

3 Personenbezogene Daten

Sowohl Art. 1 Abs. 1 DSGVO und Art. 1 Abs. 1 DSRL als auch § 1 Abs. 1 BDSG in der neuen und der alten Fassung wie auch § 35 SGB I i.V.m. § 67 Abs. 1 SGB X a.F. sowie § 67 Abs. 2 SGB X n.F. nennen als Regelungsgegenstand des Datenschutzrechts die Verarbeitung von personenbezogenen Daten. Sind die Daten nicht personenbezogen, greifen die Datenschutzregeln nicht.

3.1 Personenbezug

Kapitel 3.1 beantwortet die Frage 4.1 Satz 4. Diese lautet:

Von Interesse ist hier, ob die EU-DSGVO eher das Konzept eines „absoluten“ oder eines „relativen Personenbezugs“ unterstützt.

Ohne zu klären, wie sich der Begriff des Personenbezugs bestimmt, lassen sich keine sinnvollen Aussagen zu anonymen und pseudonymen Daten treffen. Die Antwort auf die Frage 4.1 Satz 4 ist daher grundlegend für die Antworten zu den Fragen 4.1, 4.3 und 4.4 und wird daher vor der Beantwortung dieser Fragen im Folgenden gesondert erarbeitet.

Aufgrund des Anwendungsvorrangs der Datenschutz-Grundverordnung ist die Definition personenbezogener Daten in Art. 4 Nr. 1 DSGVO entscheidend:

Danach sind personenbezogene Daten

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person‘) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Die Datenschutz-Grundverordnung führt damit weitgehend die Definition des Art. 2 lit. a) DSRL fort. Diese lautet:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck ‚personenbezogene Daten‘ alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person‘); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“.

Der Unterschied besteht nur in der Ersetzung der Worte „bestimmt oder bestimmbar“ durch die Worte „identifiziert oder identifizierbar“ und der Ergänzung der Beispiele um „Namen“, „Standortdaten“ und „Online-Kennung“ sowie der Identitäten um die „genetische“ Identität.

Der Unterschied zwischen „bestimmt oder bestimmbar“ und „identifiziert oder identifizierbar“ betrifft nur die jeweils deutschen Übersetzungen des englischen „identified or identifiable“. In der englischen Fassung des Art. 2 lit. a) DSRL und des Art. 4 Nr. 1 DSGVO heißt es übereinstimmend „identified or identifiable“. In dieser Hinsicht sind also die Datenschutz-Grundverordnung und die Datenschutz-Richtlinie identisch.²⁷ In der deutschen Fassung wurden diese Worte 1995 mit den Worten „bestimmt oder bestimmbar“ und 2017 durch die Worte „identifiziert oder identifizierbar“ übersetzt. Die zusätzlichen Beispiele in Art. 4 Nr. 1 DSGVO gelten auch für Art. 2 lit. a) DSRL,²⁸ ebenso wie die „genetische“ Identität auch von Art. 2 lit. a) DSRL erfasst ist. Sie werden nun in Art. 4 Nr. 1 DSGVO explizit im Verordnungstext genannt.

Aus alledem ist davon auszugehen, dass die Definitionen in Art. 4 Nr. 1 DSGVO und Art. 2 lit. a) DSRL in den wesentlichen Merkmalen²⁹ inhaltlich identisch

²⁷ Ebenso Laue/Nink/Kremer 2016, § 1 Rn. 12; Herbst, NVwZ 2016, 902 (903): nur unwesentliche Abweichungen.

²⁸ S. z.B. Laue/Nink/Kremer 2016, § 1 Rn. 14.

²⁹ Insbesondere wurde nach dem bisher geltenden Datenschutzrecht keine namentliche Identifizierung verlangt – s. z.B. Art. 29 Datenschutzgruppe, WP 136, 14; Dammann, in: Simitis, BDSG, § 3 Rn. 22.

sind.³⁰ Insbesondere hinsichtlich des Merkmals „bestimmt oder bestimmbar“ und „identifiziert oder identifizierbar“ stimmen sie überein. Da die gleichlautenden Definitionen der personenbezogenen Daten in § 3 Abs. 1 BDSG a.F. und § 67 Abs. 1 SGB X die Definition in Art. 2 lit. a) DSRL umsetzen, ist ihnen trotz eines etwas anderen Wortlauts – unionsrechtskonform – der gleiche Begriff der personenbezogenen Daten zu unterlegen wie in Art. 2 lit. a) DSRL. Zwar darf das Unionsrecht nicht aus dem Blickwinkel des Rechtsverständnisses eines Mitgliedstaats ausgelegt werden.³¹ Doch können die Auslegungserkenntnisse zur Datenschutz-Richtlinie auf die Datenschutz-Grundverordnung übertragen werden, die ihre Kontinuität zu dieser Richtlinie ausdrücklich in ihrem Erwägungsgrund 9 betont. Aber auch Literatur und Rechtsprechung zur Definition der personenbezogenen Daten in § 3 Abs. 1 BDSG a.F. und § 67 Abs. 1 SGB X a.F., die die Definition in Art. 2 lit. a) DSRL umsetzen, können trotz eines etwas anderen Wortlauts zum Verständnis des Art. 4 Nr. 1 DSGVO herangezogen werden,³² wenn der besondere unionsrechtliche Zusammenhang beachtet wird. Dies wird im Folgenden ergänzend zur einschlägigen Literatur und Rechtsprechung zur Datenschutz-Grundverordnung auch geschehen.

3.1.1 Bedeutung des Personenbezugs

Das Datenschutzrecht geht davon aus, dass von einer Datenverarbeitung Risiken für das Grundrecht auf den Datenschutz nach Art. 8 GRCh und für das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nur dann ausgehen können, wenn die Daten mit einer bestimmten Person in Verbindung gebracht werden können.³³ Daher greift das Datenschutzrecht als Gefahrenabwehrrecht erst und nur dann, wenn die zu verarbeitenden Daten einen Personenbezug haben und damit auf eine bestimmte Person verweisen.³⁴ Aus diesem Grund ist der Personenbezug der zu verarbeitenden Daten der zentrale Begriff, der über die Anwendung des Datenschutzrechts entscheidet.

Der Personenbezug der Daten ist entscheidend für den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung, aber auch der anderen genannten Datenschutzregelungen. Werden personenbezogene Daten verarbeitet, gilt auch der persönliche und räumliche Anwendungsbereich. Die Vorschriften der Datenschutz-Grundverordnung gelten dann für alle Verantwortlichen und Auftragsverarbeiter. Nach den Legaldefinitionen in Art. 4 Nr. 7

30 S. auch *Laue/Nink/Kremer* 2016, § 1 Rn. 13; *Karg*, DuD 2015, 520 (521); *Brink/Eckhardt*, ZD 2015, 205; *Klar/Kühling*, in: *Kühling/Buchner*, Art. 4 Nr. 1 Rn. 2; *Klabunde*, in: *Ehmann/Selmayr*, Art. 4 Rn. 6; *Ernst*, in: *Paal/Pauly*, Art. 4 Rn. 3; *Ziebarth*, in: *Sydow*, Art. 4 Rn. 7; *Krügel*, ZD 2017, 455 (455f.).

31 S. genau für diese Frage *Hofmann/Johannes*, ZD 2017, 221f. m.w.N.

32 S. z.B. *Klar/Kühling*, in: *Kühling/Buchner*, Art. 4 Nr. 1 Rn. 20.

33 S. hierzu kritisch *Roßnagel/Scholz*, MMR 2000, 721 (727f.); *Roßnagel* 2007, 185ff.

34 Zur Notwendigkeit, die Gefahrenabwehr um eine Risikoversorge zu ergänzen s. z.B. *Roßnagel/Gemmin/Jandt/Richter* 2016, 125f., 137.

und 8 DSGVO sind dann alle natürlichen oder juristischen Personen, die personenbezogene Daten allein oder im Auftrag verarbeiten, Adressaten der Datenschutzregelungen. Es wird nach Art. 3 DSGVO jede Datenverarbeitung von den Datenschutzregelungen erfasst, die im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt oder die in Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten oder ihr Verhalten in der Union zu beobachten.

