Die EU-Datenschutz-Grundverordnung in der anwaltlichen Beratungspraxis

Bearbeitet von
Von Dr. Robert Kazemi

1. Auflage 2017. Buch. Rund 400 S. Hardcover
ISBN 978 3 8240 1450 7
Format (B x L): 14,8 x 21 cm

Recht > Handelsrecht, Wirtschaftsrecht > Telekommunikationsrecht, Postrecht, IT-Recht > Datenschutz, Postrecht

schnell und portofrei erhältlich bei

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

AnwaltsPraxis

Die EU-Datenschutz-Grundverordnung in der anwaltlichen Beratungspraxis

Von
Dr. Robert Kazemi
Rechtsanwalt, Bonn

DeutscherAnwaltVerlag

Inhaltsverzeichnis

§ 2 Zentrale Begriffe

A. Vorbemerkung

Ziel des folgenden Abschnittes ist es, dem Leser die grundlegenden Begriffe näher zu bringen, deren Bedeutung sich auf das gesamte Regelungsgefüge der DSGVO erstreckt. Zum besseren Verständnis der Neuregelungen wird, soweit sinnvoll, auf die Begriffsbestimmungen der Datenschutzrichtlinie sowie des BDSG Bezug genommen, um insbesondere die Neuerungen, die mit der DSGVO einhergehen besser herauszustellen. In Abkehr von der Reihenfolge der Begriffsbestimmungen in Art. 4 der DSGVO werden die Kernbegriffe des Datenschutzrechtes hier thematisch geordnet. Dabei sollen zunächst die Akteure des Datenschutzrechts vorgestellt, anschließend dessen Gegenstand benannt, sodann die Varianten des Umgangs mit Daten dargestellt und schließlich weitere zentrale Begriffe erläutert werden. 1

B. Die Akteure des Datenschutzrechtes

I. Verantwortlicher

Normadressat der DSGVO ist der „**Verantwortliche**“, denn er ist es, der die sich aus der DSGVO ergebenden Verpflichtungen zu beachten hat. Art. 4 Nr. 7 DSGVO definiert den Verantwortlichen als „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“ und orientiert sich damit nahezu wörtlich, an der vormals in Art. 2 lit. d der Richtlinie 95/46/EG vorgegebenen Legaldefinition. Verantwortlicher ist dementsprechend derjenige, der (eigenständig) über den Zweck und die Mittel der Datenverarbeitung entscheidet. Eine nähere Ausgestaltung erfährt diese, zugegebenermaßen recht offene, begriffliche Definition in Kapitel IV, Abschnitt 1, Art. 24 DSGVO. Dessen Abs. 1 normiert den Verantwortlichen als denjenigen, der Art, Umfang und Umstände der Datenverarbeitung festlegt und in diesem Sinne über die Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten zur Verarbeitung personenbezogener Daten entscheidet.[1] Der Verantwortliche im Sinne des Datenschutzrechtes ist derjenige, der „das Heft in der Hand“ hält. Die Art. 29-Datenschutzgruppe führt hierzu aus: 2

> *„Eine Definition von „Zweck“ lautet „erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet“, und eine Definition von „Mittel“ lautet „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird.“*[2]

Der „Verantwortliche“ entscheidet daher über das „Warum“ und das „Wie“ der Datenverarbeitung. Insbesondere der Begriff des Mittels („Wie“) ist dabei sehr vielschichtig und bezeichnet 3

> *„nicht nur die technischen Methoden für die Verarbeitung personenbezogener Daten, sondern auch das „Wie“ der Verarbeitung; dazu gehören Fragen wie „Welche Daten werden verarbeitet?“, „Welche Dritte haben Zugang zu diesen Daten?“, „Wann werden Daten gelöscht?“ usw. Die Entscheidung über die „Mittel“ beinhaltet daher einerseits technische und organisatorische Fragen (wie z.B. „Welche Hardware oder Software wird verwendet?“), und andererseits wesentliche Elemente, [. . .] wie z.B. „Welche Daten werden verarbeitet?“, „Wie lange werden sie verarbeitet?“, Wer hat Zugang zu ihnen?“ usw. Daher gilt, dass die Entscheidung über die Zwecke der Verarbeitung stets eine Einstufung als für die Verarbeitung Verantwortlicher be-*

1 Erwägungsgrund 78 DSGVO.

2 Art. 29-Datenschutzgruppe, WP 169 vom 16.2.2010, S. 16, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf.

dingt, wohingegen die Entscheidung über die Mittel nur dann die Verantwortung für die Verarbeitung impliziert, wenn über wesentliche Aspekte der Mittel entschieden wird. Vor diesem Hintergrund ist es durchaus möglich, dass ausschließlich der Auftragsverarbeiter über die technischen und organisatorischen Mittel entscheidet.“[3]

Verantwortlicher ist daher derjenige, der über die wesentlichen Aspekte der Mittel entscheidet.

4 Kann in diesem Sinne nur eine Person, Behörde oder sonstige Einrichtung ausgemacht werden, die über die vorgenannten Kriterien alleinverantwortlich entscheidet, so gilt nur diese Person, Behörde oder sonstige Einrichtung im Sinne der DSGVO als Verantwortlicher. Probleme bereitet dies, soweit die Verordnung in Art. 4 Nr. 7 normiert, dass es grundsätzlich auch Situationen einer **gemeinsamen Verantwortlichkeit** geben könne. Gemäß Art. 82 Abs. 4 DSGVO, sollen diese „**gemeinsamen Verantwortlichen**“ grundsätzlich auch gemeinsam für die jeweils erfolgende Verarbeitung einstehen müssen. Dies bedeutet indes nicht, dass mehrere Stellen, die gemeinsam „dieselben Daten“ eines Betroffenen verarbeiten, im datenschutzrechtlichen Sinne als eine „einzige“ neue verantwortliche Stelle behandelt werden würden. Vielmehr behält jede Einrichtung auch im Rahmen der gemeinsamen Verarbeitung personenbezogener Daten ihre rechtliche Eigenständigkeit; sie muss sich jedoch Handlungen der jeweils anderen verantwortlichen Stelle – auch soweit diese ihr nicht zu Gute kommen – wie eigene Handlungen zurechnen lassen.[4] Die gemeinsame Verarbeitung soll sich gemäß Art. 26 Abs. 1 DSGVO dadurch kennzeichnen, dass zwei oder mehr Personen, Behörden oder sonstige Einrichtungen **gemeinsam** die Zwecke und Mittel der Verarbeitung festlegen. In diesem Fall, soll es sich um „**gemeinsam Verantwortliche**“ handeln.[5] Wollen zwei oder mehr Personen, Behörden oder sonstige Einrichtungen im vorgenannten Sinne „gemeinsam“ Daten betroffener Personen verarbeiten, so normiert die DSGVO zusätzliche Verpflichtungen, die insbesondere die Transparenz der Datenverarbeitung sicherstellen sollen. So setzt eine „gemeinsame Verantwortlichkeit“ eine (schriftliche) Festlegung der wechselseitigen Verantwortlichkeiten innerhalb der Verarbeitungsprozesse voraus, in deren Rahmen die tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen detailliert dargelegt sind. Die wesentlichen Inhalte derartiger Vereinbarungen sind den betroffenen Personen und den Datenschutzbehörden zur Verfügung zu stellen.[6] Der ursprüngliche Entwurf der DSGVO aus dem Jahre 2012 (Hinweis) sah ursprünglich die Möglichkeit der Abweichung vom Konzept der „gemeinsamen Verantwortlichkeit“ für die Verarbeitung personenbezogener Daten in Unternehmensgruppen (zum Begriff sogleich unter Rdn 14 ff.) vor. Nach Art. 26 Ziff. 5 des damaligen Entwurfes sollte die Kommission ermächtigt sein, über delegierte Rechtsakte Bedingungen festzulegen, durch die die Verarbeitung personenbezogener Daten in Unternehmensgruppen speziell zu Kontroll- und Berichterstattungszwecken vereinfacht werden konnte. Diese Ermächtigung findet sich in der nunmehr verabschiedeten Fassung der DSGVO nicht mehr. Fraglich ist deshalb, wie die verantwortliche Stelle im Rahmen der Datenverarbeitung in Konzernverbünden unter Geltung der DSGVO zu bestimmen sein wird. Zwar enthält die DSGVO in Art. 4 Nr. 19 eine Legaldefinition des Begriff der „Unternehmensgruppe“ nämlich einer Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht, doch knüpft sich an diese Legaldefinition mit Blick auf die Bestimmungen des Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO keine innerhalb der Verordnung selbst konkret definierte Rechtsfolge. Vor dem Hintergrund, dass ein herrschendes Unternehmen dasjenige sein soll, das z.B. aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder für das Unternehmen geltenden Vorschriften oder der Befugnis

3 Ebenda.
4 Art. 82 Abs. 4 DSGVO.
5 Art. 26 Abs. 1 S. 1 DSGVO.
6 Art. 26 Abs. 2 DSGVO.

Datenschutzvorschriften umsetzen zu lassen, einen „beherrschenden Einfluss“ auf die übrigen Unternehmen ausüben und die Verarbeitung personenbezogener Daten innerhalb der ihm angeschlossenen Unternehmen kontrollieren kann,[7] stellt sich die Frage, ob auch innerhalb der Datenverarbeitung innerhalb eines Konzernverbundes eine „gemeinsame Verantwortlichkeit“ der Konzernunternehmen angenommen werden muss oder hier tatsächlich nur ein Verantwortlicher, nämlich das „herrschende Unternehmen“ existiert. Für letzteres, spricht die Legaldefinition der Verantwortlichkeit in Art. 4 Nr. 7 DSGVO. Denn hiernach soll nur derjenige als Verantwortlicher im Sinne der DSGVO gelten, der schlussendlich über Zwecke und Mittel der Verarbeitung bestimmt. Erfolgt diese Bestimmung – wie bei einer Unternehmensgruppe naheliegend – faktisch allein durch das beherrschende Unternehmen, so müsste auch bei Datenverarbeitungen, die tatsächlich nur innerhalb eines Konzernunternehmens stattfinden, die aber verbindlichen Anweisungen, Richtlinien oder ähnlichen Direktiven des herrschenden Unternehmens folgen, schlussendlich allein das beherrschende Unternehmen als verantwortliche Stelle im Sinne der DSGVO gelten. Dies bereitet insbesondere dann Probleme, wenn das in diesem Sinne „herrschende“ Unternehmen, seinen Sitz in einem Drittland hat, wie es insbesondere bei internationalen Konzernverbünden oft der Fall sein wird. Problematisch wird dies deshalb, weil der europäische Gesetzgeber, wie insbesondere aus Erwägungsgrund 37 DSGVO hervorgeht, für die Feststellung, ob ein „beherrschendes Unternehmen“ und damit eine Unternehmensgruppe vorliegt, nicht auf tatsächlich erfolgende Weisungen in Bezug auf die Datenverarbeitung, sondern allein auf die Möglichkeit selbiger abstellt. Nachdem sich eine solche Möglichkeit bereits aufgrund „beherrschender“ Eigentumsverhältnisse ergeben können soll, besteht hier durchaus die Gefahr, dass für zahlreiche Unternehmensgruppen mit Inkrafttreten der DSGVO (ungewollt) der Verantwortliche in einem Drittland niedergelassen wäre. Dies wiederum bedingt u.U. die Benennung eines Vertreters in der EU gem. Art. 27 DSGVO. Um dies zu vermeiden, kann es erforderlich sein, für Datenverarbeitungen durch „abhängige Unternehmen“ eines Konzernverbundes innerhalb der Europäischen Union entsprechende Datenverarbeitungsregeln zu etablieren, die – entgegen der sich aus der DSGVO und ihren Erwägungen ergebenden Annahmen – die Verantwortlichkeit der innerhalb der Gemeinschaft agierenden „abhängigen Unternehmen“ normieren und klarstellen. Insbesondere juristische Berater, die internationale Konzerne im Rahmen der erforderlichen Umsetzungsmaßnahmen in Bezug auf die DSGVO begleiten, sollten hierauf ein besonderes Augenmerk legen und bestehende Unternehmensrichtlinien, Beherrschungsverträge und sonstige Dokumente, aus denen sich ggf. Weisungen in Bezug auf die Mittel, das Ausmaß und/oder die Zwecke von Datenverarbeitung ergeben könnten, einer näheren Prüfung unterwerfen[8] Die DSGVO selbst erlaubt jedenfalls die Verarbeitung[9] durch in Drittländern niedergelassene Verantwortliche, solange und soweit diese Verarbeitung aus dem Drittland gesteuert, nicht jedoch auch im Drittland vollzogen oder personenbezogene Daten aus einem Mitgliedstaat der Gemeinschaft heraus in das Drittland übermittelt werden.

7 Erwägungsgrund 7 DSGVO.

8 Ob die DSGVO und mit ihr der europäische Gesetzgeber tatsächlich derartig weitrechende Konsequenzen für Verarbeitungssituationen in konzernverbundenen Unternehmen bezweckt hat, ist zugegebenermaßen fraglich. Unter Berücksichtigung der Zielsetzung der DSGVO dahingehend, ein möglichst hohen Datenschutzstandard zu etablieren und unter Berücksichtigung des konkreten Wortlautes der DSGVO und ihre Erwägungsgründe selbst, lässt sich eine derartige Konsequenz aber jedenfalls nicht gänzlich ausschließen, sodass die vorbeschriebene Handlungsempfehlung jedenfalls solange sinnvoll „erscheint“, bis Klarheit über die Reichweite des Begriffs des Verantwortlichen, entweder durch Nachbesserungsmaßnahmen auf Gesetzgebungsebene oder durch Rechtsprechung nationaler oder europäischer Gerichte hergestellt worden ist.

9 Zum Begriff sogleich unter Rdn 39 ff.

II. Betroffene Personen

5 Die DSGV schützt „**natürliche Personen**“ bei der Verarbeitung ihrer personenbezogenen Daten.[10] Fraglich ist, wie der Begriff der „natürlichen Person“ im Sinne der DSGVO zu bestimmen ist, insbesondere, ob auch „ungeborenes Leben“ unter den Schutzumfang der DSGVO fallen soll. Die DSGVO selbst äußert sich weder in ihren Erwägungsgründen, noch im Rahmen der „Artikelgesetzgebung“ dazu, ab wann, der Schutzmantel der DSGVO natürlichen Personen zukommen soll. Im Rahmen ihrer Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ hat die Art. 29 Datenschutzgruppe indes bereits im Jahre 2007 zu dieser Problematik Stellung genommen,[11] und dabei – freilich unter Beachtung der zu diesem Zeitpunkt noch geltenden Richtlinienvorgaben und dementsprechend unter Beachtung der nationalstaatlichen Rechtsumsetzungen in den Mitgliedsstaaten – zur Bestimmung des Begriffes der „natürlichen Personen“ auf die zivilrechtlichen Vorgaben in den Mitgliedsstaaten abgestellt. Dabei stellte die Art. 29 Datenschutzgruppe zunächst fest, dass das Zivilrecht der Mitgliedsstaaten zwar den Begriff der „natürlichen Person“ nicht legal definiere, dieser jedoch eng mit dem Begriff „**Rechtspersönlichkeit**“ verknüpft sei, die „als mit der Geburt der Person beginnende und mit ihrem Tod endende Fähigkeit“ verstanden werde, ein Rechtsverhältnis einzugehen.

> „Personenbezogene Daten“ sind folglich Daten, die sich grundsätzlich auf bestimmte oder bestimmbare **lebende Personen** beziehen.[12]

Dies spricht zunächst dafür, die DSGVO und ihre Schutzwirkungen nicht auch auf „ungeborenes“ Leben zu erstrecken, griffe indes – auch unter Berücksichtigung der bisherigen Stellungnahmen der Art. 29 Datenschutzgruppe – zu kurz. Diese erörtert im Rahmen ihrer Stellungnahme 4/2007[13] nämlich zu Recht, in welchem Umfang Datenschutzbestimmungen – in Abweichung des zivilrechtlichen Begriffs der Rechtspersönlichkeit – auch „vor der Geburt“ Anwendung finden können. Obgleich die Art. 29 Datenschutzgruppe in diesem Zusammenhang ausführt, dass sich dies „nach dem allgemeinen Standpunkt der nationalen Rechtssysteme in Bezug auf den Schutz ungeborener Kinder“ zu richten habe, ist innerhalb der Stellungnahme eine Tendenz dahingehend zu erkennen, eher einen weitreichenden Datenschutz zu gewährleisten. So wird die Frage aufgeworfen, ob die Situation ungeborener Kinder insbesondere mit Blick auf die immer weiter fortschreitenden Möglichkeiten medizinischer Forschung, nicht auch durch das Datenschutzrecht erfasst sein könne. Hier wird bspw. der Fall „eingefrorener Embryonen“ genannt, aus denen medizinische und/oder genetische Informationen gewonnen werden können.[14] Die Art. 29 Datenschutzgruppe hatte die Frage, ob ungeborenes Leben vom Schutzbereich des Datenschutzrechtes umfasst sein sollte, schlussendlich nicht zu beurteilen, da – mit Blick auf das Richtlinienkonzept – die Umsetzung alleinige Aufgabe des jeweiligen Mitgliedsstaates war. Mit Inkrafttreten der DSGVO kann die Frage, inwieweit der Schutz der DSGVO auch auf ungeborenes Leben zu erstrecken ist, indes nicht offen gelassen, sondern muss beantwortet werden. Insoweit setzt die DSGVO nicht nur einen Mindeststandard, sondern will – wie eingangs bereits dargestellt – ein einheitliches und kohärentes Datenschutzniveau innerhalb der Europäischen Gemeinschaft sicherstellen. Dies jedoch macht es – je-

10 Art. 1 Abs. 1 sowie Art. 4 Nr. 1 DSGVO

11 Stellungnahme 4/2007 zum Begriff „personenbezogene Daten der Art. 29 Datenschutzgruppe, WP 136, vom 20.6.2007, abrufbar unterhttp://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

12 Ebenda, S. 25.

13 Ebenda, S. 26 am Ende und S. 27 oben.

14 Ebenda, S. 27.

denfalls aus hiesiger Sicht – „unmöglich", die Frage insbesondere des personellen Schutzbereichs weiterhin der mitgliedsstaatlichen Ausgestaltung zu überlassen.

6 Unter Berücksichtigung des bereits im Jahre 2007 von Seiten der Art. 29 Datenschutzgruppe festgestellten Gesichtspunktes, dass in zahlreichen Mitgliedsstaaten bereits zum damaligen Zeitpunkt auch ungeborenem Leben[15] zumindest partielle Rechtsfähigkeit zuerkannt wird und unter Berücksichtigung des Bedeutungswandels des Datenschutzes vom „Randthema" hin zu einem zentralen Themengebiet innerhalb der Bevölkerung, kann die Ausweitung des Schutzbereiches der DSGVO auf das „ungeborene Leben" jedenfalls nicht ohne Weiteres von der Hand gewiesen werden. So gilt bspw. auch in der Bundesrepublik Deutschland ein Mensch erst mit Vollendung seiner Geburt als rechtsfähig.[16] Gleichwohl wird dem noch nicht geborenen Kind jedoch bspw. die Erbrechtsfähigkeit[17] oder auch die Berechtigung zur Geltendmachung von Schadensersatzansprüchen[18] oder Ansprüchen im Falle der Tötung des Urteilspflichtigen[19] zuerkannt. Auch ist anerkannt, dass durch Verträge mit Schutzwirkung zugunsten Dritter das „vorgeburtliche" Leben begünstigt werden kann.[20] Das Übereinkommen über die Rechte des Kindes (UN Kinderrechtskonvention) spricht ebenfalls davon, dass es eines „angemessenen rechtlichen Schutzes **vor** und nach der Geburt" von Kindern bedürfe.[21] Sicherlich können auch die in Europa nach wie vor weitverbreiteten christlichen Wertvorstellungen für eine Ausweitung des Datenschutzrechts und im Speziellen der DSGVO auf „ungeborenes Leben" sprechen. Schlussendlich soll diese Frage, die im Wesentlichen von moralischen und ethischen Gesichtspunkten geprägt wird, hier nicht beantwortet werden. Es bleibt jedoch zu hoffen, dass der europäische Gesetzgeber oder auch der EuGH hier bei Gelegenheit Klarheit schafft.

