771-6.

[15] Prof. Dr. Alexander Roßnagel und Maxi Nebel. „Policy Paper: Die neue Datenschutzgrundverordnung. Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet?“ In: *Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt* (2016). ISSN: 2199-8914.

[16] Katrin Schaar. „Was hat die Wissenschaft beim Datenschutz künftig zu beachten?“ In: *RatSWD Working Papers* 257 (2016). DOI: 10.17620/02671.19.

[17] Sabine Schmitt. „EU macht Schluss mit dem Flickenteppich der Datenschutzregeln“. In: *Der Freie Zahnarzt* (2016), S. 26–27. DOI: 10.1007/s12614-016-6073-9.

[18] Adreas Streim und Susanne Dehmel. „Jedes fünfte IT-Unternehmen ignoriert bislang Datenschutzgrundverordnung“. In: *https://www.bitkom.org/Presse/Presseinformation/Jedes-fuenfte-IT-Unternehmen-ignoriert-bislang-Datenschutzgrundverordnung.html’* (2017).

[19] Verbraucherzentrale. „Wann ist deutsches bzw. EU-Datenschutzrecht anwendbar?“ In: *Website vom 30.11.2016, online verfügbar unter: http://www.verbraucherzentrale.de/Wann-ist-deutsches-bzw-EU-Datenschutzrechtanwendbar* (2016).

[20] Heiko Weber. „Internationale Datenverarbeitung und systematisches Datenschutzmanagement mit der Datenschutz-Grundverordnung“. In: *Datenschutz und Datensicherheit* 41.5 (2017), S. 282–284. ISSN: 1862-2607. DOI: 10.1007/s11623-017-0775-2.

[21] Tim Wybitul. „Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte? Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen“. In: *Zeitschrift für Datenschutz* (2016), S. 203–208.

## Gesetze

[BDSG] Bundesdatenschutzgesetz (BDSG), Ausfertigungsdatum: 20.12.1990, zuletzt geändert 31.10.2017

[CdG] Charta der Grundrechte der Europäischen Union, vom 18.12.2000, online verfügbar unter: http://www.europarl.europa.eu/charter/pdf/text_de.pdf

[DSGVO] Datenschutz-Grundverordnung (DSGVO), Verordnung (EU) 2016/679, anwendbar ab 25. Mai 2018, online verfügbar unter: https://dsgvo-gesetz.de/

[GAEB] Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl101s0904.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl101s0904.pdf%27%5D__1515600551248

[95/46/EG] Richtlinie 95/46/EG des europäischen Parlaments und des Rates, vom 24 . Oktober 1995, online verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=DE