Nur wenn personenbezogene Daten verarbeitet werden, gelten die datenschutzrechtlichen Grundsätze der Datenverarbeitung nach Art. 5 DSGVO. Nur bei Personenbezug der Daten ist eine Legitimation für die Verarbeitung der Daten erforderlich, die entweder in einer Einwilligung der betroffenen Person oder in einer gesetzlichen Erlaubnis zur Datenverarbeitung liegen kann. Nur wenn ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten verarbeitet, gelten für sie die spezifischen datenschutzrechtlichen Pflichten.³⁵ Nur bei einem Bezug der Daten auf die betroffene Person kann diese ihre Rechte und Rechtsbehelfe geltend machen. Nur die Verarbeitungen von personenbezogenen Daten unterliegen der Aufsicht durch die zuständige Aufsichtsbehörde und begründen deren Aufgaben und Befugnisse.³⁶ Nur wenn personenbezogene Daten verarbeitet werden, kann ein Verstoß gegen datenschutzrechtliche Pflichten die drakonischen Sanktionen der Datenschutz-Grundverordnung auslösen.³⁷

Entscheidend dafür, ob alle diese Rechte und Pflichten, Aufgaben und Befugnisse gelten, ist der Personenbezug der verarbeiteten Daten. Nur die mit ihnen verbundenen Risiken begründen die Notwendigkeit, den Verantwortlichen und die Auftragsverarbeiter den Regelungen des Datenschutzrechts zu unterwerfen.

3.1.2 Identifizierung durch Daten

Nach Art. 4 Nr. 1 DSGVO sind Daten personenbezogen, wenn die Informationen, die den Daten entnommen werden können, „sich auf eine identifizierte oder identifizierbare natürliche Person“ beziehen.³⁸ Von einer Identifikation ist auszugehen, wenn diese sich aus den Daten selbst ergibt.³⁹ Wann eine Person im Sinn des Art. 4 Nr. 1 DSGVO „identifiziert“ ist, wird in der Verordnung nicht erläutert. Eine natürliche Person ist identifiziert, wenn sie sich von anderen Personen einer Gruppe ohne Weiteres eindeutig unterscheiden lässt.⁴⁰ Wichtig ist, dass feststeht, dass sich die Daten auf diese und nicht auf eine

35 S. auch *Hofmann/Johannes*, ZD 2017, 221 (222).

36 S. z.B. Roßnagel, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 41ff.

37 S. auch *Hofmann/Johannes*, ZD 2017, 221 (222).

38 S. z.B. *Klar/Kühling*, in: *Kühling/Buchner*, Art. 4 Nr. 1 Rn. 18.

39 S. z.B. *Klar/Kühling*, in: *Kühling/Buchner*, Art. 4 Nr. 1 Rn. 18.

40 Art. 29-Datenschutzgruppe, WP 136, 14; *Buchner*, in: *Taeger/Gabel*, § 3 Rn. 9.



andere Person beziehen. Die Identifikation kann über eindeutige Merkmale, wie den Namen, erfolgen. Sie kann aber auch – ohne dass der Name bekannt ist⁴¹ – allein durch bestimmte Merkmale von allen anderen Personen der relevanten Gruppe unterschieden und damit individualisiert werden.⁴² Im Ergebnis ist eine Person als identifiziert anzusehen, wenn ausreichende Informationen (gemeinsam) vorliegen, die zu einer eindeutigen Identifikation notwendig sind.⁴³ Wie Erwägungsgrund 26 DSGVO deutlich macht, spielt es keine Rolle, durch welche Mittel diese eindeutige Zuordnung erreicht wurde. Dies kann auch durch Aussondern erfolgen.⁴⁴

Eine natürliche Person ist *identifizierbar*, wenn sie gemäß Art. 4 Nr. 1 DSGVO und Art. 2a) DSRL „direkt oder indirekt identifiziert werden kann“. Es genügt die Möglichkeit.⁴⁵ Diese kann sich etwa aus der „Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen“ ergeben. Diese besonderen Merkmale können die Identifizierung einer Person ermöglichen, weil sie „Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“. Ob der Schluss von den bekannten besonderen Merkmalen auf die Identität der Person möglich ist, hängt von dem verfügbaren „Zusatzwissen“ ab, das eine Verbindung von den bekannten Daten zu der spezifischen Person herstellen kann.⁴⁶ Eine Person ist somit mit Hilfe der bekannten Daten identifizierbar, wenn weitere Kenntnisse verfügbar sind, die einen Schluss von den Daten zu einer eindeutig unterscheidbaren Person ermöglichen.⁴⁷

Wenn für die Identifizierbarkeit einer bestimmten Person durch ein Datum oder mehrere Daten das Zusatzwissen entscheidend ist, das den Schluss von den Daten zu der identifizierten Person zulässt, stellt sich die Frage, auf wessen Zusatzwissen abzustellen ist. Zu dieser Frage gibt es unterschiedliche Antworten, je nachdem, ob man sie mit Blick auf die Daten, um die es geht, oder mit Blick auf den Verantwortlichen, der die Daten verarbeitet, beantwortet. In der Literatur wird hierzu ein Meinungsstreit ausgemacht, der dadurch bestimmt ist, ob das Konzept eines „absoluten Personenbezugs“ oder das Konzept eines „relativen Personenbezugs“ verfolgt wird.⁴⁸

41 S. Husemann, in: Roßnagel 2018, § 3 Rn. 6; Karg, DuD 2015, 520 (523); für die DSRL Art. 29-Datenschutzgruppe, WP 136, 14.

42 S. z.B. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 22 – Breyer; Art. 29-Datenschutzgruppe, WP 136, 14.

43 S. Tinnefeld, in: Roßnagel 2003, Kap. 4.1 Rn. 20; Karg, ZD 2012, 257.

44 Erwägungsgrund 26 Satz 3.

45 Wie diese bestimmt wird, wird im Folgenden in der Auseinandersetzung mit der „absoluten“ und der „relativen“ Konzeption der Bestimmung des Personenbezugs ausführlich dargestellt.

46 Damann, in: Simitis, § 3 Rn. 26; Roßnagel/Scholz, MMR 2000, 723; Roßnagel, digma 2011, 161.

47 Art. 29-Datenschutzgruppe, WP 136, 15; s. hierzu auch Gola/Schomerus, § 3 Rn. 10; Roßnagel/Scholz, MMR 2000, 723.

48 Ausführliche Darstellung des Streitstands Bergt, ZD 2015, 365; Haase 2015, 259ff.; Brink/Eckhardt, ZD 2015, 205; Herbst, NVwZ 2016, 902.

3.1.3 Konzept des „absoluten Personenbezugs“

Zum einen wird eine Rechtsauffassung identifiziert, die in unterschiedlicher Weise und mit unterschiedlicher Begründung davon ausgeht, dass das absolut vorhandene Wissen berücksichtigt werden muss. Nimmt man diese Meinung ernst, kommt es auf das gesamte (weltweit) theoretisch verfügbare Zusatzwissen an: Wenn ein Datum von irgendjemandem einer bestimmten Person zugeordnet werden kann, ist es personenbezogen. Danach ist der Personenbezug absolut, allein vom Datum her zu bestimmen. Er gilt unabhängig davon, ob der Verantwortliche über das notwendige Zusatzwissen verfügen kann oder sicher davon ausgeschlossen ist.⁴⁹

Allein aus dem Wortlaut lässt sich weder bei Art. 4 Nr. 1 DSGVO noch bei Art. 2 lit. a DSRL oder § 3 Abs. 1 BDSG oder § 67 Abs. 1 SGB X a.F. oder § 67 Abs. 2 SGB X-neu ein Hinweis auf einen relativen oder einen absoluten Ansatz ableiten. Da der Wortlaut der neuen und der bisherigen Fassungen dieser Vorschriften in den entscheidenden Punkten identisch ist,⁵⁰ können sie gemeinsam erörtert werden und die Rechtsprechung und die Literatur zur Datenschutzrichtlinie und zum bisherigen Bundesdatenschutzgesetz können auch zur Auslegung des gleichen Wortlauts in Art. 4 Nr. 1 DSGVO genutzt werden.