7 Unter Berücksichtigung der Vorgaben in den Erwägungsgründen der DSGVO[22] soll die DSGVO ungeachtet der Staatsangehörigkeit der betroffenen natürlichen Person Anwendung finden, sodass sich nicht nur EU-Bürger, sondern auch Drittstaatenangehörige auf die dort normierten Schutzvorgaben berufen können. In den Erwägungsgründen heißt es weiter, dass die Schutzwirkungen der DSGVO zudem „ungeachtet des Aufenthaltsortes"[23] Anwendung finden sollen. Sicherlich geht der europäische Gesetzgeber mit dieser Aussage nicht soweit, den europäischen Datenschutzstandards weltweit Geltung beimessen zu wollen, sondern die Verordnung zielt in diesem Punkt vielmehr darauf ab, dass auch Drittstaatenangehörige, soweit sie von Datenverarbeitungen „innerhalb" der Europäischen Union betroffen werden, auf die Einhaltung der in den Grenzen der Union mit der DSGVO normierten Datenschutzstandards drängen können. Dieses – auf den ersten Blick sicherlich begrüßenswerte Vorhaben – kann, insbesondere für in der EU ansässige Unternehmen, die – zeitweilig oder regelmäßig – Daten von Drittstaatenangehörigen verarbeiten, ein nicht unerhebliches Haftungspotenzial mit sich bringen. So wird der EU-DSGVO auch außerhalb der territorialen Grenzen der Europäischen Gemeinschaft „Schutzwirkung zugesprochen". Die EU-DSGVO kann in diesem Sinne auch nach dem Recht von Drittstaaten als „Schutzgesetz" anerkannt werden. Denkt man hier bspw. an die – im Vergleich zur Praxis in der Union – weitreichenden Regelungen

15 Soweit es tatsächlich zur Geburt kommt.
16 § 1 BGB
17 § 1923 Abs. 2 BGB
18 Bspw. im Rahmen vorgeburtlicher Schädigung, § 823 Abs. 1 BGB
19 § 844 Abs. 2 BGB
20 Vgl. auch § 1912 BGB zur „Pflegschaft für eine Leibesfrucht"
21 Präambel Satz 9 der UN Kinderrechtskonvention, abrufbar unter https://www.bmfsfj.de/blob/93140/8c9831a3ff3ebf49a0d0fb42a8efd001/uebereinkommen-ueber-die-rechte-des-kindes-data.pdf.
22 Erwägungsgrund 2.
23 Ebenda.

zur Schadensersatzhaftung nach US-amerikanischem Recht, so kann ein Datenschutzverstoß in Deutschland schnell zu einem erheblichen Problem innerhalb der USA werden. Insoweit stellt sich die Frage, wie zu verfahren ist, wenn die Vorgaben an die Verarbeitung personenbezogener Daten in der DSGVO nicht mit den Vorgaben zur Datenverarbeitung von betroffenen Daten in dem Drittland, in dem sich der Betroffene zum Zeitpunkt der Datenverarbeitung aufhält, übereinstimmen. Zur Vermeidung der Inanspruchnahme durch den Betroffenen nach den Grundsätzen der DSGVO wäre der Verantwortliche im Rahmen seiner Datenverarbeitungen im „territorialen Geltungsbereich der DSGVO" dazu gezwungen, die hier normierten Vorgaben einzuhalten. Weichen diese Vorgaben indes von den Verarbeitungsvorgaben des Drittlandes, in dem sich die betroffene Person aktuell befindet, ab, so besteht die Gefahr, dass eine Datenverarbeitung nach den Grundsätzen der DSGVO gegen die Vorgaben der Verarbeitung von Drittstaatenangehörigen verstößt. Der Verantwortliche könnte in diesem Sinne – auch bei rechtmäßiger Verarbeitung unter Beachtung der Grundsätze der DSGVO – mit Schadensersatz-, Unterlassung- und sonstigen Ansprüchen des Betroffenen konfrontiert werden, soweit sich dieser auf einen Verstoß gegen die Datenschutzgrundsätze des Drittlandes als seinen Aufenthaltsort beruft.

8 Unternehmen, die in diesem Sinne personenbezogene Daten natürlicher Personen aus Drittländern innerhalb der EU verarbeiten wollen, sind dementsprechend dazu gezwungen, im Rahmen ihrer Verarbeitungsvorgänge sowohl die DSGVO als auch das jeweilige Recht des Drittlandes zu beachten. Lassen sich die in beiden Rechtsordnungen normierten Verhaltensregeln nicht in Einklang bringen, so wird darüber zu entscheiden sein, ob die Verarbeitung personenbezogener Daten aus dem betroffenen Drittland tatsächlich innerhalb der EU vollzogen oder besser in das Drittland oder ein anderes Nicht-EU-Mitgliedsland „ausgelagert" werden sollte. Schließlich soll die DSGVO in personeller Hinsicht nicht für die personenbezogenen Daten Verstorbener gelten.[24] Dies auch dann nicht, soweit die Verarbeitung personenbezogener Daten einer natürlichen Person zu Archivzwecken[25] oder zu (historischen) Forschungszwecken[26] betroffen ist. Bereits in ihrer Stellungnahme 4/2007[27] hatte die Art. 29 Datenschutzgruppe betont, dass die Datenschutzrichtlinie in bestimmten Fällen – jedenfalls indirekt – auch die Daten verstorbener Personen schützen könnte. Zwar waren auch unter Berücksichtigung der Vorgaben der Datenschutzrichtlinie Informationen über verstorbene Personen grundsätzlich nicht als personenbezogene Daten anzusehen, da verstorbene Personen im Zivilrecht keine natürlichen Personen darstellten. Die Art. 29 Datenschutzgruppe betonte jedoch, dass der Schutz sich zum Einen daraus ergeben kann, dass der für die Verarbeitung Verantwortliche eventuell nicht feststellen könne, ob die Person, auf die sich die Daten beziehen, noch lebt oder bereits verstorben ist. Deshalb „könne es einfacher sein", Daten über verstorbene Personen ebenfalls im Sinne der Datenschutzbestimmungen der Datenschutzrichtlinie zu verarbeiten, als die beiden Gruppen von Daten voneinander zu trennen.[28] Weiterhin bestünde die Möglichkeit, dass sich Informationen über verstorbene Personen auch auf lebende Personen beziehen. So könne die Information, dass eine verstorbene Person an der Bluterkrankheit litt bspw. darauf hindeuten, dass auch ihre Abkömmlinge an dieser Krankheit leiden. Soweit sich Informationen, die Daten über verstorbene Personen beinhalten, in diesem Sinne gleichzeitig auf lebende Personen beziehen können, komme der verstorbenen Person damit indirekt der Schutz der Datenschutzbestimmungen der Datenschutzrichtlinie zu. Als weiterer denkbarer Fall sei bspw. an die Datensammlung durch die Inkassowirtschaft gedacht. Existiert bspw. ein Schuldner, der im gesetzlichen Güterstand der

24 Erwägungsgrund 27 DSGVO
25 Erwägungsgrund 158 S. 1 DSGVO
26 Erwägungsgrund 160 DSGVO
27 Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 „personenbezogene Daten" WP 136, vom 20.6.2007, S. 26.
28 Ebenda

§ 4 Rechtsgrundlagen der Verarbeitung

A. Datenverarbeitung aufgrund einer Einwilligung, Art. 6 Abs. 1 lit. a) DSGVO

Auch innerhalb des Regelungsgefüges der DSGVO können Verarbeitungen sowohl auf einer Einwilligung des Betroffenen beruhen, als auch ohne Einwilligung erfolgen, z.B. wenn eine Verarbeitung in Erfüllung einer gesetzlichen Verpflichtung erfolgt oder zur Durchführung eines mit dem Betroffenen geschlossenen Vertrages erforderlich ist. Ebenso kennt auch die DSGVO die Verarbeitung auf Grundlage eines berechtigten Interesses des Verantwortlichen in Abwägung mit schutzwürdigen Belangen des Betroffenen. Auch wenn die Verarbeitung auf Grundlage einer Einwilligung in der rein wirtschaftlichen und tatsächlichen Betrachtung, ebenso wie im System der Ermächtigungsnormen der DSGVO keine besondere Position einnimmt und die Verarbeitung auf Grundlage einer Einwilligung auch den anderen Ermächtigungsnormen nicht vorrangig ist,[1] soll – in Anlehnung an die Ordnungsvorgaben der Verordnung – die Datenverarbeitung aufgrund einer Einwilligung auch in diesem Werk an erster Stelle betrachtet werden. 1

I. Inhaltliche Anforderungen an die Einwilligung des Betroffenen

Nach Art. 6 Abs. 1 lit a) DSGVO soll die Verarbeitung zulässig sein, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke[2] gegeben hat. Die Formulierung macht zum einen deutlich, dass eine Einwilligung (zeitgleich) für mehrere Zwecke erteilt werden kann, zum anderen wird klar, dass sich eine Einwilligung auch in einem solchen Fall jeweils auf einen konkreten Zweck beziehen muss.[3] Der Legaldefinition der „Einwilligung" in Art. 4 Nr. 11 DSGVO folgend, ist hierunter 2

> *„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung […], mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist"*

zu verstehen. Die nähre Ausgestaltung der Einwilligung und ihrer Anforderungen sind des Weiteren in Art. 7 DSGVO,[4] Art. 8 DSGVO[5] und Art. 9 Abs. 2 lit. a) DSGVO[6] geregelt. Ergänzend ist

1 In Art. 6 Abs. 1 DSGVO heißt es, dass „mindestens eine der nachstehenden Bedingungen" zu erfüllen ist. Dies belegt zum einen, dass ein Verarbeitungsvorgang zugleich auf mehreren Ermächtigungsnomen beruhen kann, zum anderen, dass ein „Ranggefüge" der Erlaubnistatbestände nicht besteht und die in Art. 6 Abs. 1 DSGVO normierten Grundlagen daher gleichranging nebeneinander stehen. So bspw. auch *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 6 Rn 22 f.

2 Zur Zweckfestlegung § 3 Rdn 15 ff.

3 In Erwägungsgrund 32 DSGVO heißt es: „Wenn die Verarbeitung mehreren Zwecken dient, sollte **für alle diese Verarbeitungszwecke** eine Einwilligung gegeben werden."; siehe auch Erwägungsgrund 42 DSGVO: „Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person **mindestens wissen**, **wer** der Verantwortliche ist und **für welche Zwecke** ihre personenbezogenen Daten verarbeitet werden sollen."

4 Allgemeine Anforderungen.

5 Besondere Anforderungen an die Einwilligung eines Kindes.

6 Besondere Anforderungen bei Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten.

auf die Erwägungsgründe sowie die bisherige Stellungnahmen der Art. 29-Datenschutzgruppe[7] zurückzugreifen.

1. Freiwilligkeit

3 Mit Blick auf die bereits dargestellten Schutzzwecke des Datenschutzrechtes kann eine Einwilligung nur wirksam sein, soweit sie auf der freien Entscheidung des Betroffenen beruht.[8] Dieses Erfordernis der Freiwilligkeit stellt eines der wesentlichen Anforderungen an eine wirksame Einwilligungserklärung dar. Nach den Vorgaben der über Art. 6 Abs. 1 EUV in Bezug genommenen Charta der Grundrechte der Europäischen Union (Art. 8 GRCh) steht dem Einzelnen grundsätzlich frei, selbst zu entscheiden, welchen Dritten er seine Daten offenbaren möchte. Das Erfordernis der Freiwilligkeit kann insbesondere fehlen, wenn sich der Betroffene gegenüber dem Verantwortlichen in einer Situation befindet, in der der Verantwortliche dem Betroffenen rechtlich oder tatsächlich überlegen ist.

4 Bei Einwilligungen, die im Zusammenhang mit der Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, erklärt bzw. eingeholt werden, kann die Freiwilligkeit gem. Art. 7 Abs. 4 DSGVO daran scheitern, dass sich die Einwilligung nicht auf diejenigen Daten beschränkt, die für die Erfüllung erforderlich sind[9] und der Betroffene hierauf nicht deutlich hingewiesen wurde. Erforderlich ist daher stets eine klare Information dazu, welche Daten für die Vertragserfüllung zwingend erforderlich sind und bei welchen Daten es sich lediglich um nicht erforderliche Informationen handelt.

a) Freiwilligkeit im Beschäftigungsverhältnis

5 Mit Blick auf den Gesichtspunkt der Freiwilligkeit wird bereits heute die Einwilligung im Arbeitsrecht und auch bei allen anderen Beschäftigungsverhältnissen als problematisch[10] eingestuft.

6 Die Problematik konzentriert sich dabei auf die regelmäßig existenzielle Bedeutung des Arbeitsplatzes, die dazu führen soll, dass ein Beschäftigter normalerweise nicht dem „Wunsch" seines Arbeitgebers oder Dienstherrn nach einer „freiwilligen" Zustimmung wirksam entgehen könne. Deshalb wird die Möglichkeit der Einwilligung des Arbeitnehmers/Beschäftigten als Erlaubnis zur

7 Insbesondere: Stellungnahme 15/2011 zur Definition von Einwilligung vom 13.7.2011, WP 187, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf; Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies vom 2.10.2013, WP 2008, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_de.pdf; Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht vom 7.6.2012, WP 194, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_de.pdf.

8 Erwägungsgrund 32 spricht von einer eindeutigen Handlung des Betroffenen, „mit der **freiwillig** [...] bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist."

9 Erwägungsgrund 43 DSGVO a.E.

10 *Bergmann/Möhrle/Herb*, BDSG, 40. Ergänzungslieferung, Nov. 2009, § 4a Rn 5a; *Schild/Tinnefeld*, DuD 2009, 469; Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten (Arbeitspapier 48) und Arbeitspapier über eine gemeinsame Auslegung des Art. 26 Abs. 1 der Richtlinie 95/46/EG (Arbeitspapier 114) der Art. 29-Gruppe, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm; Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten vom 13.9.2001, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_de.pdf.

Erhebung und Verwendung von Arbeitnehmerdaten außerhalb der vom Gesetz ausdrücklich zugelassenen Anwendungsfälle von Teilen der bundesdeutschen Literatur generell abgelehnt.[11] Die Vertreter, die eine Einwilligung im Arbeitsverhältnis als unzulässig ansehen, begründen dies insbesondere damit, dass eine *„Einwilligung unzulässige Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers nicht legitimieren"* könne, weil dem Arbeitnehmer die nötige Unabhängigkeit fehle, die im Rahmen einer freiwilligen Entscheidungsfindung von entscheidendem Interesse sei.[12] Wegen des im Beschäftigungsverhältnis bestehenden Machtungleichgewichtes zwischen Verantwortlichem (Arbeitgeber/Dienstherr) und Betroffenem (Arbeitnehmer/Beschäftigter) sei die Freiheit des Einzelnen zur Selbstbestimmung notwendigerweise ausgeschlossen.

Man wird indes nicht generell davon ausgehen können, dass Arbeitnehmer/Beschäftigte grundsätzlich nicht in der Lage seien, frei und ohne Druck zu entscheiden, ob sie eine Einwilligungserklärung gegenüber ihrem Arbeitgeber als Verantwortlichem abgeben sollen.[13] Es wäre vielmehr mit den Grundsätzen der Charta unvereinbar, den Betroffenen im Rahmen von Arbeits- und/oder Beschäftigungsverhältnissen in der Weise zu entmündigen, dass er nicht mehr berechtigt wäre, eine Verarbeitung seiner Daten zu billigen und für deren Zulässigkeit nur noch objektive Kriterien und nicht sein subjektives Empfinden maßgebend sein zu lassen.[14] 7

Ohne auf die speziellen Fallgestaltungen des Datenschutzrechtes im Beschäftigungsverhältnis an dieser Stelle näher eingehen zu wollen, sei unter Berücksichtigung des Vorgenannten und unter dem Stichwort der Freiwilligkeit festgehalten, dass grundsätzlich auch im Arbeitsverhältnis die Möglichkeit der Erteilung einer Einwilligung in die Verarbeitung personenbezogener Daten nicht grundsätzlich ausscheidet. Es ist vielmehr davon auszugehen, dass an die Erteilung einer Einwilligung im Arbeitsverhältnis mit Blick auf die Freiwilligkeit hohe Anforderungen zu stellen sind. Eine Einwilligung scheidet nur aus, wenn nachweislich aus der Verweigerung der Einwilligung oder aus dem Widerruf der Einwilligung für den Beschäftigten ein Nachteil entsteht oder aus seiner Sicht entstehen könnte. Dabei ist zu beachten, dass der Arbeitnehmer in seiner Willensbildung grundsätzlich autonom ist und aus dem Arbeitsverhältnis „*nicht automatisch stets aufgrund einer wirtschaftlichen Machtposition des Arbeitgebers ein solcher Druck entsteht, der keinen Spielraum für Einwilligungen im Arbeitsverhältnis mehr belässt*".[15] 8

Wird eine Einwilligung vom Beschäftigten erbeten und ist die Nichteinwilligung nicht mit tatsächlichen oder potenziellen Nachteilen für ihn verbunden, so ist eine solche Einwilligung freiwillig. Nur dort, wo der Beschäftigte keine Möglichkeit zur Ablehnung hat, kann nicht von Freiwilligkeit gesprochen werden. Nach Auffassung der Art. 29-Datenschutzgruppe können insbesondere Probleme bestehen, wenn die Einwilligung Einstellungsvoraussetzung ist. Zwar habe der Bewerber in einer solchen Situation *„theoretisch das Recht, die Einwilligung zu verweigern, er müsse aber in* 9

11 *Simitis*, in: Festschrift für Dieterich, 1999, S. 601, 628; *ders.*, AuR 2001, 429, 431; *Meier*, Ortung eigener Mitarbeiter zu Kontrollzwecken in: Taeger/Wiebe (Hrsg.), von AdWords bis Social Networks – neue Entwicklung im Informationsrecht, Tagungsband Herbstakademie 2008, 2008, S. 369, 372; *Meyer*, K&R 2009, 14, 16; *Trittin/Fischer*, NZA 2009, 343, 344; *Kunst*, Individualarbeitsrechtliche Informationsrechte des Arbeitnehmers, S. 77.

12 Hamburger Datenschutzbeauftragter, 18. Tätigkeitsbericht, S. 197.

13 Zur bisherigen Rechtlage im BDSG, bspw. *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, § 4a Rn 61; *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 4a Rn 23; *Thüsing/Lambrich*, BB 2002, 1146, 1150.

14 *Gola*, in: Gola/Schomerus (Hrsg.), BDSG, 10. Aufl. 2010, § 4 Rn 9; *Müller*, in: Festschrift für Söllner, 1999, S. 809, 836; *Thüsing/Lambrich*, BB 2002, 1146, 1150.

15 So *Taeger*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, § 4a Rn 62.

diesem Fall damit rechnen, dass er die Chance auf eine bestimmte Stelle verliert, weswegen unter solchen Umständen die Einwilligung nicht freiwillig erteilt werden könne".[16]

10 Ob die Kritik in ihrer Gänze berechtigt ist, erscheint fraglich. Zwar stellt sich auch hier die Frage, ob grundsätzlich und generell davon ausgegangen werden kann, dass im Rahmen der Begründung von Arbeitsverhältnissen eine freiwillige Einwilligungserklärung des Betroffenen ausscheiden muss. Zugegeben, jeder Bewerber hofft auf den Erhalt der ausgeschriebenen Stelle, aber macht ihn dies zugleich zum Abhängigen, der grundsätzlich nicht mehr freiwillig und informiert über sein Recht auf informationelle Selbstbestimmung entscheiden kann? Dies erscheint fraglich. Vielmehr gibt es, wie *Thüsing*[17] zutreffend formuliert, „*keinen Grund dafür, den Datenschutz gegen den zu schützen, der durch den Datenschutz geschützt ist. Es wäre vielmehr eine Beschränkung der Grundrechte des Arbeitnehmers, die der Rechtfertigung bedarf – und die fehlt, wo der Entschluss des Arbeitnehmers tatsächlich freiwillig, informiert und jederzeit widerruflich erfolgt.*"[18]

11 Dementsprechend kann auch die Durchführung von Einstellungs- und Eignungstests nicht grundsätzlich als unzulässig angesehen werden. Hier wird es vielmehr darauf ankommen, dass der Beschäftigte über Sinn und Zweck des vorzunehmenden Tests hinreichend aufgeklärt ist. Hierzu gehört eine Aufklärung über dessen Art und Umfang sowie eine Offenlegung der Testergebnisse gegenüber dem Betroffenen. Soweit dieser darüber informiert ist, was im Einzelnen getestet wird und auch erfahren kann, wie das Testergebnis ausgefallen ist, kann – unter dem Gesichtspunkt, dass eine einmal erteilte Einwilligung grundsätzlich jederzeit widerruflich ist – grundsätzlich nicht davon ausgegangen werden, dass Bewerber nicht in der Lage sein sollen, eine freiwillige Entscheidung zu treffen. Ist der Bewerber mit der Durchführung eines Einstellungs- oder Eignungstestes nicht „überrannt" worden, sondern hatte hinreichend Zeit, sich darüber Gedanken zu machen, ob er an einem solchen teilnehmen will oder nicht, bestehen nach hiesiger Auffassung keine grundlegenden Bedenken gegen die Durchführung derartiger Datenerhebungen. Dies gilt jedoch sicherlich nur, soweit die Durchführung derartiger Tests überhaupt geeignet sein kann, über die Eignung des Bewerbers für die ausgeschriebene Stelle Auskunft zu geben. Unter vorgenannten Voraussetzungen sind auch ärztliche Einstellungsuntersuchungen – mit Einwilligung des Betroffenen – grundsätzlich möglich, soweit sie sich darauf beschränken, festzustellen, ob ein Bewerber für eine bestimmte Position geeignet oder ungeeignet ist. Andere Details, als die Tatsache der Eignung dürfen dem Arbeitgeber vom Arzt wegen der ärztlichen Verschwiegenheitspflicht ohne konkrete Einwilligung des Untersuchten ohnehin nicht mitgeteilt werden.[19]

Bei allem gilt es zu beachten, dass es den Mitgliedstaaten nach Art. 88 DSGVO unbenommen bleibt, den Datenschutz im Beschäftigtenverhältnis durch nationale Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischeren Vorschriften zu unterwerfen. Von dieser Möglichkeit hat der deutsche Gesetzgeber in § 26 BDSG-Neu[20] Gebrauch gemacht.[21]

16 Stellungnahme 15/2011 zur Definition von Einwilligung vom 13.7.2011, WP 187, S. 16, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf.

17 *Thüsing*, NZA 2011, 16, 18.

18 Siehe auch Erwägungsgrund 42 DSGVO: „Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine **echte oder freie Wahl** hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, **ohne Nachteile** zu erleiden."

19 *Wedde*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 28 Rn 28.

20 Hierzu BT-Drucks 18/11325 v. 24.2.2017, in der Fassung der vom Bundestag beschlossenen Beschlussempfehlung des Innenausschusses, BT-Drucks 18/12084 v. 25.4.2017, hierzu auch Plenarprotokoll BT-PlPr 18/231, S. 23306D. Die Verabschiedung durch den Bundesrat stand zum Zeitpunkt der Manuskripterstellung dieses Werkes noch aus.

21 Hierzu § 9 Rdn 14 ff.

b) Freiwilligkeit bei Auslobung finanzieller Anreize

12 Ebenfalls unter dem Stichwort der Freiwilligkeit werden Fälle diskutiert, in denen gegen das sogenannte **Kopplungsverbot** verstoßen wird. Fraglich ist, ob die Freiwilligkeit der Einwilligungserklärung dort ihre Grenze finden muss, wo dem Betroffenen seine Einwilligung von einer stärkeren Partei „abgepresst" wird.[22] Problematisch soll es insbesondere sein, wenn die Gewährung einer Leistung von einer Einwilligung in die Datenverarbeitung abhängig gemacht wird, die nicht dem eigentlichen „Geschäft" dient.[23] Dementsprechend wird vertreten, dass die Einwilligung nicht mehr auf einer freien Entscheidung des Betroffenen beruhen könne, wenn dieser durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten verleitet wurde.[24]

13 Ob Anreize finanzieller oder sonstiger Natur unter datenschutzrechtlichen Gesichtspunkten tatsächlich dazu führen können, dass die Einwilligung des Betroffenen nicht mehr auf seiner freien Entscheidung beruht, ist hingegen fraglich und nach hiesiger Ansicht im Ergebnis abzulehnen.

14 Es ist durchaus möglich, dass – unter datenschutzrechtlichen Gesichtspunkten – Einwilligungserklärungen auch „käuflich" erworben werden können, soweit der Betroffene über Sinn und Zweck der erkauften Einwilligung hinreichend informiert ist und ihm die Möglichkeit verbleibt, seine einmal erteilte Einwilligung zu widerrufen.[25] Insoweit schließt nicht jedes Werbegeschenk oder die Chance, einen bestimmten Preis zu gewinnen, das Vorliegen einer freien Entscheidung aus. Auch wenn die Leistung nur gegen die Preisgabe von Daten angeboten wird, wird es nicht generell an der Freiwilligkeit der Einwilligungserklärung fehlen,[26] solange es sich um eine „freiwillige" Leistung des Verantwortlichen handelt, die der Betroffene auch auf andere Weise erlangen kann. In einem solchen Fall ist die Erteilung einer – im Übrigen den Anforderungen des Art. 4 Nr. 11 DSGVO entsprechenden – Einwilligung vielmehr als Äquivalent einer ansonsten zu leistenden finanziellen Gegenleistung anzusehen. Es erschließt sich nicht, warum nicht auch die Preisgabe von bestimmten Daten zum Gegenstand eines „Rechtsgeschäftes" gemacht werden können sollte.[27]

15 In diesem Fall kann auch vom Grundsatz der jederzeitigen Widerruflichkeit in Art. 7 Abs. 3 DSGVO abgewichen werden. Denn, wird die Einwilligung zum Gegenstand eines konkreten Vertrages gemacht, kann ihr Widerruf eine Verletzung der übernommenen Hauptleistungspflicht des Betroffenen (hier: Einräumung der Befugnis zur Datennutzung innerhalb des vertraglich festgelegten und „erworbenen" Zweckes) darstellen.[28] In diesem Fall dient der Ausschluss des Widerrufsrechts der Ausübung von Rechtsansprüchen des Verantwortlichen im Sinne des Art. 21 Abs. 1 DSGVO, mit der Folge, dass der Widerruf der Einwilligung nur noch unter engen Voraussetzungen möglich und zulässig ist. Dies kann z.B. der Fall sein, wenn eine von der Einwilligung abweichen-

22 So *Schapper/Dauer*, RDV 1987, 169, 170.

23 *Schafft/Ruoff*, CR 2006, 499, 504.

24 *Bergmann/Möhrle/Herb*, BDSG, 40. Ergänzungslieferung, Nov. 2009, § 4a Rn 7; BGH, Urt. v. 16.7.2008 – VIII ZR 348/06, MMR 2008, 731 m. Anm. *Grapentin* = NJW 2008, 3055.

25 In diesem Sinne wohl auch Art. 29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung vom 13.7.2011, WP 187, S. 17, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf. Hier heißt es: *„Im zweiten Fall gibt es einen **kleinen finanziellen Anreiz**, sich für die elektronische Patientenakte zu entscheiden. Patienten, die nicht einwilligen, erleiden keinen Nachteil, da sich die Kosten für sie nicht ändern. Auch hier kann man sagen, dass ihre Entscheidung für oder gegen das neue System ohne Zwang erfolgt."*

26 Anders insoweit *Bergmann/Möhrle/Herb*, BDSG, 40. Ergänzungslieferung, Nov. 2009, § 4a Rn 7.

27 So nun auch BGH, Urt. v. 14.3.2017 – VI ZR 721/15, Rn 22, juris.

28 In diesem Sinne wohl auch *Gola*, in: Gola (Hrsg.), DS-GVO, 2017, Art. 4 Rn 68 a.E.; *Kugelmann*, DuD 2016, 566, 568 f..

de Verarbeitung erfolgt, die notwendige Datensicherung fehlt oder wegen sonstiger Umstände ein Festhalten an der Einwilligung nicht mehr zumutbar ist.[29]

16 Eine andere Auffassung vertritt offenbar das OLG Köln.[30] Dieses bezog sich auf die Bestimmungen des UWG und führte mit Blick auf eine durch die datenerhebende Stelle durchgeführte Ticketverlosung für Tickets anlässlich der FIFA-WM 2006 aus, dass sich die Einflussnahme auf die Entscheidung des Verbrauchers, ob er die erforderliche Einwilligung erteilen will oder nicht, nicht nur auf die Auslobung eines attraktiven Gewinnes und den aleatorischen Anreiz beschränke. Sei die Entscheidung „in unangemessener Weise verstärkt durch die psychisch schwierige Situation, in der sich der Verbraucher befindet, wenn er erstmals von der Kopplung zwischen Gewinnspielteilnahme und Einwilligungserklärung erfahre", könne vielmehr von einer freiwilligen Erklärung nicht mehr ausgegangen werden.

17 Im vom OLG Köln zu entscheidenden Fall bestand die Besonderheit darin, dass die Teilnahme von der Einwilligung in Werbemaßnahmen abhängig gemacht wurde und der Betroffene erst, nachdem er sich mit der Beantwortung einer Gewinnfrage und Anklicken der „Weiter-Schaltfläche", dem Ausfüllen der Felder mit seinen persönlichen Daten auf der Folgeseite und dem Anklicken der Schaltfläche „Senden" bereits für die Teilnahme an der Verlosung entschieden hatte, davon erfuhr. Zu diesem Zeitpunkt aber war, so das OLG Köln weiter, der auf den Verbraucher ausgeübte psychische Druck zu einer Entscheidung für die Abgabe seiner Einwilligungserklärung bereits derart hoch, dass von einer freiwilligen Einwilligungserklärung nicht mehr ausgegangen werden konnte. Auch das OLG Köln behauptet nicht, dass eine offene Kommunikation des Umstandes, dass die Teilnahme an dem vorbezeichneten Gewinnspiel von der Erklärung einer Einwilligungserklärung in Werbemaßnahmen abhängig gemacht wird, an sich zur Annahme von Unfreiwilligkeit führen muss. Dem OLG ist jedoch dahingehend zuzustimmen, dass eine verdeckte oder wesentlich verspätete Offenbarung dieses Umstandes sicherlich Zweifel an der Freiwilligkeit der Einwilligungserklärung erregen kann. Aus dem Urteil jedoch darauf zu schließen, dass immer dann nicht mehr von einer freien Entscheidung im Sinne des Art. 4 Nr. 11 DSGVO gesprochen werden kann, wenn der Betroffene durch übermäßige Anreize finanzieller oder sonstiger Natur zur Preisgabe seiner Daten verleitet wird, erscheint indes zu eng.

18 **Exkurs: Wettbewerbsrechtliche Gesichtspunkte**

Vorstehende Ausführungen beziehen – dem eigentlichen Inhalt dieses Werkes geschuldet – nur die datenschutzrechtlichen Betrachtungen in die Bewertung ein. Insbesondere mit Blick auf die Freiwilligkeit der Einwilligungserklärung könnte sich jedoch aus wettbewerbsrechtlichen Gesichtspunkten eine Unlauterkeit aus dem Umstand ergeben, dass die datenerhebende Stelle versucht, datenschutzrechtliche Einwilligungen durch die Auslobung finanzieller oder sonstiger Anreize zu beschaffen. Dies könnte unter dem Gesichtspunkt des § 4a Abs. 1 Nr. 3 UWG der Fall sein, wenn der ausgelobte finanzielle oder sonstige Anreiz geeignet ist, die Entscheidungsfreiheit der angesprochenen Verbraucher in unangemessener, unsachlicher Weise zu beeinflussen. § 4a Abs. 1 Nr. 3 UWG bezweckt in erster Linie den Schutz der geschäftlichen Entscheidungsfreiheit der potenziellen und tatsächlichen Marktpartner (Verbraucher und sonstige Marktteilnehmer) vor, bei und nach Vertragsschluss. Dabei basiert die Vorschrift auf dem Gedanken, dass Wettbewerb nur funktionieren kann, wenn die potenziellen Marktpartner ihre Marktentscheidungen frei und an ihren Bedürfnissen ausgerichtet treffen. Nach Art. 8 der Richtlinie 2005/29/EG über unlautere Geschäftsprakti-

29 Hierzu ebenfalls Art. 21 Abs. 1 DSGVO.

30 OLG Köln, Urt. v. 15.8.2007 – 6 U 63/07, abrufbar unter: http://www.jurpc.de/rechtspr/20070200.htm.

ken (UGP-Richtlinie)[31] sind insbesondere aggressive Geschäftspraktiken geeignet, den Wettbewerb in unvorteilhafter Weise zu stören. Eine Geschäftspraktik gilt als aggressiv, „wenn sie im konkreten Fall unter Berücksichtigung aller tatsächlichen Umstände die Entscheidungs- oder Verhaltensfreiheit des Durchschnittsverbrauchers in Bezug auf ein Produkt durch Belästigung, Nötigung, einschließlich der Anwendung körperlicher Gewalt oder durch unzulässige Beeinflussung tatsächlich oder voraussichtlich erheblich beeinträchtigt und dieser dadurch tatsächlich oder voraussichtlich dazu veranlasst wird, eine geschäftliche Entscheidung zu treffen, die er anderenfalls nicht getroffen hätte". Die unzulässige Beeinflussung, die im Falle der Auslobung finanzieller Anreize alleine maßgeblich sein könnte, ist in Art. 8 der UGP-Richtlinie definiert als „Ausnutzung einer Machtposition gegenüber dem Verbraucher zur Ausübung von Druck, auch ohne die Anwendung oder Androhung körperlicher Gewalt in einer Weise, die die Fähigkeit des Verbrauchers zu einer informierten Entscheidung wesentlich einschränkt". Der Begriff der Machtposition ist dabei nach allgemeiner Meinung im Interesse eines wirksamen Verbraucherschutzes weit auszulegen[32] und erfasst jede Form der Überlegenheit des Unternehmers gegenüber dem Verbraucher. Diese Überlegenheit kann grundsätzlich auch wirtschaftlich bedingt sein. Dennoch muss die Ausübung von Druck dergestalt sein, dass sie die Fähigkeit des Verbrauchers zu einer informierten Entscheidung wesentlich einschränkt. Dies ist nur gegeben, wenn im konkreten Fall das Urteilsvermögen des Verbrauchers, also seine Fähigkeit, seine Entscheidung aufgrund von Informationen und damit auch aufgrund von rationalen Erwägungen über deren Vor- und Nachteile zu treffen, beeinträchtigt ist bzw. beeinträchtigt sein kann. Ob die Druckausübung dieses Maß erreicht, beurteilt sich nach den Umständen des Einzelfalles. Dabei ist zu beachten, dass die Beeinflussung grundsätzlich „erheblich" sein muss. Es darf sich also nicht um eine geringfügige Einwirkung handeln, durch die ein verständiger Durchschnittsverbraucher nicht in seinen Entscheidungen oder seinem Verhalten beeinflusst werden kann.[33] Mit Blick auf das in Aussicht stellen finanzieller Anreize ist ein sonstiger unangemessener, unsachlicher Einfluss jedoch nur anzunehmen, wenn der finanzielle Anreiz die Fähigkeit des Verbrauchers, eine „informierte Entscheidung" zu treffen, erheblich beeinträchtigen kann. Nach der Rechtsprechung ist dies nur der Fall, wenn die Rationalität der Nachfrageentscheidung des Verbrauchers völlig in den Hintergrund tritt[34] und der verständige Durchschnittsverbraucher durch den geschaffenen finanziellen Anreiz davon abgehalten wird, Preis und Qualität des Gesamtangebotes kritisch zu überprüfen,[35] insbesondere Vergleiche mit Konkurrenzangeboten vorzunehmen.[36] Dies dürfte „nur in Ausnahmefällen anzunehmen sein".[37] Auch unter wett-

31 Richtlinie 2005/29/EG des Europäischen Parlamentes und des Rates vom 11.5.2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl EU (2005) Nr. L 149, S. 22.

32 *Köhler/Bornkamm*, UWG, 35. Aufl. 2017, § 4a Rn 1.72; *Glöckner/Henning-Bodewig*, WRP 2005, 1311, 1333; *Henning-Bodewig*, WRP 2006, 621, 625; *Steinbeck*, WRP 2008, 865, 866.

33 *Köhler/Bornkamm*, UWG, 35. Aufl. 2017, § 4a Rn 1.34.

34 BGH, Urt. v. 14.12.2000 – I ZR 147/98, GRUR 2001, 752 – Eröffnungswerbung; BGH, Urt. v. 6.6.2002 – I ZR 45/00, GRUR 2002, 1000, 1002 – Testbestellung; BGH, Urt. v. 13.6.2002 – I ZR 173/01, BGHZ 151, 84, 89 – Kopplungsangebot I; BGH, Urt. v. 22.5.2003 – I ZR 8/01, WRP 2003, 1428, 1429 – Einkaufsgutschein; OLG Naumburg, Urt. v. 26.8.2005 – 10 U 16/05, GRUR-RR 2006, 336, 339.

35 BGH, Urt. v. 17.2.2000 – I ZR 239/97, GRUR 2000, 820, 821.

36 BGH, Urt. v. 6.6.2002 – I ZR 45/00, GRUR 2002, 1000, 1002 – Testbestellung; *Köhler/Bornkamm*, UWG, 35. Aufl. 2017, § 4a Rn 1.32; BGH, Urt. v. 8.10.1998 – I ZR 107/97, WRP 1999, 516, 517.

37 So *Köhler* in: Köhler/Bornkamm, UWG, 35. Aufl. 2010, § 4a Rn 1.61; LG Frankfurt, Urt. v. 11.11.2004 – 2/3 O 241/04, GRUR-RR 2005, 96, 97.

bewerbsrechtlichen Gesichtspunkten tritt die Rationalität der Nachfrageentscheidungen in aller Regel nicht völlig in den Hintergrund, wenn der Verbraucher oder sonstige Marktteilnehmer Gelegenheit hatte, das Angebot und damit auch seinen Bedarf ausreichend zu prüfen. Selbst bei einem absolut oder relativ hohen finanziellen Anreiz ist daher nicht ohne Weiteres eine unangemessene, unsachliche Beeinflussung des Verbrauchers oder sonstigen Marktteilnehmers anzunehmen.[38] Auch finanziell hohe Anreize müssen nicht grundsätzlich zu einer irrationalen Nachfrageentscheidung führen, solange die Transparenz des Angebotes gegeben ist.[39] Es ist sogar möglich, dass gerade der hohe Wert eines finanziellen Anreizes für den verständigen Verbraucher ein wichtiges und rationales Kalkül der Nachfrageentscheidung sein kann,[40] so dass bei besonders hohen finanziellen Anreizen eher davon auszugehen ist, dass der Verbraucher oder sonstige Marktteilnehmer eine bewusste und damit freiwillige Entscheidung getroffen hat. Auch ist zu beachten, wie viel Zeit dem Verbraucher oder sonstigen Marktteilnehmer für die Erteilung seiner Einwilligung verbleibt. Kann er diese nach „reiflicher Überlegung" tätigen, so spricht ebenfalls viel dafür, nicht von einer unangemessenen, unsachlichen Beeinflussung im Sinne des § 4a UWG auszugehen. Auch unter wettbewerbsrechtlichen Gesichtspunkten ist das Bewegen des Betroffenen zur Erteilung einer Einwilligung durch die Schaffung finanzieller Anreize daher nicht unlauter bzw. unwirksam.

c) Freiwilligkeit bei Verhandlungsungleichgewicht

19 An der Freiwilligkeit kann es des Weiteren fehlen, wenn *„zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht"*.[41]

20 Dies soll nach den Erwägungsgründen der Fall sein, *„wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde"*.[42] Auch im Bereich der Versicherungswirtschaft kann dies der Fall sein.[43] Ob ein klares Ungleichgewicht vorliegt, ist im jeweiligen Einzelfall zu beurteilen; die Formulierung „klar" lässt darauf schließen, dass nicht bereits jedes (wirtschaftliche) Ungleichgewicht der Freiwilligkeit entgegensteht, sondern selbiges ein gewisses Gewicht entfalten muss, welches sich z.B. in einer besonderen Notlage des Betroffenen ausdrücken kann.

d) Erzwungene Einwilligungen

21 Schließlich sind auch erzwungene oder etwa durch arglistige Täuschung erschlichene Einwilligungen ebenso wie nicht hinreichend erläuterte Einwilligungen in aller Regel nicht als freiwillige Einwilligungen einzustufen. Die Freiwilligkeit einer Entscheidung setzt Kenntnis über ihre Reichweite voraus, sodass durch Täuschung erlangte Einwilligungserklärungen niemals freiwillig sein können. In den Erwägungsgründen[44] heiß es hierzu:

> *„Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, ob-*

38 BGH, Urt. v 10.4.2003 – I ZR 291/00, GRUR 2003, 890, 891 – Buchclub-Kopplungsangebot; OLG Stuttgart, Urt. v. 7.3.2002 – 2 U 111/01, GRUR 2002, 906, 908; *Köhler*, GRUR 2001, 1067, 1073; *Köhler* in: Köhler/Bornkamm (Hrsg.), UWG, 28. Aufl. 2010, § 4a Rn 1.70.

39 BGH, Urt. v. 13.6.2002 – I ZR 173/01, GRUR 2002, 976, 978 – Kopplungsangebot I; *Köhler*, GRUR 2001, 1067, 1069, 1073.

40 Vgl. OLG Köln, Beschl. v. 22.11.2004 – 6 W 115/04, GRUR-RR 2005, 168.

41 Erwägungsgrund 43 DSGVO.

42 Erwägungsgrund 43 DSGVO.

43 Vgl. BVerfG, Beschl. v. 23.10.2006 – 1 BvR 2027/02, DuD 2006, 817 = RDV 2007, 20; ausführlich hierzu *Kazemi/Leopold*, Datenschutzrecht in der anwaltlichen Beratung, § 3 Rn 114 ff.

44 Erwägungsgrund 43 DSGVO.

wohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."