Die Vertreter eines absoluten Personenbezugs beziehen sich bisher auf Erwägungsgrund 26 der Datenschutzrichtlinie. Dieser lautet:

„(26) Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist ...“

Aus Satz 2, der für die Bestimmbarkeit fordert, nicht nur alle Mittel der verantwortlichen Stelle zu berücksichtigen, sondern auch die Mittel, die „von einem Dritten eingesetzt werden könnten“, schließen sie, dass die Richtlinie und mit ihr das deutsche Datenschutzrecht es ausreichen lassen, wenn irgendein Dritter über das erforderliche Zusatzwissen verfügt.⁵¹ Aus Erwägungsgrund 26 DSRL lässt sich jedoch keine Aussage darüber ableiten, ob im Sinn der absoluten Sichtweise alle beliebigen Dritten gemeint sind oder im Sinn

49 S. z.B. *Pahlen-Brandt*, DuD 2008, 34ff.; *Pahlen-Brandt*, K & R 2008, 289; *Breyer*, ZD 2014, 400 (402ff.); *Schaar* 2002, Rn. 168ff. vor allem für IP-Adressen; Beschluss des Düsseldorf-Kreises vom 26./27.11.2009 in Bezug auf IP-Adressen; nicht eindeutig *Weichert*, in: Däubler u.a., § 3 Rn. 13, 15; *LG Berlin*, K&R 2007, 603; *VG Wiesbaden*, MMR 2009, 432; für ein faktisch-absolutes Verständnis *Herbst*, NVwZ 2016, 902 (905); *Bergt*, ZD 2015, 365 (369f.).

50 S. ausführlich Kap. 3.1.

51 *Pahlen-Brandt*, DuD 2008, 38.

der relativen Sichtweise nur solche Dritte, auf deren Zusatzwissen die verantwortliche Stelle zurückgreifen kann.⁵²

Dennoch werden für einen „objektiven Beurteilungsmaßstab“⁵³ auch die „europäischen Datenschutzbehörden“ herangezogen: Sie sollen im Arbeitspapier 136 der Art. 29-Datenschutzgruppe zum Begriff personenbezogene Daten⁵⁴ im Anschluss an Satz 2 des Erwägungsgrunds 26 DSRL einer absoluten Sichtweise folgen.⁵⁵ Diese „europäische Betrachtungsweise“ wird einer deutschen Position gegenübergestellt und es wird gefragt, wie lange sich diese deutsche Besonderheit⁵⁶ ihr noch entziehen könne.⁵⁷

3.1.4 Konzept des „relativen Personenbezugs“

Die herrschende Meinung geht dagegen davon aus, dass nur das Zusatzwissen, das die verantwortliche Stelle hat oder über das sie verfügen kann, entscheidend sein kann. Danach ist der Personenbezug relativ, nämlich jeweils von der verantwortlichen Stelle aus zu bestimmen, deren Datenumgang zu beurteilen ist.⁵⁸ Ist eine Person durch das Zusatzwissen einer verantwortlichen Stelle identifizierbar, kann dies bei einer anderen verantwortlichen Stelle, die über weniger Zusatzwissen verfügt, nicht so sein. Das Zusatzwissen und damit auch der Personenbezug sind eben vom Verwendungskontext der Daten und dem verfügbaren Zusatzwissen einer jeden verantwortlichen Stelle abhängig.⁵⁹

Für den relativen Begriff des Personenbezugs sprechen vor allem systematische und teleologische Gründe, aber auch Überlegungen der Rechtsfolgenbewertung.⁶⁰ Systematisch und funktional besteht ein enger Bezug des Begriffs „per-

52 Ebenso *Sachs*, CR 2010, 549f.

53 So nennen *Stiernerling/Hartung*, CR 2012, 63f. das Konzept des „absoluten“ Personenbezugs.

54 Art. 29-Datenschutzgruppe, WP 136, 14ff.

55 *Stiernerling/Hartung*, CR 2012, 63f.; *Karg*, ZD 2012, 256.

56 Gemeint ist damit das Konzept des relativen Personenbezugs. Dagegen wird für das Konzept des „absoluten“ Personenbezugs beansprucht, dass nur dieses der europäischen Konzeption der Datenschutzrichtlinie entspreche.

57 *Stiernerling/Hartung*, CR 2012, 63f.

58 Für die DSRL und das BDSG a.F. s. aus der Rspr. z.B. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 49 – Breyer; *BGH*, NJW 2017, 2416 Rn. 24ff.; *BGH*, ZD 2015, 80, Rn. 32; *BGH*, MMR 2011, 341 (344); *OLG Hamburg*, MMR 2011, 281ff.; *OLG München*, ZD 2011, 182; *LG Berlin*, K&R 2000, 603; *LG Berlin*, ZD 2013, 618; aus der Lit. s. z.B. *Dammann*, in: Simitis, § 3 Rn. 32; *Gola/Schomerus*, § 3 Rn. 10; *Tinnefeld*, in: Roßnagel 2003, Kap. 4.1 Rn. 22; *Schaffland/Wiltfang*, § 3 Rn. 17; *Bizer/Hornung*, in: Roßnagel 2013, § 12 TMG Rn. 44, *Kroschwald* 2015, 58, 69; *Roßnagel/Banzhaf/Grimm* 2003, 150f.; *Nink/Pohle*, MMR 2015, 563 (565f.); *Schmitz*, in: Hoeren/Sieber, Kap. 16.2 Rn. 83f.; *Roßnagel/Pfitzmann/Garstka* 2001, 61; *Roßnagel*, *digma* 2011, 160ff.; *Roßnagel/Scholz*, MMR 2000, 721f.; *Arning/Forgó/Krügel*, DuD 2006, 700; *Voigt*, MMR 2009, 377; *Caspar*, DÖV 2009, 966; *Meyerdierks*, MMR 2009, 9; *Sachs*, CR 2010, 548; *Eckhardt*, CR 2011, 342; *Eckhardt*, CR 2015, 113 (115); *Knopp*, DuD 2015, 527 (528); *Brink/Eckhardt*, ZD 2015, 205 (207ff.); *Krüger/Maucher*, MMR 2011, 436; *Härting*, NJW 2013, 2066; *Kühling/Klar*, NJW 2013, 3611 (3615); *Kühling/Klar*, ZD 2017, 28; *Klar* 2012, 144f.; *Krügel*, ZD 2017, 455 (458f.); einschränkend *Buchner*, in: Taeger/Gabel, § 3 Rn. 13.

59 S. z.B. Art. 29-Datenschutzgruppe, WP 136, 15; *Dammann*, in: Simitis, § 3 Rn. 38; *Tinnefeld*, in: Roßnagel, Kap. 4.1 Rn. 22; *Roßnagel/Scholz*, MMR 2000, 722f.

60 Die Argumente in *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779 – Breyer, werden in Kap. 3.1.5 ausführlich zur Bestimmung des Personenbezugs in der DSGVO herangezogen.

sonenbezogene Daten“ zum Begriff der „verantwortlichen Stelle“, wie er gemäß § 3 Abs. 7 BDSG a.F. verwendet wird. § 3 Abs. 1 BDSG a.F. bestimmt den Anwendungsbereich des Datenschutzrechts und § 3 Abs. 7 BDSG a.F. den durch das Datenschutzrecht Verpflichteten. Das gemäß § 3 Abs. 1 BDSG a.F. anwendbare Datenschutzrecht richtet sich an die gemäß § 3 Abs. 7 BDSG verantwortliche Stelle. Das Datenschutzrecht muss für sie anwendbar sein. Das ist es nur, wenn die Daten, die sie erhebt, verarbeitet oder nutzt, für sie personenbezogen sind.

Auch bei genauer Lektüre des Arbeitspapiers 136 der Art. 29-Datenschutzgruppe, das Vertreter der absoluten Theorie als Hauptbeweismittel anführen, wird deutlich, dass diese Gruppe keinen absoluten, sondern einen relativen Begriff der personenbezogenen Daten vertritt. Sie sieht den Personenbezug abhängig vom jeweiligen Kontext,⁶¹ in dem die Daten verarbeitet werden, bezieht sich immer auf den „für die Verarbeitung Verantwortlichen“⁶² und stellt auf den Zweck ab, den dieser verfolgt, sowie auf die Mittel, die er vernünftigerweise einsetzen kann. Die in Satz 2 des Erwägungsgrunds 26 DSRL erwähnten „Dritten“ werden nicht so verstanden, dass es beliebige Dritte sein können, sondern Dritte, denen Daten vom Verantwortlichen übermittelt werden, Dritte, die selbst zu Verantwortlichen werden (können), oder Dritte, auf deren Zusatzwissen der Verantwortliche zurückgreifen kann.⁶³ Immer aber wird der Bezug zu einem Verantwortlichen gewahrt und gefragt, ob „der für die Verarbeitung Verantwortliche oder eine andere beteiligte Person“ über die Mittel verfügen, den Personenbezug herzustellen.⁶⁴ Ist dies dem einen Verantwortlichen möglich, einem anderen jedoch nicht, sind die Daten nur für den ersten personenbezogen.⁶⁵

Nach Art. 2 lit. a DSRL, § 3 Abs. 1 BDSG a.F. und § 67 Abs. 1 SGB X a.F. spricht also alles für ein relatives Verständnis des Personenbezugs, das auf das Zusatzwissen des Verantwortlichen abstellt, über das er verfügt oder über das er mit einem für ihn verhältnismäßigen Aufwand mobilisieren kann.⁶⁶ Der Personenbezug ist danach relativ und kann sich von Verantwortlichem zu Verantwortlichem unterscheiden.