2. Zweckbindung „für den konkreten Fall"

Für die Wirksamkeit der datenschutzrechtlichen Einwilligung ist es weiterhin notwendig, dass der Verantwortliche den Betroffenen vor Erteilung der Einwilligung über die beabsichtigten Verarbeitungszwecke („den konkreten Fall") hinreichend informiert, denn der Betroffene kann einer Verarbeitung seiner personenbezogenen Daten nur insoweit rechtswirksam zustimmen, als Klarheit über Zweck und Reichweite seiner Einwilligung besteht; d.h. er muss wissen, worüber er eine Erklärung abgibt. 22

Der Verantwortliche hat den Betroffenen daher umfassend und rechtzeitig über die Verarbeitungszwecke, die mit der Einwilligung verfolgt werden, zu informieren.[45] Allgemein gehaltene Erklärungen, wie „der Betroffene stimmt der Verarbeitung seiner personenbezogenen Daten, welche im Rahmen der Vertragsabwicklung anfallen, zu" oder „der Betroffene ist mit jeder Form der Datenverarbeitung einverstanden", sind keinesfalls ausreichend und müssen wesentlich detaillierter formuliert werden. 23

3. Informierte Einwilligung

Die DSGVO verlangte des Weiteren eine „**informierte Einwilligung**". Die Einwilligungserklärung musste daher so bestimmt sein, dass die Art der personenbezogenen Daten hinreichend genau benannt werden.[46] Erwägungsgrund 32 formuliert: 24

„Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung." 25

Für eine informierte Einwilligungserklärung sind daher nachfolgende Fragen zu beantworten: 26

- Welche Daten werden vom Betroffenen erhoben?
- Für welche Zwecke werden die Daten verarbeitet?
- Kann der Verwendung dazu widersprochen werden?
- Werden die Daten an Dritte weitergegeben?
- Wie erfolgt die Datenverwendung innerhalb einer Unternehmensgruppe?

Der BGH hat sich in seiner sogenannten „Payback-Entscheidung"[47] mit einigen Anforderungen an eine „informierte Einwilligung" befasst und diese konkretisiert. Dabei ging es um eine Klausel folgenden Inhaltes: 27

„Mit meiner Unterschrift erkläre ich mich einverstanden, dass die von mir angegebenen Daten sowie die Rabattdaten (Waren/Dienstleistungen, Preis, Rabattbetrag, Ort und Datum des Vorganges) für an mich gerichtete Werbung (z.B. Information über Sonderangebote, Rabattaktionen) per Post und mittels ggf. von mir beantragter Services (SMS oder E-Mail-Newsletter) so-

45 Erwägungsgrund 42 DSGVO: „Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, **wer** der Verantwortliche ist und für **welche Zwecke** ihre personenbezogenen Daten verarbeitet werden sollen."

46 *Zscherpe*, MMR 2004, 723, 725.

47 BGH, Urt. v. 16.7.2008 – VIII ZR 348/06, MMR 2008, 731 = NJW 2008, 3055.

wie zu Zwecken der Marktforschung ausschließlich von der L-GmbH und den Partnerunternehmen gemäß Nr. 2 der beiliegenden Hinweise zum Datenschutz gespeichert und genutzt werden [. . .]. Hier ankreuzen, falls die Einwilligung nicht erteilt wird."

28 Der BGH sah diese Einwilligungserklärung unter datenschutzrechtlichen Gesichtspunkten als hinreichend an. Die durch Payback gegebenen Informationen über den Nutzungszweck, die Adressdaten der Übermittlung und die Form der beabsichtigten werblichen Ansprache genügten den Anforderungen des BDSG an eine „informierte Einwilligungserklärung" des Betroffenen.

29 In seiner, dem Payback-Urteil nachfolgenden Entscheidung „Happy Digits"[48] bestätigte der Bundesgerichtshof diese Rechtsprechungspraxis. Dabei ging er sogar noch weiter, als er die Klausel

„Einwilligung in Beratung, Information (Werbung) und Marketing. Ich bin damit einverstanden, dass meine bei Happy Digits erworbenen persönlichen Daten (Name, Anschrift, Geburtsdatum) und meine Programmdaten (Anzahl gesammelte Digits und deren Verwendung; und Art der gekauften Waren und Dienstleistungen; freiwillige Angaben) von der C-GmbH [. . .] als Betreiberin des Happy Digits-Programms und ihren Partnerunternehmen zu Marktforschungs- und schriftlichen Beratungs- und Informationszwecken (Werbung) über Produkte und Dienstleistungen der jeweiligen Partnerunternehmen gespeichert, verarbeitet und genutzt werden. Näheres hierzu in der Datenschutzerklärung als Teil der Teilnahmebedingungen, die Sie mit Ihrer Karte erhalten und die auch in allen K-Filialen und bei allen anderen Partnern eingesehen werden können. Sie sind nicht einverstanden, streichen Sie die Klausel. Eine Streichung hat keinen Einfluss auf Ihre Teilnahme am Programm. Ihre Einwilligung können Sie jederzeit gegenüber der C-GmbH widerrufen. Daten von Minderjährigen werden automatisch von der Datennutzung für Werbezwecke ausgeschlossen."

für zulässig erkannte. Die Entscheidung ist mit Blick auf das Erfordernis einer „informierten Einwilligungserklärung" verschiedentlich kritisiert worden.[49] Dem Kunden würden innerhalb der oben genannten Klausel die näheren Umstände der Datenverwendung bei Abgabe der Einwilligung nicht bekannt gegeben, deshalb müsse eine Einwilligung, wie die vorstehend wiedergegebene, an den strengen Voraussetzungen der „informierten Einwilligung" scheitern.[50] Der Umstand, dass eine Kenntnisnahme der Teilnahmebedingungen bei Vertragsschluss nicht möglich war, hätte zur Verwerfung dieser Klausel führen müssen, denn in der Datenschutzerklärung, die Bestandteil der Teilnahmebedingungen war, sollten die genauen Umstände der Datenverwendung dargestellt sein. Da diese dem Adressaten im Moment der Unterschrift – unstreitig – gerade nicht zugänglich waren, sei von einer „informierten Einwilligung" nicht auszugehen.

30 Der BGH hat diese Rechtsauffassung allerdings nicht bestätigt, sondern allgemein davon gesprochen, dass die Klausel inhaltlich den Anforderungen an eine informierte Einwilligung entspreche. Dies mag so zu verstehen sein, dass der Betroffene tatsächlich nicht in jedem Einzelfall über die Empfänger und die Verwendung der Daten zu informieren ist. Im Zweifelsfall sollte jedoch – unter Geltung der DSGVO – von einer derartig schwammigen Formulierung abgesehen werden.

31 Mit aktuellem Urt. v. 14.3.2017 hat der BGH[51] die Anforderungen an die Informiertheit der Einwilligung erneut konkretisiert und dabei explizit auf die in der Datenschutzrichtlinie sowie der Da-

48 BGH, Urt. v. 11.11.2009 – VIII ZR 12/08, NJW 2010, 864.
49 *Nord/Manzel,* NJW 2010, 3756, 3757 m.w.N.
50 *Nord/Manzel*, NJW 2010, 3756, 3757.
51 BGH, Urt. v. 14.3.2017 – VI ZR 721/15, Rn 24, juris.

tenschutzrichtlinie für elektronische Kommunikation[52] verwiesen. Er führt aus, dass eine Einwilligung nur in Kenntnis der Sachlage (und damit informiert) erteilt wird,

> *„wenn der Verbraucher [= der Betroffene] weiß, dass seine Erklärung ein Einverständnis darstellt und worauf sie sich bezieht. Die Einwilligung erfolgt für den konkreten Fall, wenn klar ist, welche Produkte oder Dienstleistungen welcher Unternehmen sie konkret erfasst."*

Genau diese Anforderungen waren nach Auffassung des BGH im zu entscheidenden Fall nicht erfüllt, weil die dort streitbefangene (vorformulierte) Einwilligungserklärung für E-Mail-Werbung weder den Kreis der von der Einwilligung betroffenen Werbetreibenden,[53] noch die zu bewerbenden Produkte und Dienstleistungen konkret benannt hatte. Insoweit stellt der BGH klar, dass allein aus der Nennung von Firmen nicht auf die zur zukünftigen Bewerbung anstehenden Produkte geschlossen werden könne, da sich deren Zusammensetzung und Umfang jederzeit ändern und erweitern kann.

4. Unmissverständlich

Die Einwilligung muss zudem „unmissverständlich" erfolgen. Erwägungsgrund 42 formuliert hierzu: **32**

> *„Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache* ***sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt****."*

II. Formerfordernisse, „eindeutig bestätigende Handlung"

Eine konkrete Formvorgabe für die Einwilligung enthält Art. 4 Nr. 11 DSGVO nicht. Hier ist vielmehr von einer *„Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung"* die Rede. Dies kann etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext **eindeutig** ihr **Einverständnis** mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten **signalisiert**.[54] Klar ist, dass die bislang in verschiedenen europäischen Mitgliedsstaaten[55] für zulässig erachtete **Opt-Out-Erklärung**, auch im Zusammenhang mit der Einwilligung in Werbemaßnahmen,[56] zukünftig **nicht mehr möglich** ist.[57] In den Erwägungsgründen[58] heißt es insoweit eindeutig: **33**

> *„Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen."*

52 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

53 Hier war lediglich von „Sponsoren" die Rede. Unter den Sponsoren befanden sich zudem Marketingunternehmen. Hierzu führt der Senat in Rn 25 des Urteils aus: *„Soweit es sich wie im Streitfall bei den Sponsoren auch um Marketingunternehmen handelt, die selbst für Kunden Werbekampagnen entwerfen und durchführen, wird der Kreis der beworbenen Unternehmen und Produkte gänzlich unübersehbar."*

54 Erwägungsgrund 32 DSGVO.

55 Auch in Deutschland.

56 Diese sind zukünftig jedoch ggf. auch ohne Einwilligung allein auf Grundlage eines berechtigten Interesses des Verantwortlichen im Sinne des Art. 6 Abs. 1 lit. f) DSGVO möglich, hierzu sogleich unter Rdn 166 ff.

57 So auch *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 4 Rn 9.

58 Erwägungsgrund 32 DSGVO.

34 Zulässig sind zukünftig vielmehr allein „eindeutige" Erklärungen des Betroffenen, *„etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen"* kann. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.[59]

35 Möglich ist die Einwilligung auch in Form **„einer mündlichen Erklärung"**.[60] Da der Verantwortliche, soweit die Verarbeitung mit Einwilligung der betroffenen Person erfolgt, **nachweisen** können muss, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat (Art. 7 Abs. 1 DSGVO), dürfte die mündliche Erklärung jedoch in der Praxis mit erheblichen Risiken verbunden sein. Es empfiehlt sich daher, eine mündlich erteilte Einwilligungserklärung (unverzüglich) gegenüber dem Betroffenen zu bestätigen. Vor dem Hintergrund, dass „Stillschweigen" zukünftig eine Willensbekundung nicht ersetzen kann, liefert auch die schriftliche Bestätigung einer mündlich erteilten Einwilligung zwar keine abschließende Sicherheit in Bezug auf das **Nachweisbarkeitserfordernis in Art. 7 Abs. 1 DSGVO.** Wer jedoch nicht ganz auf die Entgegennahme mündlicher Einwilligungserklärungen verzichten will, schafft über eine solche Vorgehensweise jedoch ein gewisses Mindestmaß an Sicherheit. Denkbar wäre natürlich auch die Aufnahme eines „Voice-Files", soweit hierfür seinerseits des Verantwortlichen zuvor die Einwilligung des Betroffenen eingeholt wird.

III. Vorformulierte Erklärungen

36 Unbeschadet des Erfordernisses einer eindeutigen Erklärung des Betroffenen (Opt-in), kann die Einwilligungserklärung durch den Verantwortlichen auch vorformuliert werden. In diesem Fall muss die vorformulierte Einwilligungserklärung „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten."[61] Sie darf – dies ergibt sich unmittelbar aus Art. 7 Abs. 2 DSGVO – auch mit anderen Erklärungen des Betroffenen verbunden sein.

37 Die Einwilligungserklärung ist dann jedoch abgesetzt von den anderen Erklärungen an deutlich sichtbarer Stelle aufzunehmen. Sie darf nicht an versteckter Stelle mitten in einem vorformulierten Text untergebracht werden. In der Praxis kann der Hervorhebungspflicht dadurch genügt werden, dass die datenschutzrechtliche Einwilligungsklausel fett gedruckt und entsprechend überschrieben („Datenschutzrechtliche Einwilligungsklausel") vom übrigen Text abgesetzt wird. Des Weiteren empfiehlt es sich, die datenschutzrechtliche Einwilligung – soll sie mit anderen Erklärungen zusammen abgegeben werden – auch optisch vom sonstigen Text abzuheben. Dies kann z.B. durch Sperrschrift, Unterstreichung, Einrahmung, Verwendung anderer Schrifttypen, durch Trennlinien oder ähnliches geschehen.[62] Ebenso sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.[63]

38 Vorformulierte Einwilligungserklärungen unterfallen zudem der Klauselkontrolle der §§ 305 bis 310 BGB. Handelt es sich bei dem Betroffenen um einen Verbraucher i.S.d. § 13 BGB, finden die Vorschriften über die AGB-Kontrolle zudem auch Anwendung, wenn die Erklärung nur für den

59 Erwägungsgrund 32 DSGVO.
60 Erwägungsgrund 32 DSGVO.
61 Erwägungsgrund 42 DSGVO.
62 So z.B. BGH, Urt. v. 27.4.1994 – VIII ZR 223/93, NJW 1994, 1800, 1801; OLG Köln, Urt. v. 11.1.2002 – 6 U 125/01, RDV 2002, 237, 238.
63 Erwägungsgrund 42 DSGVO.

Einzelfall vorformuliert wurde (§ 310 Abs. 3 Nr. 1 BGB). Die Anwendung der Grundsätze über die AGB-Kontrolle führt dazu, dass gemäß § 305c Abs. 2 BGB die Einwilligungserklärung stets so auszulegen ist, wie sie den Betroffenen am wenigsten belastet. Dies bedeutet, dass der Einwilligungserklärung ein möglichst geringer Anwendungsbereich gegeben wird.[64] Maßstab für die Beurteilung von Einwilligungsklauseln in AGB ist in erster Linie § 307 Abs. 1 BGB und damit die Frage, ob die vorformulierte Einwilligungsklausel den Betroffenen entgegen dem Gebot von Treu und Glauben unangemessen benachteiligt. Pauschale Einwilligungserklärungen sind vor dem Hintergrund des in § 307 Abs. 1 Satz 2, Abs. 3 Satz 2 BGB vorgeschriebenen Transparenzerfordernisses zu vermeiden.[65] Einwilligungsklauseln in vorformulierten Erklärungen unterliegen zudem der engen Auslegungskontrolle gemäß § 305c Abs. 2 BGB, sodass Zweifel bei der Auslegung stets zu Lasten des Verwenders gehen und mehrdeutige Klauseln, die eine unzulässige Auslegungsvariante beinhalten, unwirksam sind. Sie verstoßen dann ebenfalls gegen den Aspekt der „Unmissverständlichkeit". Ebenso führen widersprüchliche Angaben zum Zweck der Verarbeitung zur Unwirksamkeit.

IV. Einwilligungsfähigkeit von Kindern, Art. 8 DSGVO

39 Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da sie sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Einen solchen besonderen Schutz normiert Art. 8 DSGVO, soweit es um die Einwilligungserteilung im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft geht. Die hier normierten besonderen Anforderungen treten neben die allgemeinen Anforderungen an die Einwilligungserteilung in Art. 4 Nr. 11 DSGVO und Art. 7 DSGVO.[66]

1. Dienste der Informationsgesellschaft

40 Was unter „Diensten der Informationsgesellschaft" zu verstehen ist, definiert Art. 4 Nr. 25 DSGVO, der insoweit auf eine Dienstleistung im Sinne des Art. 1 Nr. 1 lit. b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9.9.2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft[67] verweist. Hiernach ist ein „Dienst"

> *„eine Dienstleistung der Informationsgesellschaft, d.h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.*

Im Sinne dieser Definition bezeichnet der Ausdruck

- „im Fernabsatz erbrachte Dienstleistung" eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;
- „elektronisch erbrachte Dienstleistung" eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht,

64 *Däubler,* in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG, 3. Aufl. 2010, § 4a Rn 31.

65 OLG Hamburg, Urt. v. 4.3.2009 – 5 U 160/08, K&R 2009, 414, 416; AG Hagen, Urt. v. 11.11.2004 – 10 C 275/04, zit. nach juris.

66 *Frenzel*, in: Paal/Pauly, Datenschutz-Grundverordnung, 2017, Art. 8, Rn 1; *Feiler/Forgó*, EU-DSGVO, 2017, Art. 8 Rn 1; *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 8 Rn 1; *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl. 2017, Art. 8 DSGVO, Rn 1; *Schulz*, in: Gola (Hrsg.), DS-GVO, 2017, Art. 8 Rn 3.

67 ABl L 241 v. 17.9.2015, S. 1.

über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;

- „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird."[68]

41 Die Einschränkung des Schutzes von Kindern auf Einwilligungen, die im Zusammenhang mit Diensten der Informationsgesellschaft erbracht werden, führt dazu, dass ein wesentlicher Teil, der speziell an Kinder gerichteten Angebote hinsichtlich der Wirksamkeit der Einwilligung „nur" an Art. 7 DSGVO und den allgemeinen Einwilligungserfordernissen des Art. 4 Nr. 11 DSGVO zu messen ist.[69] So sind beispielsweise Fernsehdienste und Hörfunkdienste ebenso ausgenommen, wie der klassische Vor-Ort-Verkauf.[70]

2. Einwilligung bei Diensten der Informationsgesellschaft

42 Ein Kind ist eine Person unter 18 Jahren, sofern sie das gesetzliche Erwachsenenalter nicht bereits vor diesem Alter erreicht.[71] Soweit eine Einwilligung in die Verarbeitung im Zusammenhang mit einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, eingeholt werden soll, so ist die durch das Kind erteilte Einwilligung nur rechtmäßig, wenn das Kind das **sechzehnte Lebensjahr** vollendet hat oder die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird (Art. 8 Abs. 1 DSGVO).

a) Mindestens 13, höchstens 16 Jahre

43 In Bezug auf die in Art. 8 Abs. 1 DSGVO normierte Altersgrenze für die Einwilligungsfähigkeit von Minderjährigen verbleibt den Mitgliedstaaten gem. Art. 8 Abs. 1 S. 3 DSGVO insoweit nationalstaatlicher Handlungsspielraum, als dass die Altersgrenze bis auf das vollendete 13. Lebensjahr herabgesetzt werden kann. Eine Erhöhung des Höchstalters von 16 Jahren ist nicht möglich, so dass die Altersgrenze für die Einwilligung von Kindern im Zusammenhang mit der Erbringung von Diensten der Informationsgesellschaft zukünftig europaweit zwischen 13 und 16 Jahren liegen wird. Der Bundesgesetzgeber hat von der Möglichkeit der Herabsetzung der Atlersgrenze im Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)[72] keinen Gebrauch gemacht. Eine Herabsetzung hätte auch nicht der bisherigen Datenschutztradition innerhalb der Bundesrepublik entsprochen, die z.T. sogar darauf abzielt, Minderjährigen generell die Einwilligungsfähigkeit abzusprechen.[73]

Über die Befugnis zur Herabsetzung der Altersgrenze hinaus räumt die Verordnung den Mitgliedstaaten keinerlei Änderungs- und leider auch keinerlei Konkretisierungsbefugnisse ein.[74]

68 In Anhang I der Richtlinie (EU) 2015/1535 findet sich eine Beispielliste der nicht unter diese Definition fallenden Dienste („Negativkatalog").

69 Vgl. *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 8 Rn 13 ff.

70 Die außerhalb der Dienste der Informationsgesellschaft an die Einwilligung von Kindern gestellten Anforderungen werden unter Rdn 210 behandelt.

71 Artikel 1 des Übereinkommens der Vereinten Nationen über die Rechte des Kindes, 20.11.1989.

72 BT-Drucks 18/11325 v. 24.2.2017, in der Fassung der vom Bundestag beschlossenen Beschlussempfehlung des Innenausschusses, BT-Drucks 18/12084 v. 25.4.2017, hierzu auch Plenarprotokoll BT-PlPr 18/231, S. 23306D. Die Verabschiedung durch den Bundesrat stand zum Zeitpunkt der Manuskripterstellung dieses Werkes noch aus.

73 Hierzu und zu dem damit ggf. verbunden verfassungsrechtlichen Problemen, *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 8 Rn 30.

74 Hierzu: Minutes of the fourth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 vom 2.12.2016, S. 3, abrufbar unter: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=30923&no=2 (nur in englischer Sprache).

§ 7 Sicherungsmechanismen zur Einhaltung der DSGVO

A. Vorbemerkungen

Datenschutz ist ohne **Datensicherheit** nicht vorstellbar. Letztere ist nicht primär ein juristischer Themenkomplex, sondern vornehmlich technischer Natur. Dies auch deshalb, weil die Datenverarbeitungen immer komplexer werden und die Komplexität der Datenverarbeitung durch ebenso immer komplexer werdende technische (Soft- und Hardware-)Systeme Unterstützung finden bzw. in vielen Fällen auch überhaupt erst umsetzbar wird. Selbst die juristische Tätigkeit ist auf dem Weg sich maßgeblich zu verändern. LegalTech ist kein Randthema mehr, sondern war aktuell der bestimmende Gegenstand des 68. Deutschen Anwaltstags in Essen.[1] Auch in der Finanzbranche, beispielsweise im Bereich der Inkassodienstleistungen, mehrt sich der Einsatz von Technologien und FinTech-Unternehmen drängen zuhauf auf den deutschen und europäischen Markt. 1

Die DSGVO trägt der zunehmenden **Technisierung** an verschiedenen Stellen Rechnung. So wird der „Stand der Technik" zu einem maßgeblichen Faktor in der Umsetzung von Schutzmaßnahmen, die Themenbereiche „**data privacy by design**" und „**data privacy by default**" sind ebenso maßgeblich auf (technische) Sicherungsmechanismen und -Maßnahmen zur Absicherung der datenschutzrechtlichen Vorgaben gerichtet. Zukünftig wird die datenschutzrechtliche Beratung zunehmend nicht mehr allein von Juristen vollzogen werden können, sondern die **Einbindung technischen Sachverstandes wird erforderlich**.[2] Dies beschränkt sich, blickt man bspw. auf Art. 32 Abs. 1 lit. c) DSGVO, der zur Sicherheit der Verarbeitung neben der Vertraulichkeit, auch die Integrität, Verfügbarkeit und Belastbarkeit der Systeme adressiert, nicht allein auf den IT-technischen Sachverstand. So kann ein plötzlicher Stromausfall Schäden an Datenbanken auslösen, ein Blitzschlag kann vollständige Unternehmensnetzwerke zerstören, aber auch Feuer oder Wasser können unmittelbaren Einfluss auf die Verfügbarkeit und die Integrität eingesetzter Systeme haben. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Rahmen der Datenverarbeitung kann auch die **Hinzuziehung von Brandschutzexperten, Elektrikern**, die für eine elektrische Absicherung der Systeme Sorge tragen oder auch Klimatechnikern,[3] erforderlich werden. Datenschutz(recht) ist damit zukünftig weit mehr als IT-Technische **Datensicherheit**. 2

Der Darstellung des umfangreichen Systems der innerhalb der DSGVO normierten Schutzmechanismen und -maßnahmen dient dieser Abschnitt. 3

B. Grundsätzliches

Nach Art. 24 Abs. 1 DSGVO ist der Verantwortliche verpflichtet, sicherzustellen und nachzuweisen, dass die von ihm vollzogenen Verarbeitungen unter Einhaltung der DSGVO erfolgen. Hierzu hat er unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die 4

1 Https://anwaltsblatt.anwaltverein.de/de/news/deutscher-anwaltstag-legal-tech-ist-chance-fuer-kleinere-kanzleien.

2 Dies berücksichtigt z.B. das EuroPriSe-Siegel bereits seit Anbeginn und fordert neben einem rechtlichen auch stets ein technisches Zertifizierungsgutachten. Der Autor dieses Werkes hat in laufenden Projekten zur Umsetzung bestehender Datenverarbeitungsprozesse im Zusammenhang mit der DSGVO selbst bereits vielfach mit technischen Datenschutzexperten zusammengearbeitet und damit gute Erfahrungen gemacht.

3 Soweit es um die hinreichende Klimatisierung von IT-Anlagen geht.

Rechte und Freiheiten natürlicher Personen[4] geeignete technische und organisatorische Maßnahmen und – dort wo dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht – „**geeignete Datenschutzvorkehrungen**" (Art. 24 Abs. 2 DSGVO) zu etablieren.

5 Art. 24 DSGVO konkretisiert zum einen die in Art. 5 Abs. 2 DSGVO normierte Rechenschaftspflicht[5] des Verantwortlichen und beschreibt zugleich die an ihn[6] gerichteten Anforderungen. Die DSGVO setzt dabei auf einen **risikoorientierten Ansatz** und nimmt den Verantwortlichen in die Pflicht, über „geeignete technische und organisatorische Maßnahmen" die rechtmäßige Verarbeitung personenbezogener Daten sicherzustellen. Dies ist grundsätzlich nicht neu: Schon die Datenschutzrichtlinie forderte derartige Maßnahmen und

> *„zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern".*[7]

Nach Art. 17 Abs. 1 Datenschutzrichtlinie waren hierfür Maßnahmen zu etablieren, die unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Art. 24 DSGVO normiert leicht modifiziert und detaillierter, dass die Maßnahmen nach Art, Umfang, Umständen und den Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignet sein müssen. Diese Formulierung findet sich in ähnlicher Form auch in Art. 25 DSGVO sowie in Art. 32 DSGVO.

6 Eine nähere Definition der Kriterien Art, Umfang, Umstände und Zwecke der Verarbeitung findet sich in der Verordnung selbst nicht. Die Erwägungsgründe beschreiben besondere Verarbeitungssituationen, in denen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person bestehen kann. So soll sich aus der **Verarbeitung besonderer Kategorien personenbezogener Daten**, wie Informationen über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Zugehörigkeit zu einer Gewerkschaft oder der Verarbeitung von genetischen Daten, Gesundheitsdaten oder Daten über das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln ein grundsätzliches Risiko für die Rechte und Freiheiten von natürlichen Personen ergeben. Dies gilt ebenso, „wenn persönliche Aspekte **bewertet** werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen". Weiterhin soll auch die **Lebenssituation der betroffenen Person** eine Rolle spielen, z.B., wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden. Auch können die Verarbeitung einer großen **Menge** personenbezogener Daten und/oder eine große **Anzahl** von betroffenen Personen ein Risiko bedeuten.

4 Die Verordnung spricht insoweit nicht allein von den Rechten und Freiheiten der betroffenen Person, sondern von den Rechten und Freiheiten „natürlicher Personen" und zieht den Kreis der zu schützenden damit wesentlich weiter.

5 In Art. 24 Abs. 1 S. 1 DSGVO heißt es „[...] um den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.", zur Rechenschaftspflicht auch Rdn 171 ff.

6 Auftragsverarbeiter sind von Art. 24 DSGVO nicht umfasst.

7 Erwägungsgrund 46 der Datenschutzrichtlinie.

Hieraus lässt sich für die **inhaltliche Bestimmung der in die Risikobewertung** einzustellenden Kriterien nahfolgendes ableiten: 7

(1) Die **Art der Verarbeitung** beschreibt zum einen die in Art. 4 Nr. 2 DSGVO beschriebenen „**Verarbeitungsstadien**“,[8] aus denen sich unterschiedliche Risiken für die betroffene Person ergeben können. So kann eine Pseudonymisierung oder Anonymisierung personenbezogener Daten die mit ihrer Verarbeitung verbundenen Risiken für die betroffene Person erheblich reduzieren oder gänzlich ausschließen, während eine „Offenlegung durch Übermittlung“ den Kreis der mit der Verarbeitung erfassten Daten auf Dritte erstreckt, was für die betroffene Person mit einem hohen Risiko verbunden sein kann, weil die personenbezogene Daten den Einflussbereich des Verantwortlich verlassen. Weiterhin ist hiermit auch die **Durchführung der Verarbeitung** beschrieben (nicht automatisiert, automatisiert, automatische Entscheidungsfindung).

(2) Der **Umfang der Verarbeitung** beschreibt ein quantitatives Kriterium und bezieht sowohl die Anzahl der betroffenen personenbezogenen Daten, als auch die Anzahl der von einer Verarbeitung betroffenen natürlichen Personen mit ein.

(3) Die **Umstände der Verarbeitung** beschreiben die konkrete Verarbeitungssituation, ihr Umfeld und die für die Verarbeitung eingesetzten Mittel (bspw. Verarbeitung innerhalb eines Arbeitsverhältnisses, Verarbeitung durch mehrere (gemeinsam) Verantwortliche, Ort der Verarbeitung, eingesetzte technische Hilfsmittel).[9] Dabei sind auch die Lebenssituation der betroffenen Person(en) und die Schutzbedarfskategorien[10] der von der Verarbeitung betroffenen Daten zu berücksichtigen.

(4) Die **Zwecke der Verarbeitung** beschreiben die Erhebungs- oder Weiterverarbeitungszwecke,[11] wie sie vom Verantwortlichen festgelegt wurden. Auch die Interessen, die vom Verantwortlichen verfolgt werden, können Beachtung finden.

Die vorgenannten Kriterien sind zur Ermittlung der Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person heranzuziehen,[12] wobei das Risiko anhand einer objektiven Betrachtung zu bewerten ist, bei der festgestellt wird, ob die Datenverarbeitung „nur“ ein Risiko oder ein „hohes“ Risiko birgt.[13] 8

Die **Risiken** für die Rechte und Freiheiten natürlicher Personen können sich in einem physischen, materiellen oder immateriellen **Schaden** der betroffenen Person äußern. Die Erwägungsgründe[14] nennen beispielhaft: 9

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanzieller Verlust,
- Rufschädigung,

8 Hierzu oben Rdn 98 ff.; die DSGVO sieht zwar anders als das bisherige BDSG keine phasenweise Betrachtung vor, beschreibt aber in Art. 4 Nr. 2 DSGVO gleichwohl verschieden Verarbeitungsstadien, um dem Verarbeitungsbegriff eine bessere Kontur zu geben.

9 *Hartung*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 24 Rn 14; *Martini*, in: Paal/Pauly (Hrsg.). Datenschutz-Grundverordnung, 2017. Art. 24 Rn 32; *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl. 2017, Art. 24 DSGVO Rn 6.

10 Ausführlich hierzu oben § 4 Rdn 217 ff.; siehe auch https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf.

11 Hierzu Rdn 140 ff.

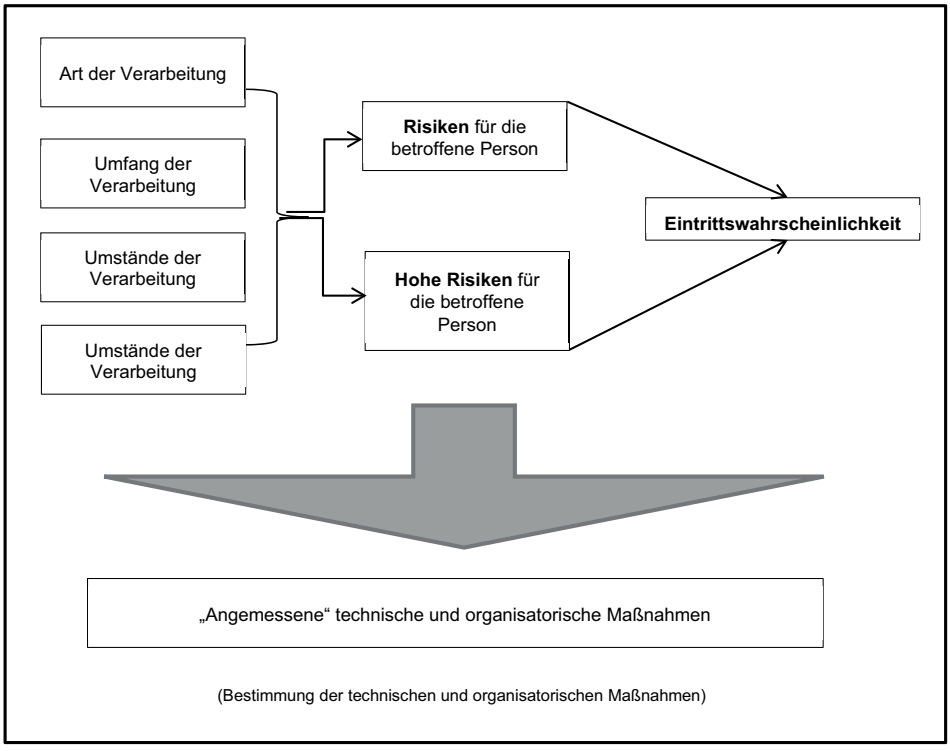
12 Erwägungsgrund 76 S. 1 DSGVO.

13 Erwägungsgrund 76 S. 2 DSGVO.

14 Erwägungsgrund 78 DSGVO.

- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- unbefugte Aufhebung der Pseudonymisierung oder
- andere erhebliche wirtschaftliche oder
- gesellschaftliche Nachteile oder
- sonstige physische, materielle oder immaterielle Schäden beim Betroffenen.

10 Die ermittelten Risiken sind wiederum für die Bestimmung der vom Verantwortlichen zu etablierenden technischen und organisatorischen (Schutz-)Maßnahmen ausschlaggebend. Diese werden vom Verantwortlichen grundsätzlich (nur) insoweit eingefordert, als sich ihre Etablierung als dem Risiko angemessen (= verhältnismäßig) darstellt.



11 Welche technischen und organisatorischen Maßnahmen im Einzelnen in Betracht kommen, legt Art. 24 DSGVO – mit Ausnahme der Maßnahme der „Anwendung geeigneter Datenschutzvorkehrungen“ – nicht fest; zum Teil werden sie in Art. 25, Art. 28 Abs. 1 und Art. 32 DSGVO umschrieben. Ein der Anlage zu § 9 Satz 1 BDSG vergleichbarer Maßnahmenkatalog existiert nicht. Die hier beschriebenen Maßnahmen

- der Zutrittskontrolle,
- der Zugangskontrolle,
- der Zugriffskontrolle,
- der Weitergabekontrolle,
- der Eingabekontrolle, der Auftragskontrolle,
- der Verfügbarkeitskontrolle,
- des Gebotes der getrennten Verarbeitung sowie

- des Einsatzes von Verschlüsselungsverfahren,

können aber weiterhin Anhaltspunkte für die in Betracht kommenden technischen und organisatorischen Maßnahmen liefern.[15]

12 Nach Art. 24 Abs. 3 DSGVO können entsprechende Maßnahmen auch in genehmigten Verhaltensregeln gemäß Art. 40 DSGVO normiert sein. Soweit Art. 24 Abs. 2 DSGVO von der „**Anwendung geeigneter Datenschutzvorkehrungen**" als mögliche technische und organisatorische Maßnahme spricht, sind hiermit – wie ein Blick in die englische Sprachfassung[16] zeigt – interne, wie externe **Unternehmensrichtlinien**[17] in Bezug auf die Einhaltung der Vorgaben der DSGVO angesprochen. Eine 100 %tige Sicherheit fordert die DSGVO nicht; sie wird sich unter Berücksichtigung des Stands der Technik ohnehin kaum realisieren sein. Zudem ist nur von „angemessenen" Maßnahmen die Rede und nicht von solchen, die ein Risiko gänzlich ausschließen.

13 Der Nachweis angemessener Maßnahmen im Einzelfall erfordert eine entsprechende Dokumentation der technischen und organisatorischen Maßnahmen durch den Verantwortlichen. Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder das erfolgreiche Durchlaufen eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO können zusätzliche Anhaltspunkte für die Etablierung geeigneter und angemessener technischer und organisatorischer Maßnahmen bilden.

C. Umsetzung technischer und organisatorischer Maßnahmen, Art. 32 DSGVO

14 Die grundlegende Verpflichtung zum Schutz personenbezogener Daten im Rahmen der Verarbeitung konkretisiert Art. 32 DSGVO, der besondere Anforderungen an die Sicherheit der Verarbeitung stellt. Hiernach sind vom Verantwortlichen und etwaigen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen Auftragsverarbeitern geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

15 - Die Kriterien der der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung entsprechen den in Art. 24 DSGVO aufgeführten. Zum Stand der Technik[18] kann ebenso wie zu den berücksichtigungsfähigen Implementierungskosten[19] auf die Ausführungen zu § 22 Abs. 2 BDSG-Neu verwiesen werden. Die geforderte Abwägung vollzieht sich im Wesentlichen wie im Rahmen von Art. 24 DSGVO beschrieben (siehe Rdn 5 ff.). Dabei hat der Verantwortliche **keine absolute Sicherheit**, sondern lediglich ein den festgestellten Risiken **angemessenes Schutzniveau** sicherzustellen. Zu verhindern ist insbesondere, dass personenbezogene Daten unbeabsichtigt und/oder unrechtmäßig
- vernichtet,
- verändert oder
- unbefugt offengelegt werden oder
- auf sonstige Weise verloren gehen bzw.

15 In diesem Sinne auch *Grages*, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl. 2017, Art. 32 DSGVO Rn 4.
16 Hier wird von von „implementation of appropriate **data protection policies** by the controller" gesprochen.
17 *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl. 2017, Art. 24 DSGVO Rn 11.
18 § 4 Rdn 326.
19 § 4 Rdn 327.

- Dritte unbefugt Zugang zu verarbeiteten personenbezogenen Daten erhalten (Art. 32 Abs. 2 DSGVO).

Anders als Art. 24 DSGVO normiert Art. 32 Abs. 1 DSGVO einen nicht abschließenden[20] Beispielkatalog[21] von Maßnahmen, die im Einzelfall als geeignet angesehen werden können.

I. Pseudonymisierung

16 Eine in der Regel über technische Maßnahmen im Rahmen der automatisierten Verarbeitung umsetzbare Schutzmaßnahme kann in der Pseudonymisierung[22] der zu verarbeitenden Daten liegen. Diese kommt überall dort in Betracht, wo der Verantwortliche zur Erreichung der mit der Verarbeitung verfolgten Zwecke und Ziele nicht zwingend auf die Kenntnis der betroffenen Person angewiesen ist. Deutlich wird dies anhand nachfolgender Praxisbeispiele:

1. Medizinische Forschung und Diagnostik

17 Ein Anwendungsbereich, in dem Pseudonymisierung angezeigt sein kann, ist in der medizinischen Forschung und Diagnostik zu sehen.

18 Die **medizinische Forschung**[23] ist überall dort, wo sie sich auf evidenzbasierte Daten stützt, auf die Verarbeitung von Gesundheitsdaten von Probanden angewiesen. Im Bereich der behördlichen Arzneimittelzulassung ist die klinische Erprobung zwingende Zulassungsvoraussetzung.[24] Für die Durchführung der Forschung sind jedoch in der Regel Informationen, die einen bestimmten Probanden als solchen identifizieren, wie sein Vor- und Nachname oder seine Adressdaten, nicht erforderlich. Mit Blick auf eine langzeitige Risikobetrachtung – und zum Schutz der Probanden – dürfte in den meisten Fällen gleichwohl eine anonyme Teilnahme an medizinischen Forschungsprojekten ausscheiden. Man denke nur daran, dass erst Monate oder gar Jahre nach der Durchführung einer Forschungsmaßnahme Nebenwirkungen bekannt werden, die ein Einschreiten erfordern. Wäre der Proband in einem solchen Fall auch für den Forschungsträger anonym, würden Hilfemaßnahmen nur schwer, ggf. sogar überhaupt nicht umgesetzt werden können. Der mit einer Forschungsmaßnahme **verfolgte Zweck der Verarbeitung**, z.B. die Ermöglichung der klinischen Arzneimittelzulassung, die Überprüfung der Wirksamkeit neuer Behandlungsmethoden oder die Forschung zu bestimmten Erkrankungen, erfordert keine Identifizierung des Probanden. Die Anzahl der im Rahmen der medizinischen Forschung verarbeiteten Daten ist – je nach Forschungsziel – in der Regel hoch; da die Qualität von medizinischen Studien zudem maßgeblich von einer möglichst hohen Fallzahl[25] abhängig ist.[26] Regelmäßig ist auch eine große Zahl von natürlichen Personen von der Verarbeitung betroffen (Umfang der Verarbeitung). Die Verarbeitung erfolgt ausnahmslos automatisiert, mit Blick auf den Forschungszweck zudem mit dem Ziel, Vergleichbarkeit zwischen den betroffenen Personen herzustellen und diese auch aktiv zu vergleichen. Zudem sind mit Gesund-

20 „unter anderem".

21 Vgl. *Jandt*, in: *Buchner/Kühling*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 32 Rn 14, der die Qualifikation als „Beispielmaßnahmen" aus der Formulierung „unter anderem" ableiteten will. Deutlicher wird dies in der englischen Sprachfassung, die den Katalog der in Art. 32 Abs. 1 lit. a) bis d) beschriebenen Maßnahmen mit den Worten „including inter alia *as appropriate*" einleitet.

22 Zum Begriff Rdn 117 ff.

23 Ausführlich hierzu auch Stabsstelle Datenschutz der Universität Düsseldorf, Orientierungshilfe: Pseudonymisierung in der medizinischen Forschung, abrufbar unter: http://www.uni-duesseldorf.de/home/fileadmin/redaktion/ZUV/Stabsstelle_Datenschutz/Orient-hilfe_DS_Pseud-med-Forsch.pdf.