3.1.5 Personenbezug nach der Datenschutz-Grundverordnung

Hat sich dieses Verständnis des Personenbezugs durch die Datenschutz-Grundverordnung verändert? Diese Frage wird überwiegend verneint und auch für

⁶¹ Art. 29-Datenschutzgruppe, WP 136, 15, 24.

⁶² Art. 29-Datenschutzgruppe, WP 136, 16, 18, 19, 20, 23.

⁶³ Art. 29-Datenschutzgruppe, WP 136, 18ff.

⁶⁴ Art. 29-Datenschutzgruppe, WP 136, 19, 23.

⁶⁵ Art. 29-Datenschutzgruppe, WP 136, 23.

⁶⁶ *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 – Breyer; *BGH*, NJW 2017, 2416 Rn. 24ff.;

die Datenschutz-Grundverordnung ein relativer Personenbezug angenommen.⁶⁷

3.1.5.1 Wortlaut

Der Wortlaut des Art. 4 Nr. 1 DSGVO ist hinsichtlich des zu berücksichtigenden Zusatzwissens nicht eindeutig.⁶⁸ Er stellt nur fest, dass eine natürliche Person dann als identifizierbar angesehen wird, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung identifiziert werden kann. Wer diese Zuordnung vornehmen muss oder kann, bestimmt die Definition nicht. Sie lässt damit gerade die umstrittenste Frage des Begriffs „personenbezogene Daten“ offen.

3.1.5.2 Erwägungsgründe

Die Datenschutz-Grundverordnung erläutert ihr Verständnis der personenbezogenen Daten nach Art. 4 Nr. 1 in Erwägungsgrund 26 DSGVO wie folgt:

„Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.“

67 S. z.B. Hofmann/Johannes, ZD 2017, 221; Barlag, in: Roßnagel 2017, § 3 Rn. 9; Husemann, in: Roßnagel 2018, § 3 Rn. 7; Roßnagel/Kroschwald, ZD 2014, 495 (496f.); Schantz, NJW 1841 (1843); Schantz, in: Schatz/Wolf 2017, Rn. 279ff.; Marnau, DuD 2016, 428, (430); Kartheuser/Gilsdorf, MMR-Aktuell 2016, 382533; Moos/Rothkegel, MMR 2016, 845 (847); Laue/Nink/Kremer 2016, § 1 Rn. 116; Ziebarth, in: Sydow, Art. 4 Rn. 37; Gola, in: ders., Art. 4 Rn. 17; Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 26; Krügel, ZD 2017, 455 (458f.); a.A. Buchner, DuD 2016, 155 (156); widersprüchlich Albrecht/Iotzo 2017, Teil 3 Rn. 3, die eine „absolute Betrachtung“, aber zugleich eine Prüfung des Einzelfalls bei jedem Verantwortlichen fordern.

68 Ebenso Buchner DuD 2016, 155 (156); Hofmann/Johannes, ZD 2017, 221 (222).

Zwar gehören die Erwägungsgründe nicht zum verfügenden Teil der Verordnung und sind daher nicht rechtsverbindlich.⁶⁹ Jedoch geben sie die Ziele an, auf die sich die unterschiedlichen Unionsorgane, die zusammen den Unionsgesetzgeber bilden, geeinigt haben und nennen zu jeder Vorschrift die nach Art. 296 UAbs. 2 AEUV erforderliche Begründung. Auch wenn sie nicht rechtsverbindlich sind, können die Erwägungsgründe wichtige Hinweise zur Auslegung einer Vorschrift bieten. Allerdings können sie keine vom Wortlaut abweichende Auslegung rechtfertigen.⁷⁰ Der Europäische Gerichtshof nutzt regelmäßig die Erwägungsgründe zur Auslegung von Vorschriften des Unionsrechts.⁷¹

Erwägungsgrund 26 Satz 3 DSGVO könnte im Sinn eines absoluten Personenbezugs verstanden werden, wenn danach „alle Mittel berücksichtigt werden“ sollen, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“.⁷² Allerdings stellt dieser Satz nicht auf die absolute Möglichkeit einer Identifizierung ab, sondern bezieht sich auf die Wahrscheinlichkeit, dass der konkrete Verantwortliche oder eine andere konkrete Person, die über die Daten verfügt, die Mittel nutzen wird. Die Formulierung „genutzt werden“ ist ganz konkret und stellt auf die relativen Möglichkeiten des Verantwortlichen ab. Die Identifizierbarkeit hängt hier erkennbar vom gegebenen Kontext ab.⁷³ Nicht in das Konzept des absoluten Personenbezugs passt es auch, dass die Bestimmung auf den Verantwortlichen abstellt. Für dieses Konzept ist es nämlich unerheblich, wer die Identifizierung vornehmen kann.

Für die Feststellung der Wahrscheinlichkeit einer Identifizierung sollen nach Satz 4 des Erwägungsgrunds 26 DSGVO „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden“. Auch sollen die „zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen“ berücksichtigt werden. Die Bestimmung der Wahrscheinlichkeit, dass verfügbare Mittel zur Identifizierung einer natürlichen Person genutzt werden, und die Aufforderung, die Kosten und den Aufwand der Identifizierung sowie die verfügbare Technologie zu berücksichtigen, sprechen gegen das Konzept eines absoluten Personenbezugs.⁷⁴ Denn diese wären dafür irrelevant. Vielmehr kann die zu bestimmende Wahrscheinlichkeit von Person zu Person unterschiedlich sein.⁷⁵ Dies gilt sowohl für das Interesse, die betroffene Person zu identifizieren, als auch

69 *EuGH*, Urteil vom 19.11.1998 – C 162/97 – ECLI:EU:C:1998:554, Rn. 54 – Nilsson u.a.; *EuGH*, Urteil vom 24.11.2005 – C 316/04 – ECLI:EU:C:2005:716, Rn. 32 – Deutsches Milchkontor.

70 *EuGH*, Urteil vom 19.11.1998 – C 162/97 – ECLI:EU:C:1998:554, Rn. 54 – Nilsson u.a.

71 *EuGH*, Urteil vom 13.5.2014 – C 131/12 – ECLI:EU:C:2014:317, Rn. 54 – Google Spain und Google.

72 So z.B. *Buchner*, DuD 2016, 155 (156).

73 *Husemann*, in: Roßnagel 2018, § 3 Rn. 7.

74 So im Ergebnis auch *Hofmann/Johannes*, ZD 2017, 221 (224f.); *Kroschwald* 2015, 58.

75 S. auch *Hofmann/Johannes*, ZD 2017, 221 (224).

für die jeweiligen Mittel zur Identifizierung, über die der Verantwortliche verfügen kann. Die individuelle Wahrscheinlichkeit der Identifizierung kann jedenfalls nicht allgemein danach bestimmt werden, dass irgendwo auf der Welt ausreichende Mittel zur Verfügung stehen, um die betroffene Person zu identifizieren.⁷⁶ Erwägungsgrund 26 DSGVO spricht daher für ein relatives Verständnis des Personenbezugs.

Eindeutig geht Erwägungsgrund 30 DSGVO von einem relativen Personenbezug aus. Dieser geht davon aus, dass natürliche Personen nur „unter Umständen“ Online-Kennungen „wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet“ werden können. Dies ist dann der Fall, wenn die IP-Adressen und Cookie-Kennungen „in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren“. Nach diesem Erwägungsgrund gibt es also Verantwortliche, für die diese Daten personenbezogen sind, weil sie sie mit eindeutigen Kennungen kombinieren können, und andere Verantwortliche, für die sie mangels dieses Zusatzwissens nicht personenbezogen sind.⁷⁷

3.1.5.3 Systematik

Die Verwendung des Begriffs der personenbezogenen Daten in anderen Vorschriften oder die Nichtanwendung der Datenschutz-Grundverordnung auf bestimmte Daten können Rückschlüsse auf das Verständnis des Begriffs personenbezogene Daten in Art. 4 Nr. 1 DSGVO bieten.