24 Vgl. § 22 Abs. 2 AMG.

25 Benötigte Zahl der Beobachtungseinheiten, wie zum Beispiel Patienten bzw. Probanden.

26 Hierzu *Röhrig/du Prel/Blettner*, Deutsches Ärzteblatt 2009, 184, 187.

heitsdaten besondere Kategorien personenbezogener Daten mit einem hohen Schutzbedarf von der Verarbeitung betroffen und in aller Regel auch innerhalb des Verantwortlichen zahlreiche Personen mit der Verarbeitung betraut. In zunehmendem Maße werden für zudem Blut- oder Gewebeproben benötigt und damit ggf. auch genetische Daten verarbeitet. Die Forschungsergebnisse werden regelmäßig Dritten gegenüber bekannt gegeben. Oftmals wird den Forschern auch online Zugriff auf die erhobenen Daten gewährt (Umstände der Verarbeitung). Art, Umfang, Umstände und Zwecke der Verarbeitung bedingen insoweit nicht unerhebliche Risiken für die betroffene Person, allen voran der Verlust der Vertraulichkeit von, dem Berufsgeheimnis unterliegenden personenbezogenen Daten (§ 203 StGB). Maßnahmen der Pseudonymisierung können dem entgegenwirken und sind daher grundsätzlich als „erforderliche" technische Schutzmaßnahmen zu etablieren. Soweit im Rahmen der Forschung nicht nur auf selbst erhobene Daten zurückgegriffen wird, sondern, wie in jüngster Zeit vermehrt festzustellen Forschungskooperationen gebildet werden, die deutschland- und z.T. auch europa- oder weltweit agieren, führt dies dazu, dass die personenbezogenen Daten die eigentliche Forschungseinrichtung verlassen, was zusätzliche Sicherungsmaßnahmen, wie etwa die Etablierung von Verschlüsselungstechniken erforderlich macht.

Patientendaten finden zunehmend auch in der **medizinischen Diagnostik** Verwendung, etwa, wenn es um Screening-Maßnahmen geht. Hier hat sich in den vergangenen Jahren eine Vielzahl von Anbietern am Markt etabliert, die Software anbieten, die bei der Erkennung bestimmter Krankheiten oder Krankheitsrisiken unterstützt.[27] 19

2. Videoüberwachung

Soweit – in sicherheitsrelevanten Bereichen – die Einführung von Videoüberwachungstechniken grundsätzlich als rechtmäßig betrachtet werden kann,[28] stellt sich die Frage, ob derartige Daten unter Berücksichtigung des mit einer Videoüberwachung verbundenen Eingriffs in das allgemeine Persönlichkeitsrecht der betroffenen Personen zur Zweckverfolgung zwingend „klar" angezeigt werden müssen. Auch hier sind zahlreiche Softwarelösungen am Markt,[29] die eine Pseudonymisierung und sogar die vollständige Anonymisierung ermöglichen, indem gefilmte Personen „maskiert und verschleiert" dargestellt werden. Je nach gewählter Verschleierungsmethode sind lediglich verpixelte Bewegungen wahrnehmbar. Nicht verpixelte Bilder werden in einem getrennten zugriffsgeschützten System aufgezeichnet und nur dann verarbeitet, wenn dies z.B. zur Aufdeckung einer Straftat erforderlich ist. 20

In diesem Zusammenhang ist auch auf die Neuregelung in § 4 BDSG-Neu hinzuweisen, die Regelungen zur Videoüberwachung öffentlich zugänglicher Räume enthält und insoweit eine, § 6b BDSG weitgehend entsprechende Regelung enthält. Soweit Videoüberwachungsanlagen in öffentlichen Räumen eingesetzt werden sollen, soll der Einsatz nach dem Willen des deutschen Gesetzgebers auch zukünftig nur zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig sein. Eine Einschränkung der datenschutzrechtlichen Vorgaben der DSGVO kann damit nicht verbunden sein, nachdem die DSGVO für eine der- 21

27 Vgl. z.B. die Screening-Software SRAdoc, die eine Verifizierung und Dokumentation des Vorhofflimmerns über eine automatische softwaregestützte Analyse von Langzeit-EKG vollzieht. Hierfür wird auf „historische" Behandlungsdaten und Ergebnisse zurückgegriffen; siehe auch die Software der Mint Medical aus Heidelberg (https://mint-medical.com/de/) die radiologische Befunddaten zur Erleichterung des onkologischen Staging genutzt und ausgewertet werden. In solchen Projekten ist die Kenntnis der hinter einem Datum stehenden Person grundsätzlich nicht erforderlich.

28 So auch *Lachenmann*, ZD 2017, 407, 409 f.

29 Vgl. die von EuroPriSe zertifizierten Systeme KiwiVision Privacy Protector (https://www.european-privacy-seal.eu/EPS-en/KiwiVision-Privacy-Protector) und die Videomanagement-Lösung vimacc (https://www.european-privacy-seal.eu/eps-en/accellence-vimacc).

artige Einschränkung keine Öffnungsklausel bereithält.[30] Die Norm kann in diesem Sinne allenfalls als Regelbeispiel verstanden werden.

3. Test-, Demo- oder Trainingssysteme

22 Pseudonymisierung ist zudem grundsätzlich dort erforderlich, wo es um Test-, Demo- oder Trainingszwecke geht. Hier kommen allzu oft Produktivdaten zum Einsatz, insbesondere im Zusammenhang mit Funktions- und Leistungstests nicht-produktiver IT-Systeme.[31] Gerade diese sind oft nicht hinreichend gegen unberechtigte Datenzugriffe gesichert; die Integrität der Systeme ist in der Regel nicht überprüft. Dies birgt das erhöhte Risiko des Datenverlustes mit daraus resultierenden Schäden für die betroffenen Personen. Eine Verschlüsselung der Daten ist in der Regel nicht möglich, auch die „Generierung" von fiktiven Daten ist oft aufgrund der Komplexität von Systemen mit unverhältnismäßigem Aufwand und einer hohen Fehleranfälligkeit verbunden. Hier kann über das sog. **Data Masking**[32] eine Pseudonymisierung durchgeführt und die „Echtdaten" so verfremdet werden, dass sie lesbar bleiben und ihren Kontext und ihre Informationsstruktur möglichst weitgehend behalten, aber gleichsam die Rechte und Freiheiten der betroffenen natürlichen Personen geschützt werden.

4. Umsetzungsmöglichkeiten für Pseudonymisierung

23 Einen guten Überblick über die verschiedenen Möglichkeiten der Umsetzung von Pseudonymisierungen in der Praxis liefert das Arbeitspapier „Datenschutzfreundliche Technologien" des bayerischen Landesbeauftragten für den Datenschutz.[33] Demnächst erscheint das aktuelle Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz, das Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen im Unternehmensumfeld enthalten wird.[34] Zu den Umsetzungsmöglichkeiten in der Werbebranche kann auch der Beitrag „Pseudonymisierung, Hashing: Das neue Bewusstsein für Datenschutz im Online-Werbemarkt" von *Antrup*[35] empfohlen werden, der insbesondere die Methoden des sog. Hashing und des sog. Scrambling anschaulich darstellt und beschreibt.

II. Verschlüsselung

24 Als weitere mögliche technische Maßnahme mit der die Sicherheit der Verarbeitung erhöht werden kann, nennt Art. 32 Abs. 1 lit. a) DSGVO den Einsatz von Verschlüsselungstechniken. Dort, wo eine Verletzung des Schutzes personenbezogener Daten zu einem Zugriff durch unberechtigte Dritte führt kann, die Daten aber vom Dritten nicht oder nur unter unverhältnismäßigem Aufwand ausgewertet oder sichtbar gemacht werden können, ist die Sicherheit der Verarbeitung gewährleistet.

30 Hierauf weist auch *Lachenmann*, ZD 2017, 407, 410, hin, der die Regelung in § 4 BDSG-Neu zu Recht als europarechtswidrig einstuft.

31 Ausführlich hierzu bspw. *Lang*, Anonymisierung/Pseudonymisierung von Daten für den Test, abrufbar unter: https://omen.cs.uni-magdeburg.de/alang/paper/lang-anonymisierung-dach2012.pdf.

32 Https://de.wikipedia.org/wiki/Data_Masking; siehe auch http://www.it-zoom.de/it-director/e/vorgaben-der-eu-datenschutz-grundverordnung-14408/; *Lee/Breslaw*, Anforderungen der Datenschutzgrundverordnung für Data Masking, abrufbar unter: https://www.all-about-security.de/fileadmin/micropages/Whitepaper_Security_Management/Delphix_WP_DSGVO.pdf; siehe auch https://docs.microsoft.com/de-de/azure/sql-database/sql-database-dynamic-data-masking-get-started.

33 Https://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm#nr12.

34 Hierzu https://www.rdv-online.com/aktuelles/fokusgruppe-datenschutz-erarbeitet-whitepaper-zur-pseudonymisierung.

35 Abrufbar unter: http://www.absatzwirtschaft.de/anonymisierung-pseudonymisierung-hashing-das-neue-bewusstsein-fuer-datenschutz-im-online-werbemarkt-90685/.

Dabei muss es sich um eine nach dem Stand der Technik sichere **Verschlüsselung** handeln.[36] Der DES -Algorithmus sollte daher ebenso wenig Verwendung finden wie WEP- und WPA-Verschlüsselungen, die nach *Lenhard*[37] *„selbst von Laien mit einer Anleitung aus dem Internet in wenigen Minuten überwunden werden“* können. Neben dem Einsatz von Verschlüsselungstechniken wäre auch der Einsatz bestimmter, nur beim Verantwortlichen eingesetzter und nur diesem bekannter „**Dateiformate**“, die sich auch nicht einfach in gängige maschinenlesbare Formate transferieren lassen, eine mögliche Schutzvorkehrung, die eine Benachrichtigungspflicht entfallen lassen könnte.

Die Verschlüsselung personenbezogener Daten bezieht auch die Verschlüsselung bei der Speicherung mit ein, die im Einzelfall die Verschlüsselung von Datenträgern, die Nutzung verschlüsselter Container (Datei mit internem Datei-System), die Verschlüsselung einzelner Dateien oder Verzeichnisse und mobiler, von Diebstahl bedrohter Geräte umfassen kann. 25

III. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

1. Vertraulichkeit

Die Vertraulichkeit von Systemen (Hardware) und Diensten (Software) setzt im Rahmen der Verarbeitung personenbezogener Daten zwingend ein Zugriffskonzept voraus, das mit Gruppen- und Benutzerrechten arbeitet und den Zugriff auf einzelne Daten im Rahmen der Verarbeitung abhängig von den erforderlichen Prozessen ermöglicht. Dies kann über eine Benutzerverwaltung des Betriebssystems, eine proprietäre Benutzer- und Rechteverwaltung von Anwendungssystemen oder hybride Formen der Benutzer- und Rechteverwaltung erfolgen. Hierzu gehören auch Maßnahmen der Zutrittskontrolle, der Zugangskontrolle und der Zugriffskontrolle, etwa durch bauliche Maßnahmen. 26

2. Integrität

„Die Integrität ist neben Verfügbarkeit und Vertraulichkeit eines der drei klassischen Ziele der Informationssicherheit.“[38] 27

Laut Glossar des Bundesamtes für Sicherheit in der Informationstechnik bezeichnet Integrität die

„Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen“.[39]

Im Sinne der Verordnung erfordert die Sicherstellung von Integrität zusätzlich die Richtigkeit von personenbezogenen Daten, sowie die Erkennung von Modifikationen. Die Integrität umfasst sowohl die Korrektheit der Daten an sich (Datenintegrität) als auch die korrekte Funktionsweise des Systems (Systemintegrität).

Die Integrität von Systemen und Diensten erfordert ihre Absicherung gegen Manipulationen. Dies umfasst u.a.

- die Wahrung der referentiellen Integrität in Datenbanken,[40]
- die Protokollierung von Änderungen,

36 *Lenhard*, a.a.O., Fn 979, weist zu Recht darauf hin, dass „der Stand der Technik sich ständig weiter[entwickelt]“ und es durchaus denkbar ist, dass eine Methode, die in einem Moment als sicher bezeichnet wird, schon wenige Wochen später als veraltet gilt.

37 Ebenda.

38 Https://de.wikipedia.org/wiki/Integrit%C3 %A4t_(Informationssicherheit).

39 Https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

40 Kann ein eingesetztes Softwaresystem die Integrität der Daten sicherstellen?

- das Durchführen von Plausibilitätsprüfungen,
- die Verhinderung der Eingabe ungültiger Werte (z.B. 25"9,– EUR),
- die ungewollte Löschung, Überschreibung oder Änderung von Daten.

Es ist sicherzustellen, dass Programme und Daten „nicht verfälscht und/oder falsche Daten nicht verarbeitet werden, damit sie (nicht unbemerkt) fehlerhafte Ergebnisse erzeugen oder Funktionen ausführen, die nicht erwünscht sind."[41]

> *„Datenintegrität soll durch geeignete Schutzmaßnahmen sicherstellen, dass jederzeit ein übermittelter Datenstrom rekonstruiert werden kann. Auf diese Weise wird sichergestellt, ob und wie Daten eventuell manipuliert worden sind."*[42]

3. Verfügbarkeit

28 Im Glossar des IT-Grundschutz-Kataloges des Bundesamtes für Sicherheit in der Informationstechnik[43] wird Verfügbarkeit wie folgt definiert:

> *„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können."*

29 Damit ist die **jederzeitige Betriebsbereitschaft** von Systemen und Diensten im Sinne der Sicherstellung einer „jederzeitigen Nutzbarkeit"[44] angesprochen. Diese kann durch verschiedene äußere, wie innere Einflüsse gefährdet sein. So kann Hardware defekt sein, ein plötzlicher Stromausfall kann Schäden an Datenbanken auslösen, ein Blitzschlag kann Unternehmensnetzwerke ebenso vollständig zerstören, wie Feuer oder Wasser; auch Sabotage kann die Integrität von Systemen schädigen. Entsprechend vielfältig und umfangreich können daher auch die Maßnahmen zur Sicherstellung von Integrität ausfallen.[45] Dies beginnt bei der richtigen Verkabelung, der richtigen Standortwahl[46] bis zur effektiven Absicherung der Systeme gegen unberechtigten Zugriff durch Dritte.[47] Ebenso können Wartungs- und Austauschpläne erforderlich sein. Ggf. sind Systeme redundant vorzuhalten,[48] mit einer unabhängigen Stromversorgung (USV) und einem professionellen Blitzschutz zu versehen, RAID-Systeme einzusetzen, und/oder eine hinreichende Klimatisierung der IT-Anlagen sowie Brandmeldeeinrichtungen und Löschanlagen im Bereich der zentralen IT oder eine redundante elektrische Versorgung[49] zu installieren.

4. Belastbarkeit

30 Die Belastbarkeit umfasst u.a., dass Systeme ausreichend dimensioniert[50] sind, um Verarbeitungen ohne Ausfälle und Wartezeiten durchführen zu können. Ebenso ist mit Belastbarkeit die

41 Https://datenschutz-berlin.de/content/technik/begriffsbestimmungen/verfuegbarkeit-integritaet-vertraulichkeit-authentizitaet.
42 Https://www.it-service24.com/lexikon/d/datenintegritaet/.
43 Https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.
44 *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 32 Rn 25.
45 Ebenda.
46 Z.B. Nicht im hochwassergefährdetem Keller.
47 Bspw. über ein Antivirenkonzept, eine entsprechende Sicherheitskonfiguration von Firewall, Router, Gateway, Proxy-Server, etc.
48 Bspw. NAS, Cluster, RZ, Cloud.
49 Netzteil, Stromnetz, Notstromgenerator.
50 Leistung, wie Speicherkapazität.

„**Toleranz eines Systems gegenüber Störungen**“[51] angesprochen,[52] die in der IT mit „**Resilienz**“[53] beschrieben wird. Sie umfasst auch die Ausfallsicherheit der IT-Systeme und Dienste.[54]

Die Sicherstellung der Integrität und der hierfür erforderlichen Maßnahmen kann die Hinzuziehung von Experten aus anderen Fachbereichen wie z.B. Brandschutz, Elektrotechnik, Klima- und Lüftungstechnik oder Sicherheitstechnik erforderlich machen. Eine Validierung sollte nur durch einen ausgewiesenen Fachexperten erfolgen. 31

IV. Wiederherstellbarkeit

Als weitere technische und organisatorische Maßnahme beschreibt Art. 32 Abs. 1 lit. c) DSGVO die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. 32

Dies umfasst die Etablierung von Wiederherstellungsmöglichkeiten (Backup und Recovery), wie die 33

- Sicherung von Installationen (Bare-Metal-Recovery),
- Sicherung von Daten,
- Sicherung von Systemdateien und Datencontainern,
- Sicherung von Log-Dateien,
- Sicherung von Benutzerkonten,
- Sicherung von Konfigurationen (Einstellungen, Freigabe).

Entscheidend ist auch der Ort, an dem Sicherungen verfügbar gehalten werden. Eine Sicherung im Netzwerk bringt oft nicht viel. So sind von Krypto-Trojanern (sog. **Ransomware**) in vielen Fällen auch Netzwerklaufwerke verschlüsselt worden; auch bietet eine Sicherung vor Ort im Fall eines Brandes keine hinreichende Wiederherstellungsgarantie. Ein funktionierendes Datensicherungskonzept kann generell entscheidend für den Fortbestand eines Unternehmens sein. Um zu beantworten, welche konkreten Maßnahmen im Einzelnen erforderlich sind, sind u.a. nachfolgende Fragestellungen maßgeblich: 34

- Welche Daten werden durch das System verarbeitet?
- Wer nutzt das System?
- Welche maximale Standzeit eines Systems ist akzeptabel?
- Wie wird gewährleistet, dass innerhalb der maximalen Standzeit das System wieder in Betrieb geht?

V. Organisatorische Maßnahmen

Neben den vorgreiflich technischen Maßnahmen beschreibt Art. 32 Abs. 4 DSGVO eine organisatorische Maßnahme. Der Verantwortliche hat sicherzustellen, dass die ihm unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Wie dies umzusetzen ist, beschreibt die Verordnung nicht näher. In Betracht kommen Umsetzungen innerhalb von Arbeitsverträgen, Betriebsvereinbarungen oder auch 35

51 *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 32 Rn 26.

52 Die Studie „The Future of IT: Migrations, Protection & Recovery Insights“ der Vision Solutions stellt fest, dass Unternehmen nicht ausreichend darauf vorbereitet sind, Resilienz für ihre IT-Systeme zu bieten, abrufbar unter: http://www.visionsolutions.com/webforms/state-of-resilience/state-of-resilience-2015.

53 In der englischen Sprachfassung wird dementsprechend auch von „resilience of processing systems and services“ gesprochen.

54 Hierzu https://www.springerprofessional.de/technische-informatik/it-organisation/unternehmen-wissen-nicht-wie-belastbar-ihre-it-infrastrukur-ist/6607330.

Dienstanweisungen. Da eine Sicherstellung gefordert wird, muss der Verantwortliche geeignete Maßnahmen ergreifen, um die Einhaltung derartiger Anweisungen durch seine Beschäftigten zu überprüfen. Dies kann über den Einsatz von Testpersonen oder unangemeldete Kontrollen erfolgen.

36 Eine Verpflichtung zur Sicherstellung dahingehend, dass die Verarbeitung nur nach Anweisung des Verantwortlichen erfolgt, besteht nicht, soweit die dem Verantwortlichen unterstellten natürlichen Personen „nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet" sind. Dies ist bei Ärzten der Fall, die im Rahmen der eigentlichen ärztlichen Behandlung grundsätzlich weisungsfrei und eigenverantwortlich zu handeln haben.

VI. Regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

37 Nach Art. 32 Abs. 1 lit. d) DSGVO sind die vom Verantwortlichen ergriffenen technischen und organisatorischen Maßnahmen zudem regelmäßig systematisch zu überprüfen und in Bezug auf ihre Wirksamkeit zur Gewährleistung der Sicherheit der Verarbeitung zu bewerten und zu evaluieren.

38 Die regelmäßige Überprüfung umfasst dabei die regelmäßige Durchführung und Dokumentation von Rücksicherungstests der erzeugten Backups.[55] Auch das Durchlaufen sog. **Penetrationstests** kann eine regelmäßige Überprüfungsmaßnahme darstellen.

39 Je nach Umfang der vorhandenen IT-Anlagen, sollte in einem Zeitraum zwischen ein und drei Jahren ein **Datenschutzaudit** durch einen unabhängigen Sachverständigen durchgeführt werden. Im Rahmen des Audits sollten die technischen Anlagen ebenso überprüft werden, wie der aktuelle Stand der Dokumentationen, Betriebsvereinbarungen, Dienstanweisungen und/oder Unternehmensleitlinien (Bewertung und Validierung).

40 Nach Art. 32 Abs. 3 DSGVO können entsprechende Maßnahmen auch in genehmigten Verhaltensregeln gemäß Art. 40 DSGVO normiert sein. Der Nachweis angemessener Maßnahmen im Einzelfall erfordert eine entsprechende **Dokumentation** der technischen und organisatorischen Maßnahmen durch den Verantwortlichen. Die **Einhaltung genehmigter Verhaltensregeln** gemäß Art. 40 DSGVO oder das erfolgreiche **Durchlaufen eines genehmigten Zertifizierungsverfahrens** gemäß Art. 42 DSGVO können zusätzliche Anhaltspunkte für die Etablierung geeigneter und angemessener technischer und organisatorischer Maßnahmen bilden.

D. Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DSGVO

41 Die DSGVO normiert in Art. 25 DSGVO die Grundsätze des Datenschutzes durch Technikgestaltung (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default). Sie greift mit der Vorschrift einen Regelungsbereich auf, der sich in dieser Form und Ausprägung weder in der Datenschutzrichtlinie, noch in den nationalen Datenschutzgesetzen fand.

55 Oftmals werden Backups einfach weggelegt, ohne zu prüfen, ob dies auch erfolgreich war. In einem vom Autor betreuten Fall war erst bei einer Havarie aufgefallen, dass der Sicherungsroboter zwar regelmäßig Bänder wechselte, diese jedoch bereits seit langer Zeit offenbar nicht ausgewechselt waren und die Sicherungsbänder keine Beschichtung mehr aufwiesen. Es war also gar nichts aufgeschrieben worden. Das System hatte hier indes keine Fehler gemeldet.

I. Zentrale Begriffe und ihre Grundlagen

1. Datenschutz durch Technik – Data protection by Design

a) Historische Entwicklung

Die Zielsetzung dieses Werkes liegt in der Unterstützung des Lesers im Rahmen der praktischen Handhabung des Datenschutzrechtes in der täglichen Beratungs- und Umsetzungspraxis, gleichwohl kann man sich dem Themenkomplex des „data privacy by design" auch praktisch nicht nähern, ohne die historischen Grundlagen des dahinter stehenden Konzeptes näher zu beleuchten. Der europäische Gesetzgeber tut nicht viel dafür – sowohl in Art. 25 DSGVO, als auch in den hierauf bezogenen Erwägungsgründen[56] -, dem Begriff eine genaue Kontur zu verleihen. Vielmehr wird der Begriff als „bekannt" vorausgesetzt. Dies enttäuscht anlässlich des Stellenwertes, den der Gesetzgeber den Regelungen in Art. 25 DSGVO beigemessen hat[57] und macht eine intensivere Befassung mit dem Konzept des data protection by design erforderlich. 42

Der Begriff „data privacy by design" wird auf die wissenschaftlichen Arbeiten der langjährigen Informationsfreiheits- und Datenschutzbeauftragten der kanadischen Provinz Ontario, *Ann Cavoukian*,[58] die zwischenzeitlich als Executive Director of the Privacy and Big Data Institute an der kanadischen Ryerson University tätig ist,[59] zurückgeführt. 43

Tatsächlich, so kann es in der siebenteiligen Abhandlung „Privacy by Design: Vom Recht zum Code" von *Schulzki-Haddouti*[60] nachgelesen werden, wurde der Begriff wohl von einer kanadischen IT-Firma im Jahre 2000 geprägt[61] und von *Cavoukian* lediglich übernommen, fortentwickelt und vor allem in die internationale Datenschutzdiskussion eingeführt.

Cavoukian vertritt im Zusammenhang mit ihrem Privacy by Desgin (PbD)-Ansatz insgesamt sieben Kernthesen:[62] 44

1. Proactive not Reactive; Preventative not Remedial[63]
2. Privacy as the Default[64]

56 Erwägungsgrund 78 DSGVO.

57 Gem. Art. 83 Abs. 4 lit. a) DSGVO können bei Verstößen gegen die folgenden Bestimmungen Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden.

58 Https://de.wikipedia.org/wiki/Ann_Cavoukian.

59 Http://www.ryerson.ca/pbdi/about/people/cavoukian/.

60 Eine Übersicht der verlinkten Einzelbeiträge des äußerst lesenswerten Papiers findet sich auf der Internetseite der Autorin unter http://schulzki-haddouti.de/?p=1012. Die Einzelbeiträge sind auf der Plattform https://www.datenschutzbeauftragter-online.de/ erschienen.

61 *Schulzki-Haddouti,* Ideengeschichte des Privacy by Design – Teil 4: Wege in die Gestaltung, abrufbar unter: https://www.datenschutzbeauftragter-online.de/ideengeschichte-privacy-by-design-teil-4-wege-gestaltung/10036/.

62 Vgl. etwa *Cavoukian*, IDIS (2010) 3, 247, abrufbar unter: https://link.springer.com/article/10.1007/s12394–010–0062-y.

63 „The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events. It does not wait for risks to materialize, nor does it offer remedies for resolving infractions once they have occurred—it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.", *Cavoukian*, IDIS (2010) 3, 247, 249.

64 „We can all be certain of one thing—the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy—it is built into the system, by default.", *Cavoukian*, IDIS (2010) 3, 247, 250.

3. Privacy Embedded into Design[65]
4. Full Functionality—Positive-Sum, not Zero-Sum[66]
5. End-to-End Lifecycle Protection[67]
6. Visibility and Transparency[68]
7. Respect for User Privacy[69]

45 PbD umfasst in diesem Sinne sowohl software-technische Maßnahmen in Bezug auf die (internen) Verarbeitungsvorgänge des Verantwortlichen, als auch Maßnahmen zur Schaffung von effektiven Kontrollmöglichkeiten der betroffenen Person, wobei letztere im Europäischen Kontext wohl eher im Rahmen des – ebenfalls in Art. 25 DSGVO beschriebenen – Grundsatzes des „Data Privacy by Default" Geltung erlangen.

46 Bezogen auf die vom Verantwortlichen zu treffenden Maßnahmen beschreibt PbD einen proaktiven Ansatz und sieht in der Beachtung von Datenschutzfragen bereits in der Planungsphase von neuen IT-Projekten einen entscheidenden Vorteil gegenüber dem bislang maßgeblich verfolgten sanktionierenden Datenschutz.[70] Gerade weil die automatisierte Verarbeitung immer mehr an Bedeutung gewinnt, ist es entscheidend, dass bereits in der Planungsphase Risiken ermittelt und angemessene Schutzmaßnahmen ergriffen werden.

47 Ein anschauliches Beispiel der (an die vom Verantwortlichen eingesetzte Softwareumgebung und damit auch an die Softwarehersteller[71] gestellten) Rahmenbedingungen liefert ein Beitrag von

65 „Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality", *Cavoukian*, IDIS (2010) 3, 247, 250.

66 „Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum, or doubly enabling „win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. It avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.", *Cavoukian*, IDIS (2010) 3, 247, 250.

67 „Privacy, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.", Cavoukian, IDIS (2010) 3, 247, 250.

68 „Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.", Cavoukian, IDIS (2010) 3, 247, 250.

69 „Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric—focused on the individual.", Cavoukian, IDIS (2010) 3, 247, 250.

70 *Rost/Bock*, DUD 2011, 30, 31.

71 In Erwägungsgrund 78 DSGVO heißt es insoweit eindeutig: „In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, **sollten die Hersteller der Produkte, Dienste und Anwendungen** ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden."

Cavoukian/Jonas[72] aus dem Jahre 2012 zur Umsetzung von PbD-Technologien in Big Data Anwendungen. Der Beitrag beschreibt die von *Jonas*, Chief Scientist of the IBM Entity Analytics,[73] bereits im Jahre 2008 begonnene Entwicklung eines „sinnstiftenden"[74] Softwaredesigns, das dabei helfen soll, schnellere und zugleich aus Sicht des Datenschutzes bessere Entscheidungen im Rahmen der Verarbeitung von Daten zu treffen. PbD folgt hier dem Prinzip, dass sich die Daten selbst finden und die für einen Verarbeitungsschritt relevanten Informationen erst dann den Systemnutzer „finden" („the data finds the data, and the relevance finds the unser"[75]). Das von *Jonas* entwickelte PbD-System folgt dabei sieben Grundprinzipien:

48

1) „**Full Attribution**": Jedes Datum wird im System so abgelegt, dass jederzeit bestimmt werden kann, von wo und wann es in das System gelangte.
2) **„Data Tethering"**: Jede Veränderung eines Datums im Hauptsystem führt zwangsläufig zu einer Änderung des Datums in jedem Unter- und Folgesystem, welches das Datum verwendet.
3) **Analytics on anonymized Data**: Um die Risiken, die mit der Verarbeitung von Daten einhergehen zu vermindern, werden – überall dort, wo es technisch möglich ist – Anonymisierungs- oder Pseudonymisierungstechniken eingesetzt. Jedes Datenfeld innerhalb eines Systems kann administrativ – auch für einzelne Verarbeitungsschritte – anonymisiert oder pseudonymisiert werden.
4) **Tamper Resistant Audit Logs**: Jeder Zugriff auf ein Datum durch einen Nutzer im System wird durch das System manipulationssicher (anhand des Datums) protokolliert und erfasst. Auch Administratoren des Systems können nicht „unbemerkt" auf Daten zugreifen.
5) **False Negative Favoring Methods**: Das System sollte so eingestellt sein, dass es eher dazu tendiert, Daten nicht zu verarbeiten, als sie zu verarbeiten.
6) **Self Correcting False Positives**: Das System sollte so eingestellt sein, dass es fälschlicherweise zum Gegenstand einer Verarbeitung gemachte Daten erkennt, indem jede neue zusätzliche Information zu einem Datensatz mit vorherigen Informationen abgeglichen und stetig aktualisiert werden.
7) **Information Transfer Accounting**: Jedes Datum wird im System so abgelegt, dass jederzeit bestimmt werden kann an wen es wann übermittelt wurde.

Die im Big-Data-Projekt von *Jonas* umgesetzten Maßnahmen entsprechen den in den Erwägungsgründen[76] der DSGVO eher abstrakt umschriebenen. Hiernach sollen Maßnahmen unter anderem darin bestehen,

- *„dass die Verarbeitung personenbezogener Daten minimiert wird,*
- *personenbezogene Daten so schnell wie möglich pseudonymisiert werden,*
- *Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird,*
- *der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und*
- *der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern."*

72 *Cavoukian/Jonas,* Privacy by Design in the Age of Big Data, Juni 2012, abrufbar unter: http://gpsbydesign.org/wp-content/uploads/2016/07/privacy-by-design-in-the-age-of-big-data.pdf.

73 Https://www.research.ibm.com/theworldin2050/bios-Jonas.shtml.

74 „Sensemaking-style system", *Cavoukian/Jonas,* Privacy by Design in the Age of Big Data, Juni 2012, S. 8, abrufbar unter: http://gpsbydesign.org/wp-content/uploads/2016/07/privacy-by-design-in-the-age-of-big-data.pdf.

75 *Cavoukian/Jonas,* Privacy by Design in the Age of Big Data, Juni 2012, S. 5, abrufbar unter: http://gpsbydesign.org/wp-content/uploads/2016/07/privacy-by-design-in-the-age-of-big-data.pdf.

76 Erwägungsgrund Nr. 78 DSGVO.

b) Schlussfolgerungen für die inhaltliche Bestimmung von pdD

49 Sicherlich betreffen die Arbeiten von Jonas ein ganz spezielles Produkt und einen speziellen Anwendungsbereich. Gleichwohl wird deutlich, dass PbD mehr ist, als blanke Theorie und dass der oft zu Unrecht vorschnell als „gefährlich" abgetane Einsatz technischer Systeme dem Datenschutz nicht zwingend hinderlich sein muss, sondern Datenschutz vielmehr aktiv fördern kann. Wie das Beispiel von *Jonas* verdeutlicht, kann PbD als **systemische automatisierte Entscheidungsunterstützung** verstanden werden. Hierfür ist es erforderlich, ein personenbezogenes Datum auch innerhalb technischer Systeme als solches und nicht bloß als einfachen Datensatz zu begreifen und bestimmte, an der Vorgaben der DSGVO orientierte, Informationen als sog. Metainformationen jedem personenbezogenen Datum „anzuheften", um die automatisierte Verarbeitung unter Beachtung der Datenschutzgrundsätze zu erleichtern und sicherzustellen.[77]

50 Die DSGVO fordert vom Verantwortlichen, dass dieser über die Herkunft und die Empfänger eines Datums Auskunft erteilen kann. Dies kann systemisch dadurch sichergestellt werden, dass eben diese Information jedem personenbezogenen Datensatz angeheftet und dauerhaft mit diesem verbunden ist. So kann sicher beurteilt werden, wann ein Datum von wo in das System gelangt und an wen es aus dem System wann wieder herausgegeben wurde. Metainformationen zu Verarbeitungszwecken, die unter Berücksichtigung der im Rahmen einer Datenschutzfolgenabschätzung erkannten Risiken die Verarbeitung eines Datums in einem bestimmten Kontext gestatten oder verbieten, könnten eine datenschutzkonforme Verarbeitung personenbezogener Daten ebenso sicherstellen. Bestimmte Daten (bspw. Kontoinformationen) beim Datenaufruf könnten durch einen Call-Center-Agent, der lediglich Reklamationen zu einem bestimmten Produkt entgegen nimmt oder im Out-Bound für ein neues Produkt Werbung betreibt, bei Aufruf des Kundenprofils von vornherein ausgeblendet und damit für eine Verarbeitung durch den Agent gesperrt werden. Dies wäre sicherlich wesentlich effektiver, als derartige Informationen anzuzeigen und sich lediglich darauf zu beschränken, über eine Dienstanweisung die Verwendung dieser Daten zu untersagen.

51 Verantwortliche, wie auch die Hersteller der von ihnen für die automatisierte Verarbeitung eingesetzten Softwaresysteme sind mit Inkrafttreten der DSGVO gehalten, sich mit den bestehenden Möglichkeiten, die die Technik zur Lösung derartiger Probleme bereitstellt, zu befassen und diese – soweit möglich und zumutbar – zum Einsatz zu bringen.[78] Insoweit wird sich zukünftig auch die Softwareentwicklung an den datenschutzrechtlichen Vorgaben zu orientieren und diese umzusetzen haben.[79]

2. Datenschutz durch datenschutzfreundliche Voreinstellungen – Data protection by Default

52 Art. 25 Abs. 2 DSGVO enthält die Verpflichtung des Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit, heißt es im Gesetzestext wörtlich (sog. Data protection by Default, nachfolgend kurz: DpD).

77 So auch *Martini*, in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 25 Rn 30, der davon spricht, dass die Daten bei ihrer Erhebung mit einem elektronischen Etikett zu versehen sind, die Daten dauerhaft einem bestimmten Verarbeitungszweck zuordnen.

78 Siehe Erwägungsgrund Nr. 78 S. 4 DSGVO.

79 Erwägungsgrund Nr. 78 DSGVO spricht insoweit auch davon, dass die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen „auch bei öffentlichen Ausschreibungen Rechnung getragen werden" soll.

Die Verpflichtung zur Etablierung von DpD-Maßnahmen durch den Verantwortlichen konkretisiert die in Art. 5 Abs. 1 lit. b) und c) DSGVO normierten Datenschutzgrundsätze der Zweckbindung und der Datenminimierung.[80] Nähere Angaben dazu, wie dieser Grundsatz umzusetzen ist, finden sich in der DSGVO nicht. Art. 25 DSGVO wird gleichwohl in dem Sinne zu verstehen sein, dass der Grundsatz der datenschutzfreundlichen Voreinstellungen sowohl innerhalb des Verantwortlichen, als auch im Verkehr mit Dritten zu beachten ist. 53

Ein anschauliches Beispiel für „datenschutzunfreundliche Voreinstellungen" liefert ein lesenswerter Beitrag von *Franck,*[81] der sich – zwar im Wesentlichen wettbewerbsrechtlich motiviert – mit von zahlreichen Herstellen mobiler Endgeräte (Handys) im Rahmen der E-Mail-Funktionalität etablierten Voreinstellung einer Absendersignatur befasst, die darüber aufklärt, dass eine E-Mail von einem bestimmten Markengerät abgesendet wurde.[82] Eine derartige Information ist sicherlich personenbezogen. Sie gibt Auskunft darüber, dass der Absender die E-Mail über ein Smart-Phone bearbeitet hat, welches Smart-Phone er nutzt (was wiederum Erkenntnisse zur vermeintlichen Kaufkraft des Absenders liefern könnte) und darüber, dass er zum Zeitpunkt des Verfassens einer E-Mail unterwegs war.[83] Der kleine Satz, den die Smart-Phone-Hersteller sicherlich zu Werbezwecken[84] einsetzen, ist damit weder datenschutzneutral, noch steht er im Einklang mit dem Grundsatz des DpD. 54

Ähnliches gilt für die auf vielen Webportalen im Rahmen des Anmeldevorganges voreingestellt gesetzten Häkchen „**angemeldet bleiben**".[85] Auch hier handelt es sich um eine datenschutzunfreundliche Voreinstellung, die zukünftig unzulässig sein dürfte. 55

Innerhalb der Unternehmensorganisation eines Verantwortlichen könnte die Verpflichtung zur Umsetzung von DpD-Maßnahmen ggf. eine Verpflichtung begründen, Mitarbeiter, die mit Verarbeitungen befasst werden, durch entsprechende Software-Vorgaben darin zu unterstützen, nur solche personenbezogenen Daten zu verarbeiten, die für die vom Verantwortlichen verfolgten Zwecke auch erforderlich sind. Ein klassisches Beispiel für in der Regel unnötige Erhebungen sind die in vielen Softwarelösungen vorzufindenden sog. **Freitextfelder**, in die der Nutzer grundsätzlich jede Information ablegen kann, ohne dass eine Kontrolle hinsichtlich der datenschutzrechtlichen Erforderlichkeit derartiger Informationen stattfindet. Beispiel: Ein Kunde meldet sich auf eine Zahlungsaufforderung bei einem Sachbearbeiter seines Gläubigers und berichtet, dass er die Zahlung am Tag, an dem die Mahnung bei ihm eingegangen ist, überwiesen hat. Die für die Sachbearbeitung erforderliche Information, „auf Mahnung bezahlt durch Überweisung am" ist damit vorhanden. Der Kunde berichtet nunmehr jedoch darüber hinaus auch über die Gründe der nicht frist- 56

80 In diesem Sinne auch *Feiler/Forgó*, EU-DSGVO, 2017, Art. 25. Rn 8; *Martini*, in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 25, Rn 12; siehe auch *Niemann/Scholz*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, 2012, S. 109, 114.

81 *Franck*, K&R 2017, 226.

82 Bspw. „Gesendet von meinem IPhone" oder „Von meinem Samsung gesendet". Zu den Möglichkeiten, dies auszustellen vgl. bspw. http://www.kylook.com/de/faq/android-die-e-mail-signatur-aendern/.

83 Ein Arbeitnehmer, der normalerweise im Büro am Schreibtisch sitzen sollte, versendet eine Mail über sein Smart-Phone und lässt damit zumindest Raum für Spekulationen darüber, ob er sich – arbeitsrechtswidrig – nicht an einem anderen Ort aufhält.

84 Hierzu ausführlich, *Franck*, K&R 2017, 226, 227.

85 Über diese Funktion wird ein entsprechender Cookie gesetzt.

gerechten Zahlung.[86] Der Mitarbeiter schreibt diese Informationen im Freitext mit, da sie ggf. nützlich sein könnten. Zudem soll einem etwaigen anderen Sachbearbeiter der Umgang mit dem Kunden erleichtert werden. So werden zahlreiche für die eigentliche Sachbearbeitung nicht erforderliche Informationen erhoben (= verarbeitet), die sich nicht auf ein bestehendes Vertragsverhältnis mit dem Schuldner beziehen, sondern auch besondere Kategorien personenbezogener Daten über Dritte (hier vielleicht den Partner des Schuldners und seine Gesundheit), weitergehende Informationen über den Schuldner und seine Beziehungen zu Dritten. Die Verarbeitung derartiger Daten ist in der Regel nicht erforderlich und folgt auch keiner konkreten Zweckfestsetzung. Freitextfelder werden einfach befüllt und verbleiben danach auf immer und ewig im System. Die datenschutzrechtliche Relevanz ist dabei unbestritten, so dass eine datenschutzfreundliche Voreinstellung in der beschriebenen Konstellation darin gesehen werden könnte, dass Freitextfelder entfernt und stattdessen auf eine strukturierte Datenerhebung gesetzt wird.