Anonyme Daten werden von der Datenschutz-Grundverordnung – im Gegensatz zu § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8 SGB X a.F. – in keiner Vorschrift geregelt.⁷⁸ Dies erfolgt nur indirekt in Erwägungsgrund 26 Satz 5 DSGVO, der darlegt, dass anonyme Daten von der Verordnung nicht erfasst werden. Dieser Ausschluss anonymer Daten aus dem Anwendungsbereich der Verordnung in Erwägungsgrund 26 Satz 5 DSGVO stützt den Standpunkt, von einem relativen Personenbezug auszugehen. Müsste man nämlich von einem absoluten Verständnis des Personenbezugs ausgehen, gäbe es so gut wie keine anonymen Daten, da es irgendjemandem nahezu immer möglich ist, den Personenbezug herzustellen, sodass anonyme Daten nie aus dem Anwendungsbereich der Verordnung ausgeschlossen wären.⁷⁹

⁷⁶ S. z.B. Kroschwald 2015, 58.

⁷⁷ S. Schantz, NJW 2016, 1841 (1843); Brink/Eckhardt, ZD 2015, 205 (209).

⁷⁸ S. zu anonymen Daten näher Kap. 3.2.

⁷⁹ Roßnagel/Kroschwald, ZD 2014, 495 (497); Herbst, NVwZ 2016, 902 (905); Barlag, in: Roßnagel 2017, § 3 Rn. 9; Hofmann/Johannes, ZD 2017, 221 (223); Kühling/Klar, NJW 2013, 3611 (3616); Nink/Pohle, MMR 2015, 563 (565f.); Eckart, CR 2015, 113 (115).

„Pseudonymisierung“ von personenbezogenen Daten definiert Art. 4 Nr. 5 DSGVO so, dass personenbezogene Daten in einer Weise verarbeitet werden, dass sie ohne Hinzuziehung zusätzlicher Informationen „nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“.⁸⁰ Soweit pseudonymisierte Daten nicht mehr einer bestimmten Person zuordenbar sind, sind sie nicht mehr personenbezogen. Der Personenbezug kann allerdings unter Hinzuziehung zusätzlicher Informationen, einer Zuordnungsregel, wieder hergestellt werden.⁸¹ Daher fordert die Definition in Art. 4 Nr. 5 DSGVO vom Inhaber der zusätzlichen Informationen Sicherungsmaßnahmen, „diese zusätzlichen Informationen gesondert“ aufzubewahren sowie technische und organisatorische Maßnahmen zu ergreifen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“. Diese rechtliche Konstruktion geht von relativen Bezügen aus. Sie unterstellt, dass die personenbezogenen Daten so pseudonymisiert werden können, dass die Daten für alle außer dem Inhaber der Zuordnungsregel nicht mehr einer bestimmten Person zuordenbar sind,⁸² dem Inhaber der Zuordnungsregel aber schon.⁸³ Die Definition des Art. 4 Nr. 5 DSGVO spricht daher für einen relativen Personenbezug.⁸⁴

3.1.5.4 Sinn und Zweck

Dies entspricht auch einer teleologischen Betrachtung der Datenschutz-Grundverordnung: Der Verantwortliche nimmt durch seine Verarbeitung der Daten der betroffenen Person einen Eingriff in ihr Grundrecht auf Datenschutz und informationelle Selbstbestimmung vor.⁸⁵ Vor diesem Eingriff, sofern er rechtswidrig ist, soll das Datenschutzrecht die betroffene Person schützen – immer, aber auch nur gegenüber dem jeweils Eingreifenden. Das Datenschutzrecht soll die Gefahr einer Verletzung dieser Grundrechte ausschließen. Eine solche Gefahr kann aber von einem bestimmten Verantwortlichen nur ausgehen, wenn er zumindest die Möglichkeit hat, die Daten der betroffenen Person zuzuordnen. Wenn diese Zuordnung ausgeschlossen ist, dann ist auch die Gefahr einer Grundrechtsverletzung durch diesen Verantwortlichen ausgeschlossen. Für das Datenschutzrecht besteht dann kein Schutzauftrag.

Das Grundrecht auf Datenschutz soll – ebenso wie das Grundrecht auf informationelle Selbstbestimmung⁸⁶ – den betroffenen Personen gewährleisten,

80 S. zu pseudonymen Daten ausführlich Kap. 3.3.

81 S. Roßnagel/Scholz, MMR 2000, 721ff.

82 S. hierzu näher Kap. 3.3.1.

83 Daher bleiben die Daten nach Erwägungsgrund 26 Satz 2 DSGVO für alle, die über die zusätzlichen Informationen verfügen können, personenbezogen.

84 Ebenso Hofmann/Johannes, ZD 2017, 221 (222f.); Marnau, DuD 2016, 428 (430).

85 S. ausführlich Roßnagel/Pfitzmann/Garstka 2002, 46ff.

86 Zum Verhältnis zwischen dem Grundrecht auf Datenschutz und dem Grundrecht auf informationelle Selbstbestimmung s. z.B. Masing, NJW 2012, 2305ff.; Danwitz, DuD 2015, 581ff.; Geminn/Roßnagel, JZ 2015, 703ff.



dass sie immer „wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.⁸⁷ Dies ist die Voraussetzung, damit sie das Wissen ihres Gegenübers über ihre Situation einschätzen können. Nur dann sind sie frei, sich diesem Wissen entsprechend zu entscheiden und zu verhalten. Für dieses Ziel der informationellen Selbstbestimmung und des Datenschutzes ist also entscheidend, was jeweils derjenige, der die Daten des Betroffenen verarbeitet, über ihn weiß. Die normativen Anforderungen der informationellen Selbstbestimmung sollen somit eine soziale Beziehung gestalten. Sie gewährleisten Transparenz und Freiheit der Selbstbestimmung jeweils gegenüber dem Verantwortlichen. Wer diese Freiheit nicht bedroht, weil er die Daten nicht in einer Beziehung zum Betroffenen nutzen kann, muss die Anforderungen der informationellen Selbstbestimmung und des Datenschutzes nicht erfüllen. Diesem Schutzziel entspricht ein relatives Verständnis des Begriffs „personenbezogene Daten“, nicht ein absolutes.

Umgekehrt betrachtet, ist die Anwendung des Datenschutzrechts mit seinem Grundsatz, dass es dem Verantwortlichen nicht erlaubt, Daten der betroffenen Person zu verarbeiten, solange er hierfür keine Einwilligung der betroffenen Person oder keine Erlaubnis eines Rechtsetzers hat, ein Eingriff in die Grundrechte des Verantwortlichen aus Art. 5 Abs. 1 und 3, 12 Abs. 1 und 2 Abs. 1 GG⁸⁸ sowie Art. 11, 13, 15 und 16 GrCh. Dieser Eingriff ist nur gerechtfertigt, wenn er geeignet, erforderlich und zumutbar ist, um eine Gefahr für das Grundrecht auf Datenschutz nach Art. 8 GRCh und auf informationelle Selbstbestimmung des Betroffenen nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abzuwehren.⁸⁹ Nach der absoluten Sichtweise muss der Verantwortliche diesen Grundrechtseingriff jedoch hinnehmen, auch wenn von der Datenverarbeitung in keiner Weise eine Gefahr für die informationelle Selbstbestimmung und den Datenschutz der betroffenen Person ausgehen kann – weil er die Daten ihr nicht zuordnen kann.⁹⁰ In diesem Fall ist der Eingriff in die Grundrechte des Verantwortlichen aber weder geeignet noch erforderlich noch ihm zumutbar.⁹¹

Die absolute Betrachtungsweise würde sogar dazu führen, dass Verantwortliche, die ein bestimmtes Datum verarbeiten, datenschutzrechtliche Pflichten erfüllen müssen, wenn auch nur eine einzige Stelle auf der Welt in der Lage sein könnte, das Datum einer bestimmten Person zuzuordnen. Es gibt keinen Grund, warum deren Wissen zulasten aller anderen Verantwortlichen wirken und bei diesen Grundrechtseingriffe begründen sollte.⁹² Im Gegenteil verstößt

87 S. *BVerfGE* 65, 1 (43).

88 S. z.B. *Roßnagel/Pfitzmann/Garstka* 2001, 48ff.

89 S. z.B. *Buchner*, in: *Täger/Gabel*, § 3 Rn. 12f.; *Stiernerling/Hartung*, CR 2012, 64.

90 Dass das *BVerfGE* 65, 1 (46) feststellt, dass es unter den Bedingungen der modernen Datenverarbeitung „kein harmloses“ Datum gibt, begründet zwar ein Schutzbedürfnis der betroffenen Person bezogen auf die Verarbeitung aller personenbezogenen Daten, aber nicht einen Grundrechtseingriff durch alle Verantwortlichen – insbesondere, wenn diese keinen Personenbezug herstellen können.

91 Im Ergebnis ebenso *Hofmann/Johannes*, ZD 2017, 221 (225).

92 S. *BGH*, ZD 2015, 80, Rn. 28; *Brink/Eckhardt*, ZD 2015, 205 (209).

eine solche Sichtweise gegen das Bestimmtheitsgebot, weil die Anwendbarkeit des Datenschutzrechts davon abhinge, ob irgendjemand weitere Kenntnisse hat, ohne dass der Verantwortliche dies wissen oder beeinflussen kann.⁹³ Auch wäre der Verantwortliche, der den Bezug zur betroffenen Person gar nicht kennt, nicht in der Lage, seine Pflichten zur Information, zur Auskunft, zur Berichtigung oder zur Löschung zu erfüllen. Grundrechtskonform kann das Datenschutzrecht daher nur angewendet werden, wenn sein jeweiliger Adressat eine „Grundrechtsgefahr“ darstellt. Dies ist – mit dem relativen Begriff des Personenbezugs – nur dann der Fall, wenn der Adressat mit Hilfe seines verfügbaren Zusatzwissens die betroffene Person bestimmen kann.⁹⁴

3.1.5.5 Bedeutungslosigkeit des Theorienstreits

Das Konzept des „absoluten“ Personenbezugs ist nur dann konsequent, wenn seine Vertreter die Meinung vertreten, dass es auf das weltweit verfügbare Wissen über die Zuordnungsmöglichkeit eines Datensatzes zu einer bestimmten Person ankommt. Dies führt dazu, dass nahezu jedes Datum personenbezogen ist und jedes Datum die datenschutzrechtlichen Pflichten und Rechte, Aufgaben und Befugnisse⁹⁵ hervorruft.⁹⁶ Denn zu jedem Datum kann objektiv zumindest ein Bezug zu seinem Erzeuger, Verarbeiter, Verwender oder der betroffenen Person hergestellt werden. Dieses Ergebnis wäre – jenseits der vielen Gründe, die gegen dieses Konzept vorgetragen wurden – absurd.

Den Vertretern des Konzepts des „absoluten“ Personenbezugs kommt der Verdienst zu, darauf hingewiesen zu haben, dass unter den Bedingungen von ubiquitous computing, Internet-Tracking und Big Data jedem Datum ein Bezug zu einer natürlichen Person zukommen kann. Auch wenn die Daten statistisch aggregiert, pseudonymisiert, anonymisiert, verschlüsselt oder auf sonstige Weise ihres Bezugs zu einer bestimmten Person beraubt zu sein scheinen, ist nicht auszuschließen, dass irgendjemand zu einem späteren Zeitpunkt diesen Bezug herstellen kann.⁹⁷ Dieses Risiko besteht und ist ernst zu nehmen.⁹⁸ Dem Anliegen der Vertreter des Konzepts eines absoluten Personenbezugs muss dadurch entsprochen werden, dass alle denkbaren Möglichkeiten der Identifizierung nachgegangen wird und auch die Zukunftsdynamik Berücksichtigung findet.

93 Meyerdierks, MMR 2009, 8 (11); Ziebarth, in: Sydow, Art. 4 Rn. 39.

94 Roßnagel/Scholz, MMR 2000, 723.

95 S. Kap. 3.1.1.

96 S. z.B. Husemann, in: Roßnagel 2018, § 3 Rn. 7; Brink/Eckhardt, ZD 2015, 205 (207); Nink/Pohle, MMR 2015, 563 (565).

97 S. z.B. Bergt, ZD 2015, 365 (369); Herbst, NVwZ 2016, 902 (904); s. hierzu auch Brink/Eckhardt, ZD 2015, 205 (206).

98 Ihm müsste mit einem Konzept der Datenschutzvorsorge begegnet werden – s. z.B. Roßnagel/Scholz, MMR 2000, 721 (728ff.); Roßnagel 2007, 185ff.; Roßnagel/Geminn/Jandt/Richter 2016, 137.



Dieses Risiko begründet jedoch nicht, es jedem Datenverarbeiter zuzurechnen und ihn zur Bekämpfung dieses Risikos mit allen datenschutzrechtlichen Pflichten zur Gefahrenabwehr zu belasten. Wenn aber zwischen der NSA und Google einerseits und dem „Bäcker um die Ecke“ andererseits differenziert werden muss, dann kann nur ein Konzept rechtlich vertreten werden, das den Personenbezug risikobezogen und relativ von den Handlungsmöglichkeiten des Verarbeiters her bestimmt.⁹⁹ Mit dieser Erkenntnis löst sich der Streit zwischen den beiden Konzepten auf und wendet sich pragmatisch den Fragen zu, welches mögliche Zusatzwissen dem jeweiligen Datenverarbeiter zuzurechnen ist.

3.1.5.6 Praktisch verfügbares Zusatzwissen

Entscheidend ist also, über welches Zusatzwissen der Verantwortliche verfügen kann. Nach Erwägungsgrund 26 Satz 3 DSGVO ist für das Zusatzwissen auf die Mittel abzustellen, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“. Demnach soll anhand einer Risikoprognose geprüft werden, ob „auf Grund allgemeiner Lebenserfahrung oder auf Grund wissenschaftlicher Expertise ... mit einer Aufdeckung des Personenbezugs zu rechnen ist“.¹⁰⁰ Die „rein hypothetische Möglichkeit zur Bestimmung der Person“ reicht nicht aus, um die Person als ‚bestimmbar‘ anzusehen“.¹⁰¹ Ein Personenbezug scheidet somit aus, wenn die Wahrscheinlichkeit einer Bestimmung so gering ist, dass das Risiko praktisch vernachlässigbar ist.¹⁰² Die Bestimmbarkeit ist demnach nicht absolut zu beurteilen, sondern nach ihrer faktischen Durchführbarkeit.¹⁰³ Ob eine Angabe tatsächlich zugeordnet werden kann, ist daher eine Frage der Wahrscheinlichkeit.¹⁰⁴

Das Wahrscheinlichkeitsurteil ergibt sich aus einer Zweck-Mittel-Abwägung. Nach Erwägungsgrund 26 Satz 4 DSGVO sind hinsichtlich der eingesetzten Mittel für das Gewinnen des Zusatzwissens die „Kosten der Identifizierung und der dafür erforderliche Zeitaufwand“ sowie „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen“. Es sollen „alle objektiven Faktoren“ bedacht werden. Die Aufzählung „Kosten und Zeit“ ist nicht abschließend, sondern ausdrücklich exemplarisch. „Alle“ deutet auf eine umfassende Berücksichtigung der Aufwandsfaktoren hin.¹⁰⁵ Entscheidend für die Prognose über die Verwendung

99 Eine Modifikation des Konzepts des absoluten Personenbezugs kann es nicht geben, da es bei Einschränkungen nicht mehr absolut ist.

100 Roßnagel/Scholz, MMR 2000, S. 721 (723).

101 Art. 29-Datenschutzgruppe, WP 136, 17 zur insoweit identischen Datenschutzrichtlinie.

102 Dammann, in: Simitis, § 3 Rn. 23; Art. 29-Datenschutzgruppe, WP 136, 17.

103 So EuGH, Urteil vom 19.10.2016, C-582/14, EU:C:2016:779, Rn. 46 – Breyer; BGH 2017, 2416 Rn. 24ff. zur insoweit identischen Datenschutzrichtlinie.

104 Hofmann/Johannes, ZD 2017, 221 (224); Roßnagel/Scholz, MMR 2000, 726; Tinnfeld, in: Roßnagel 2003, Kap. 4.1 Rn. 23.

105 Hofmann/Johannes, ZD 2017, 221 (224).

der Mittel ist auch das im Rahmen einer Risikobetrachtung zu ermittelnde Interesse, das der Verantwortliche oder die andere Person an der Identifizierung haben. Es kann für einen von beiden mit der Identifizierung beispielsweise ein hohes wirtschaftliches Interesse verbunden sein.¹⁰⁶ Daher ist auch der Wert¹⁰⁷ oder der wirtschaftliche Nutzen¹⁰⁸ einer personenbezogenen Zuordnung für den Verantwortlichen oder Dritten in die Wahrscheinlichkeitsprognose einzustellen.¹⁰⁹ Außerdem sollten „der beabsichtigte Zweck, die Strukturierung der Verarbeitung, der von dem für die Verarbeitung Verantwortlichen erwartete Vorteil, die auf dem Spiel stehenden Interessen für die Personen sowie die Gefahr organisatorischer Dysfunktionen (z.B. Verletzung von Geheimhaltungspflichten) und technischer Fehler ... ebenfalls Berücksichtigung finden“.¹¹⁰

Schließlich sind die möglichen Folgen für die betroffene Person zu berücksichtigen. Die nach allgemeinem Ermessen zu bestimmende Wahrscheinlichkeit muss umso geringer sein, je größer der Schaden eines Missbrauchs der Daten für die betroffene Person wäre. Je weniger belastende Folgen für sie anzunehmen sind, desto geringer darf der Anspruch sein, sie zu vermeiden.¹¹¹ Die Anforderungen an den Ausschluss der Identifizierung dürften daher im Gesundheitsbereich in der Regel höher sein als im Bereich Online-Spiele.