57 Beispielhaft nennt Art. 25 Abs. 2 S. 3 DSGVO eine Maßnahme der datenschutzfreundlichen Voreinstellung, die darin bestehen soll, sicherzustellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Hier ist das automatisierte Teilen von Posts mit Dritten auf Social-Media-Plattformen angesprochen. Auch ohne Eingreifen des Nutzers vom System bereitgestellte Statusmeldungen dürften hierunter fallen.[87]

II. Umsetzungspflicht des Verantwortlichen

58 Art. 25 DSGVO normiert eine konkrete Verpflichtung des Verantwortlichen zur Etablierung der hier beschriebenen Maßnahmen unter Berücksichtigung der Kriterien der des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.[88]

E. Dokumentation von Verarbeitungstätigkeiten

59 Mehr als bislang setzt das neue Datenschutzrecht auf den Aspekt der Transparenz als Mittel der Sicherung eines angemessenen Datenschutzniveaus. Datenschutz im Sinne der DSGVO realisiert sich vor allem über den Aspekt der „**Datenverarbeitungstransparenz**". Dies wird besonders deutlich anhand des in Art. 5 Abs. 2 DSGVO normierten „**Rechenschaftsprinzips**", das dem Verantwortlichen auferlegt, jederzeit die Rechtmäßigkeit der von ihm vollzogenen Verarbeitung nachweisen zu können. Die Rechenschaftspflicht selbst normiert – wie bereits beschrieben (siehe § 3 Rdn 45 ff.) – für sich genommen keine bestimmte Dokumentationspflicht des Verantwortlichen. Vor dem Hintergrund der geforderten Nachweisbarkeit nimmt die Dokumentation von Verarbeitungsvorgängen jedoch zukünftig einen wesentlich größeren Stellenwert ein als bisher.[89]

86 „Wissen Sie, als die Rechnung einging war ich im Urlaub. Als ich zurückkam, erlitt mein Partner bei Auslanden des Autos eines schweren Herzinfarkt und musste ins Krankenhaus. Jetzt ist der in der Reha und ich muss mich mit meinen beiden Kindern abwechseln, um ihn zu besuchen, damit er nicht so allein ist. Nach seinem Burn-Out im Februar ist er da nicht mehr so belastbar. Und für mich ist es nach der Knie-Op auch nicht so einfach da immer hinzulaufen. Und die Tanja, meine Tochter, kann mit der Kleinen, die ist ja gerade erst zwei Monate alt, auch nicht so einfach jeden Tag dahin, nachdem man ihr auch noch das Auto weggepfändet hat."

87 Hierzu auch *Martini*, in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 25 Rn 52.

88 Zum Stand der Technik, kann ebenso wie zu den berücksichtigungsfähigen Implementierungskosten auf die Ausführungen zu § 22 Abs. 2 BDSG-Neu verwiesen werden, oben § 4 Rdn 326 ff.

89 *Gossen/Schramm*, ZD 2017, 7, 10.

Dabei kennt die DSGVO sowohl ausdrücklich normierte Dokumentationspflichten, als auch solche, deren Erforderlichkeit sich in Zusammenschau des Art. 5 Abs. 2 DSGVO mit anderen an den Verantwortlichen gerichteten Verpflichtungen nach der DSGVO ergibt. 60

I. Verzeichnis über Verarbeitungstätigkeiten des Verantwortlichen, Art. 30 DSGVO

1. Abweichungen zum bisherigen Recht

Bereits nach bisherigem deutschen Datenschutzrecht war der Verantwortliche verpflichtet, eine Übersicht über seine Verarbeitungstätigkeiten zu erstellen (sog. **Verfahrensverzeichnis**). Das Verfahrensverzeichnis nach deutschem Recht gliederte sich dabei in einen öffentlichen, auf Verlangen jedermann zur Verfügung zu stellenden, und einen nicht-öffentlichen Teil, der lediglich der zuständigen Datenschutzaufsicht auf deren Verlangen hin auszuhändigen war.[90] Diese Verpflichtung ist flankiert durch die bislang in § 4d BDSG normierte Meldepflicht, nach der grundsätzlich alle Verfahren[91] automatisierter Verarbeitungen personenbezogener Daten bei der Datenschutzaufsichtsbehörde gemeldet werden müssen.[92] Die DSGVO verzichtet nicht nur auf die Beibehaltung einer generellen Meldepflicht für jede automatisierte Verarbeitung, sondern auch auf die Verpflichtung des Verantwortlichen, sein Verfahrensverzeichnis auf Anfrage jedermann zugänglich zu machen. Das sog. **Jedermannverzeichnis** oder öffentliche Verfahrensverzeichnis wird damit ab dem 25.5.2018 Geschichte sein. Auf den ersten Blick sieht es aus, als sei damit eine Herabsetzung des bisherigen Datenschutzniveaus verbunden; dies ist jedoch tatsächlich nicht der Fall. Der Verzicht auf die Zurverfügungstellung des Jedermannverzeichnisses erfährt ebenso wie der Verzicht auf die – auch bislang in den Fällen, in denen der Verantwortliche einen Datenschutzbeauftragten bestellt hatte, ohnehin nicht zur Anwendung gelangte – Verpflichtung zur Meldung gegenüber der Datenschutzbehörde ihre Kompensation in den in Art. 13 und 14 DSGVO normierten aktiven Informationspflichten des Verantwortlichen gegenüber der betroffenen Person, die unbeschadet einer entsprechenden Anfrage des Betroffenen entstehen und zu erfüllen sind. Wie bereits ausführlich dargestellt (siehe § 5), gehen die Informationspflichten der DSGVO dabei z.T. weit über das hinaus, was bislang mit dem öffentlichen Teil des Verfahrensverzeichnisses gegenüber der betroffenen Person bekannt zu geben war, so dass mit Wirksamwerden der DSGVO tatsächlich ein gleichwertiges, wenn nicht sogar höheres Datenschutzniveau etabliert wird. 61

Das Verfahrensverzeichnis, wie man es bisher, auch aus Art. 18 der Datenschutzrichtlinie kannte, verschwindet nicht gänzlich aus dem Regelungskomplex der DSGVO, sondern bleibt als sog. **Verzeichnis über Verarbeitungstätigkeiten** gem. Art. 30 DSGVO weiterhin – wenn auch „nur" zum Zwecke der Einsichtnahme durch die Datenschutzaufsichtsbehörden – existent.[93] 62

90 § 4g Abs. 2 und § 4e BDSG.

91 „Unter Verfahren ist die Gesamtheit an Verarbeitungen zu verstehen, mit denen eine oder mehrere miteinander verbundene Zweckbestimmung(en) realisiert werden sollen. Daher kann ein Verfahren eine Vielzahl von DV-Dateien umfassen", Merkblatt zur Meldepflicht verantwortlicher nicht-öffentlicher Stellen bei der Aufsichtsbehörde für den Datenschutz nach § 4d BDSG, abrufbar unter: https://www.datenschutz-wiki.de/Merkblatt_zur_Meldepflicht.

92 Zu den Ausnahmen von der Meldepflicht, siehe das Merkblatt zur Meldepflicht verantwortlicher nicht-öffentlicher Stellen bei der Aufsichtsbehörde für den Datenschutz nach § 4d BDSG, abrufbar unter: https://www.datenschutz-wiki.de/Merkblatt_zur_Meldepflicht.

93 *Licht*, ITRB 2017, 65, 67; Art. 30 Abs. 4 DSGVO.

2. Formale und inhaltliche Anforderungen

63 Nach Art. 30 Abs. 3 DSGVO ist das Verzeichnis über Verarbeitungstätigkeiten „schriftlich zu führen", was auch in einem elektronischen Format, also auch in der im deutschen Recht bekannten Textform, erfolgen kann.

64 Das Verarbeitungsverzeichnis muss gem. Art. 30 Abs. 1 lit. a) bis g) bestimmte inhaltliche Mindestanforderungen erfüllen und über nachfolgende Punkte informieren:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b) die Zwecke der Verarbeitung;
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

65 Die Vorgaben gleichen in weiten Teilen denen in Art. 13, 14 DSGVO, so dass zur Konkretisierung auf die dortigen Ausführungen (siehe § 5 Rdn 7 ff. und 121 ff.) verwiesen werden kann. Bzgl. der Verwendung der Begrifflichkeit „Kategorien" wird klargestellt, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen beziehen muss. Mit Blick auf die grundlegenden Anforderungen in Art. 32 DSGVO dürfte die in Art. 30 Abs. 1 lit. g) normierte Einschränkung „wenn möglich", in der Praxis keine Bedeutung erfahren, so dass das Verarbeitungsverzeichnis generell eine allgemeine Beschreibung der vom Verantwortlichen etablierten technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO enthalten muss.[94] Da es sich ohnehin empfiehlt, diese entsprechend zu dokumentieren, kann im Verarbeitungsverzeichnis auf eine solche gesonderte Dokumentation Bezug genommen werden. Dabei ist darauf zu achten, dass es trotz entsprechender Verweise für die Aufsichtsbehörde weiterhin möglich ist, die wesentlichen Inhalte und Schlussfolgerungen unmittelbar aus der Verarbeitungsübersicht heraus nachzuvollziehen.

3. Ausnahmen von der Verpflichtung zur Führung eines Verarbeitungsverzeichnisses

66 Art. 30 Abs. 5 normiert Ausnahmen von der Verpflichtung zur Führung eines Verzeichnisses über Verarbeitungstätigkeiten zugunsten solcher Unternehmen, die regelmäßig weniger als 250 Mitarbeiter beschäftigen. Gerade kleine und mittlere Unternehmen hören an dieser Stelle oft auf, das Gesetz zu lesen und wiegen sich in Sicherheit. Diese Erfahrung hat jedenfalls der Autor dieses Werkes im Rahmen seiner zahlreichen Vorträge zu den mit der DSGVO einhergehenden Verände-

94 So auch *Plath*, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl. 2017, Art. 30 Rn 2; *Raum*, in: Ehmann/Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2017. Art. 30 Rn 10; *Klug*, in: Gola (Hrsg.), DS-GVO, 2017, Art. 30 Rn 9.

rungen in den vergangenen zwei Jahren gemacht. Wer Art. 30 Abs. 5 DSGVO bis zum Ende liest, der erkennt schnell, dass hier tatsächlich eine echte und in vielen Konstellationen sicherlich nicht Platz greifende Ausnahme beschrieben wird, die eher restriktiv zu handhaben sein wird.[95]

67 Eine Verpflichtung auch bei Unternehmen mit weniger als 250 Mitarbeitern soll bestehen, sofern die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt. Diese „**Öffnungsklausel**" ist bereits recht weitreichend, geht doch mit jeder Verarbeitung personenbezogener Daten ein gewisses Risiko für die Rechte und Freiheiten der betroffenen Personen einher, so dass man sich bereits fragen kann, wo vor diesem Hintergrund überhaupt noch ein Anwendungsbereich für die Ausnahme verbleibt.[96] Zu denken ist hier ggf. an wirkliche Kleinstbetriebe, bei denen die Verarbeitung personenbezogener Daten eher „Randerscheinung" denn eigentlicher Geschäftszweck ist. So mag der einzelunternehmerisch tätige Handwerker, der außer zum Zwecke der Terminswahrnehmung und der Rechnungsstellung gegenüber seinen Kunden, keine personenbezogenen Daten verarbeitet, von der Verpflichtung nach Art. 30 Abs. 1 DSGVO ausgenommen sein; ebenso diejenigen Unternehmen, die im reinen B2C-Verkehr agieren und die Verarbeitung nur gelegentlich erfolgt (so bspw. im klassischen Tante-Emma-Laden").

68 Ebenfalls entfällt die Verpflichtung nicht, soweit die Verarbeitung personenbezogener Daten einen Kernbestandteil der eigentlichen geschäftlichen Aktivität des Verantwortlichen bildet, so z.B. in der Inkasso- oder der Werbewirtschaft. Hier soll es gerade nicht darauf ankommen, wie viele Mitarbeiter ein Verantwortlicher im Rahmen seiner Verarbeitungsvorgänge beschäftigt. Ebenso entfällt eine Verpflichtung zur Führung eines Verarbeitungsverzeichnisses dort nicht, wo besondere Datenkategorien gemäß Art. 9 Abs. 1 DSGVO verarbeitet werden oder die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO erfolgt. Sämtliche Leistungserbringer im Gesundheitswesen dürften in diesem Sinne zum Kreis der nach Art. 30 Abs. 1 DSGVO Verpflichteten zu zählen sein.

II. Verzeichnis über Verarbeitungstätigkeiten des Verantwortlichen

69 Die DSGVO verpflichtet nunmehr auch den Auftragsverarbeiter zum Führen eines speziellen Verzeichnisses über seine Verarbeitungstätigkeiten im Auftrag. Näheres hierzu ist in Art. 30 Abs. 2 DSGVO normiert und soll – dem Zusammenhang geschuldet – im Rahmen des Abschnittes zur Auftragsverarbeitung (siehe § 8) behandelt werden.

III. Aus anderen Bestimmungen abzuleitende Dokumentationspflichten

70 Aus den Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO ergibt sich die Verpflichtung des Verantwortlichen, die Einhaltung der in Art. 5 Abs. 1 DSGVO normierten Datenschutzgrundsätze auf Verlangen der Datenschutzaufsicht nachweisen zu können. Wie bereits erläutert, werden die in Art. 5 Abs. 1 DSGVO normierten Datenschutzgrundsätze der

- Rechtmäßigkeit,
- Verarbeitung nach Treu und Glauben,
- Transparenz,
- Zweckbindung,

95 So auch *Klug*, in: Gola (Hrsg.), DS-GVO, 2017, Art. 30 Rn 14; *Lepperhoff*, in: Lepperhoff/Müthlein (Hrsg.), Leitfaden zur Datenschutz-Grundverordnung, 2017, S. 75; *Martini*, in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 30 Rn 29; *Bertermann*, in: Ehmann/Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2017. Art. 30 Rn 5.

96 In diesem Sinne auch *Martini*, in Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 30 Rn 32.

- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung sowie
- Integrität und Vertraulichkeit

in den nachfolgenden Artikeln der Verordnung näher konkretisiert und ausgestaltet. Die Einhaltung der daraus resultierenden Verpflichtungen hat der Verantwortliche nachzuweisen. Es folgen zwar keine konkret normierten Dokumentationspflichten, gleichwohl aber entsprechende Dokumentationsempfehlungen an den Verantwortlichen.

71 So ist – mit Blick auf den Grundsatz der Rechtmäßigkeit der Verarbeitung – die **Dokumentation** der für einzelne Verarbeitungsschritte herangezogenen **Rechtsgrundlagen** zu empfehlen. Da die DSGVO ihrerseits keine abstrakte, sondern eine konkrete, auf das einzelne Datum und seine Verarbeitung bezogene Rechtsgrundlage fordert, sollte die Dokumentation auch den einzelnen Verarbeitungsvorgang erfassen und – im Falle entsprechender Rückfragen durch die betroffene Person oder die Aufsichtsbehörde – nachweisbar machen. Soweit ein Verantwortlicher – was regelmäßig der Fall sein dürfte – weitgehend gleichlaufende Verarbeitungen vollzieht, die sich lediglich in Bezug auf die jeweils betroffene Person unterscheiden, sollte es als ausreichend angesehen werden, die entsprechenden Verarbeitungsschritte und -szenarien zu gruppieren und – ähnlich der Vorgehensweise im Rahmen einer Datenschutzfolgenabschätzung nach Art. 35 DSGVO – die den Verarbeitungsgruppen jeweils zugrunde liegenden Rechtsgrundlagen zu dokumentieren.[97] Gleiches gilt für die Berücksichtigung des Grundsatzes der Verarbeitung nach Treu und Glauben.

72 Nicht nur aus Art. 5 Abs. 1 lit a.) DSGVO, sondern insbesondere aus Art. 12 DSGVO folgt die Verpflichtung, der betroffenen Person alle **Informationen und Mitteilungen** zur Verarbeitung personenbezogener Daten **leicht zugänglich** und **verständlich** und in **klarer und einfacher Sprache** zugänglich zu machen. Unbeschadet des Umstandes, dass die Übermittlung derartiger Informationen im Einzelfall über eine Kopie der an den Betroffenen übermittelten Information nachgewiesen werden kann, empfiehlt sich in der Praxis – je nach Unternehmensgröße – ggf. zusätzlich die Erarbeitung entsprechender Informationsstrukturen und -leitlinien, etwa im Rahmen von (schriftlich verfassten) Dienstanweisungen.

73 Hinsichtlich des Nachweises der **Zweckbindung** jeder Datenverarbeitung kann auf die Ausführungen zu Art. 25 DSGVO (siehe Rdn 41 ff.) verwiesen und empfohlen werden, auch die jeweiligen Zweckbestimmungen, denen ein Datum im gewöhnlichen Verarbeitungsverlauf eines Verantwortlichen dienen kann, dem Einzeldatum als Metainformation anzuhängen. Hierüber ließe sich dann, im Sinne der Umsetzung des Datenschutzes durch Technik, auch die Verarbeitung des Datums für andere Zwecke bereits systemisch unterbinden.

74 Der Nachweis der Einhaltung des Grundsatzes der Minimierung der Datenverarbeitung lässt darüber hinaus die schriftliche Fixierung eines **Sperr- und Löschkonzeptes** sinnvoll erscheinen, aus dem Fristen für die Löschung oder regelmäßige Überprüfung vorhandener Daten(bestände) ebenso

97 Werden z.B. in einem Inkassounternehmen zur Erfüllung der Erstinformationspflichten aus § 11a RDG regelmäßig Name, Vorname, Adresse, Vertragsdatum und Forderungshöhe einer betroffenen Person verarbeitet, kann dieser Verarbeitungsschritt einheitlich beschrieben und der Rechtgrundlage in Art. 6 Abs. 1 lit. c) DSGVO [Erfüllung einer rechtlichen Verpflichtung] zugeordnet werden. Es geht in diesem Sinne darum, die Verarbeitungsprozesse im Unternehmen zu erfassen, was ohnehin in jedem Unternehmen nützlich sein sollte. Diese zu gruppieren und entsprechenden Rechtsgrundlagen zuzuordnen. Dies kann – mit Blick auf die Umsetzung des Datenschutz durch Technik – sicherlich auch softwareseitig erfolgen, beispielsweise indem die Rechtsgrundlagen die einer Verarbeitung zugrunde liegen können, dem jeweiligen personenbezogenen Datum als Metainformationen dauerhaft beigefügt werden.

ersichtlich werden, wie die Kriterien, denen die Festlegung und regemäßige Überprüfung von Speicherfristen folgt.

Mit Blick auf das Erfordernis der Aktualität und Richtigkeit von Daten sollte ein entsprechendes **Prüfkonzept** erarbeitet und dokumentiert werden. Da personenbezogene Daten so verarbeitet werden sollen, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können und Daten zudem gegen Verfälschung, Ergänzung und Beschränkung durch Dritte zu sichern sind, empfiehlt sich die Etablierung und Fixierung eines entsprechenden **Sicherheitskonzeptes** durch den Verantwortlichen. 75

Weiterhin erfordern die Informationen, die der betroffenen Person zu erteilen sind, im Einzelfall eine entsprechende Dokumentation. So sollten Maßnahmen etabliert werden, über die sichergestellt werden kann, dass sowohl die Herkunft eines Datums, als auch seine (potentiellen) Empfänger durch den Verantwortlichen dokumentiert werden. Anders als im Rahmen der allgemeinen Information nach Art. 13 und 14 DSGVO ist der betroffenen Person – auf Verlangen – nämlich nicht nur Auskunft über die mögliche Quellen und Empfänger eines Datums, sondern die konkreten Quellen und Empfänger zu erteilen. Sind selbige nicht (sinnvollerweise ebenso als Metainformation dem Datum angeheftet) vorhanden, kann der Verantwortliche seiner Auskunftspflicht nicht vollumfänglich nachkommen und riskiert insoweit das Vorliegen eines Datenschutzverstoßes. Insoweit empfiehlt sich unter Berücksichtigung von Art. 13, 14 DSGVO die Dokumentation nachfolgender Gesichtspunkte: 76

- die **Zwecke der Datenverarbeitung**
- die **berechtigten Interessen des Verantwortlichen**
- die **Empfänger**
- die **Dauer der Speicherung**
- das Vorliegen einer **Einwilligung**
- die **Quelle** aus der die personenbezogenen Daten stammen
- das Kriterium der **öffentlich zugänglichen Quelle**

Mit Blick auf Art. 7 Abs. 1 DSGVO, ergibt sich die Verpflichtung zur Dokumentation einer Einwilligung in die Datenverarbeitung. Art. 22 DSGVO bedingt die Erforderlichkeit der Dokumentation der zwingenden schutzwürdigen Gründe der weiteren Verarbeitung. 77

Schließlich ergeben sich Dokumentationserfordernisse aus

- Art. 29 DSGVO, der normiert dass sowohl der Auftragsverarbeiter, als auch jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen

und

- Art. 32 DSGVO, der normiert, dass der Verantwortliche und der Auftragsverarbeiter Schritte zu unternehmen haben, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Auch derartige Weisungen sollten entsprechend dokumentiert werden.[98]

98 Ein guter Überblick über mögliche weitere Dokumentationsgegenstände nach der DSGVO findet sich auch bei *Lepperhoff*, in: Lepperhoff/Müthlein (Hrsg.), Leitfaden zur Datenschutz-Grundverordnung, 2017, S. 67 f.