Letztlich wird die Wahrscheinlichkeit nach einem objektiven Maßstab bestimmt durch eine Kosten-Nutzen-Risiko-Relation, die für den jeweiligen Verantwortlichen oder Auftragsverarbeiter anzustellen ist.¹¹² Nur wenn danach wahrscheinlich ist, dass er in der Lage ist, die Daten und sein erreichbares Zusatzwissen zu nutzen, um die betroffene Person zu identifizieren, handelt es sich für ihn um personenbezogene Daten.

Erwägungsgrund 30 DSGVO gibt einen Hinweis, wie verfügbare Technologien für die Identifizierung von natürlichen Personen genutzt werden können:

„Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.“

106 Hofmann/Johannes, ZD 2017, 221 (224).

107 Dammann, in: Simitis, § 3 Rn. 25.

108 Gola/Schomerus, § 3 Rn. 44.

109 Hofmann/Johannes, ZD 2017, 221 (224); Kroschwald 2015, 58f.; Nink/Pohle, MMR 2015, 563 (565); Marnau, DuD 2016, 428, (430).

110 Art. 29-Datenschutzgruppe, WP 136, 18.

111 Zu der aus dem Grundrechtsschutz und dem Verhältnismäßigkeitsgrundsatz abgeleitete Je-Desto-Formel s. BVerfGE 49, 89 (136ff.).

112 S. z.B. auch Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 23; Kroschwald 2015, 58f.; Dammann, in: Simitis, § 3 Rn. 25.

Datenspuren, die im Internet oder im Ubiquitous Computing hinterlassen werden, können durch Kombination mit anderen Daten wie eindeutigen Kennungen und anderen eingehenden Daten dazu benutzt werden, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren. Sowohl die erfassten Datenspuren als auch die aus ihnen angelegten Profile sollen somit als personenbezogene Daten betrachtet werden und dem Datenschutzrecht unterfallen. Damit ist für IP-Adressen¹¹³ und Cookies eindeutig geklärt, dass sie personenbezogene Daten sein können.

Die Zweck-Mittel-Relation ist nicht statisch, sondern kann sich mit der Zeit verändern.¹¹⁴ Daher muss für die Bestimmung möglichen Zusatzwissens auch die Zeitdimension einbezogen werden. Der Aufwand zur Bestimmung von Personen kann sich etwa mit der fortlaufenden Erweiterung der zugänglichen Datenmenge sowie mit den Möglichkeiten zur technischen Zusammenführung und Verknüpfung von Daten reduzieren.¹¹⁵ Aktuell als nicht personenbezogen eingestufte Daten können zukünftig personenbezogen werden.¹¹⁶ Daher fordert Satz 4 des Erwägungsgrunds 26 DSGVO, neben der „zum Zeitpunkt der Verarbeitung verfügbare(n) Technologie“ auch die „technologische(n) Entwicklungen zu berücksichtigen“.¹¹⁷ Hierfür ist zumindest für die nähere Zukunft die Dynamik der absehbaren technischen Entwicklungen in die Prognose der Identifizierbarkeit aufzunehmen.¹¹⁸ Wenn der Verantwortliche in absehbarer Zeit über neue technische Mittel zur Identifizierung verfügt oder verfügen kann, bestimmen diese die Wahrscheinlichkeit der Identifizierung. Die Prüfung des Personenbezugs muss – so die Art. 29-Datenschutzgruppe zur insoweit identischen Datenschutzrichtlinie – zumindest „die Entwicklungsmöglichkeiten in dem Zeitraum berücksichtigen ..., für den die Daten verarbeitet werden“.¹¹⁹ Dabei ist eine Abwägung vorzunehmen zwischen der zeitlichen Verfügbarkeit neuer technischer Mittel und dem Wert und der Verwendbarkeit von Informationen im Zeitablauf. Wenn die Daten nur kurzfristig aufbewahrt werden, ist ein langer Blick in die Zukunft voraussichtlich nicht notwendig. „Bei einer Aufbewahrungsdauer von zehn Jahren hingegen sollte der für die Verarbeitung Verantwortliche die Möglichkeit der Identifizierung berück-

113 Die hM nimmt ohnehin einen Personenbezug an, s. *Dammann*, in: Simitis 2014, § 3 Rn. 63 m.w.N.; s. auch *EuGH*, Urteil vom 24.11.2011, Rs. C-70/10, ECLI:EU:C:2011:771, *Scarlet Extended*; *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, *Breyer*; *BGH*, ZD 2015, 80; zum Streit um den Personenbezug von IP-Adressen s. z.B. *Düsseldorfer Kreis* 2009; *Eckhardt*, CR 2011, 339; *Krüger/Maucher*, MMR 2011, 433; *Meyerdierks*, MMR 2009, 8; *Nink/Pohle*, MMR 2015, 563; *Pahlen-Brandt*, K&R 2008, 286; *Sachs*, CR 2010, 547; *Breyer*, ZD 2014, 400.

114 S. z.B. *Kroschwald* 2015, 59; *Marnau*, DuD 2016, 428, (429).

115 S. *BVerfGE* 65, 1 (45).

116 *Dammann*, in: Simitis, § 3 Rn. 36; *Kroschwald* 2015, 59f.; *Kühling/Klar*, NJW 2013, 3613f.

117 Die Bewertung der Identifizierungsmöglichkeiten sind daher nach Erwägungsgrund 26 DSGVO nicht auf den Zeitpunkt der Datenverarbeitung beschränkt, so *Kühling/Klar*, NJW 2013, 3611 (3613), sondern berücksichtigt auch absehbare technische Entwicklungen, so auch *Marnau*, DuD 2016, 428, (429); *Klar/Kühling*, in: *Kühling/Buchner*, Art. 4 Nr. 1 Rn. 24; *Schantz*, in: *Schatz/Wolf* 2017, Rn. 283.

118 Im Ergebnis ebenso *Hofmann/Johannes*, ZD 2017, 221 (224f.).

119 Art. 29-Datenschutzgruppe, WP 136, 18; *Kroschwald* 2015, 60.

sichtigen, die im neunten Jahr der Aufbewahrungsdauer der Daten entstehen könnte und die sie in diesem Moment zu personenbezogenen Daten machen würden. Das System sollte diesen Entwicklungen angepasst werden können und dann zum gegebenen Zeitpunkt die geeigneten technischen und organisatorischen Maßnahmen einbeziehen.“¹²⁰

3.1.5.7 Zusatzwissen Dritter

Nach Satz 3 des Erwägungsgrunds 26 DSGVO sollten bei der Entscheidung, ob eine Person identifizierbar ist, auch „alle Mittel berücksichtigt werden, die von ... einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“. Mit diesen Dritten sind nicht beliebige Dritte gemeint. Die Frage nach dem Personenbezug stellt sich immer in einer Situation, in der über die Anwendbarkeit des Datenschutzrechts auf einen bestimmten Umgang mit bestimmten Daten entschieden werden muss. Für die Auslegung des Erwägungsgrunds 26 Satz 3 DSGVO kann auf die Rechtsprechung und Literatur zu dieser Frage in der Datenschutzrichtlinie zurückgegriffen werden. Danach ist für diesen Datenumgang das Zusatzwissen Dritter dann relevant, wenn die Dritten

- Daten vom Verantwortlichen oder Auftragsverarbeiter erhalten (sollen) (Veröffentlichung, Übermittlung) oder sich beschaffen (können), sodass sie in Bezug auf diese Daten selbst zum Verantwortlichen werden,¹²¹
- mit dem Verantwortlichen oder dem Auftragsverarbeiter in irgendeiner Weise zusammenarbeiten (können), um die Person zu identifizieren¹²² oder
- ihr Zusatzwissen auf andere Weise dem Verantwortlichen oder Auftragsverarbeiter zur Verfügung stellen können oder müssen.¹²³

Allerdings kann eine Weitergabe der Daten von dem Dritten an weitere Dritte oft „nach allgemeinem Ermessen“ nicht ausgeschlossen werden. Dadurch kann der Kreis des einzubeziehenden Zusatzwissens stark erweitert werden.¹²⁴ In diesem Fall ist auch dieses Zusatzwissen für die Frage der Identifizierbarkeit der betroffenen Person zu berücksichtigen. Macht also ein Verantwortlicher Daten, mit denen er keine betroffene Person identifizieren kann, einem Dritten zugänglich, der – wie etwa ein großes Unternehmen mit umfangreichen Sammlungen von Persönlichkeitsprofilen oder ein Geheimdienst – Iden-

120 Art. 29-Datenschutzgruppe, WP 136, 18. *Kühling/Klar*, NJW 2013, 3613f.; *Dammann*, in: Simitis, § 3 BDSG, Rn. 38; *Kroschwald* 2015, 60.

121 S. z.B. Art. 29-Datenschutzgruppe, WP 136, 18ff.; *Dammann*, in: Simitis, § 3 Rn. 33f.; *Eckhardt*, CR 2011, 343f.

122 S. z.B. Art. 29-Datenschutzgruppe, WP 136, 22f.

123 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 43f. – Breyer; *BGH* 2017, 2416 Rn. 24ff.; *Kühling/Klar*, ZD 2017, 28.

124 *Dammann*, in: Simitis, § 3 Rn. 34.



tifizierungen vornehmen kann, so handelt es sich um personenbezogene Daten.¹²⁵

Das Zusatzwissen Dritter ist aber nur zu berücksichtigen, soweit „nach allgemeinem Ermessen“ mit seinem Einsatz zu rechnen ist. Es kommt also auf die Frage an, ob der Verantwortliche oder die andere Person die ihm oder ihr zur Verfügung stehenden technischen oder rechtlichen Möglichkeiten vernünftigerweise nutzen wird.¹²⁶ Dementsprechend qualifiziert der Europäische Gerichtshof dynamische IP-Adressen dann als personenbezogen, wenn dem Verantwortlichen rechtliche Mittel wie etwa Auskunftsansprüche zur Verfügung stehen, mit deren Hilfe er an Zusatzinformationen gelangen kann, die einem Dritten vorliegen.¹²⁷ Dabei reicht die grundsätzliche Berechtigung, ein rechtliches Mittel geltend zu machen, aus, ohne dass es auf die tatsächliche Durchsetzbarkeit der Ansprüche im konkreten Fall ankommt.¹²⁸

Zusatzwissen Dritter ist für die Frage, ob der Betroffene identifizierbar ist, in der Regel nicht zu berücksichtigen, wenn die Verwendung des Zusatzwissens gesetzlich verboten ist.¹²⁹ Selbstverständlich ist illegales Verhalten zu berücksichtigen, wenn es stattfindet.¹³⁰ In einem Rechtsstaat kann aber nicht jedem Beteiligten ohne Anlass eine Neigung oder gar Absicht zum Rechtsbruch unterstellt werden, wenn die Befolgung eines Weitergabe- oder Verwendungsverbots weitgehend gesichert ist.¹³¹ Dabei ist es gleichgültig, ob das rechtliche Verbot an den Verantwortlichen oder an den Dritten, der über das Zusatzwissen verfügt, gerichtet ist. Entscheidend ist, ob dem Zusammenbringen beider Komponenten Hindernisse von einer Qualität entgegenstehen, dass damit „nach allgemeinem Ermessen“ praktisch nicht zu rechnen ist.¹³² Ein Rechtsbruch ist daher zu berücksichtigen, wenn es Hinweise darauf gibt, dass rechtliche Verbote nicht beachtet, nicht kontrolliert oder nicht durchgesetzt werden. Eine gesetzliche oder vertragliche Verpflichtung, etwa ein Verbot zur

125 S. z.B. *Kroschwald* 2015, 68; *Kühling/Klar*, NJW 2013, 3611 (3615); *Klar* 2012, 145; *Gola*, in: ders., Art. 4 Rn. 21; *Gola/Schomerus*, § 3 Rn. 10, 44a; *Klar/Kühling*, in: *Kühling/Buchner*, Art. 4 Nr. 1 Rn. 27. Dies ist ein Hauptargument der Vertreter für einen „absoluten“ Personenbezug, dem aber auch das Konzept eines „relativen“ Personenbezugs gerecht werden kann.

126 *Hofmann/Johannes*, ZD 2017, 221 (224); *Haase* 2015, 304; *Ziebarth*, in: *Sydow*, Art. 4 Rn. 37.

127 *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 49 – *Breyer*; *Kühling/Klar*, ZD 2017, 28.

128 S. *Hofmann/Johannes*, ZD 2017, 221 (224); *Weinhold*, ZD-Aktuell 2016, 05366.

129 Gegen die Berücksichtigung z.B. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46 – *Breyer*; *BGH* 2017, 2416 Rn. 24ff.; *BGH*, ZD 2015, 80, Rn. 32; *AG München*, ZUM-RD 2009, 414; *Hofmann/Johannes*, ZD 2017, 221 (224); *Nink/Pohle*, MMR 2015, 563 (565); *Meyerdierks*, MMR 2009, 8 (11ff.); *Krüger/Maucher*, MMR 2011, 433 (437f.); *Arning/Forgó/Krügel*, DuD 2006, 700 (703); *Eckhardt*, CR 2011, 342; *Kühling/Klar*, NJW 2013, 3611 (3613); *Kühling/Klar*, ZD 2017, 28; *Brink/Eckhardt*, ZD 2015, 205 (211); *Eckhardt*, CR 2015, 113 (115); a.A. und für die Berücksichtigung z.B. *Weichert*, DuD 2010, 681; *ders.*, in: *Däubler u.a.* 2010, § 3 Rn. 47; *Pahlen-Brandt*, K&R 2008, 286 (289); *Dammann*, in: *Simitis*, § 3 Rn. 36; *Bergt*, ZD 2015, 365 (370); *Herbst*, NVwZ 2016, 902 (905); *AG Berlin-Mitte*, K&R 2007, 601.

130 *Brink/Eckhardt*, ZD 2015, 205 (211).

131 *Meyerdierks*, MMR 2009, 8 (11f.); *Krüger/Maucher*, MMR 2011, 433 (437f.); *Arning/Forgó/Krügel*, DuD 2006, 700 (703).

132 *Dammann*, in: *Simitis*, § 3 Rn. 33; *Kroschwald* 2015, 67. Vertragliche Absprachen reichen hierfür nicht aus.

Datenherausgabe, kann in solchen Fällen allein nicht ausreichen, um den Personenbezug zu verneinen und das Datenschutzrecht für unanwendbar zu erklären.¹³³

In Fällen mit internationalem Datenverkehr und erschwelter Durchsetzung von rechtlichen Regelungen wird zu der rechtlichen Beschränkung, den Personenbezug herzustellen, noch eine tatsächliche Beschränkung, mit den Daten die betroffene Person identifizieren zu können, hinzukommen müssen.¹³⁴ Diese könnte beispielsweise in technisch-organisatorischen Maßnahmen bestehen.¹³⁵ Existieren nicht nur rechtliche, sondern auch technische und organisatorische Hürden, kann für den Dritten eine Bestimmung des Betroffenen „nach allgemeinem Ermessen“ unverhältnismäßig sein, sodass ein Personenbezug entfällt. Die Art. 29-Datenschutzgruppe hat diese Anforderungen, bezogen auf die insoweit identische Vorschrift des Art. 2 lit. a DSRL, wie folgt zusammengefasst:

*Ist „die Reidentifizierung in Übermittlungs- und Verfahrensvorschriften ausgeschlossen“ und ist „die Identifizierung ... keinesfalls beabsichtigt oder zu erwarten, weswegen geeignete technische Maßnahmen (z.B. Verschlüsselung, nicht rücknehmbares Hashing) getroffen wurden, die genau dies verhindern sollen, ... sind die vom ursprünglichen Verantwortlichen verarbeiteten Informationen nicht als Daten anzusehen, die sich auf bestimmte oder bestimmbare Personen beziehen, wenn alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden. Die Bestimmungen der Richtlinie finden somit auf ihre Verarbeitung keine Anwendung.“ Dies soll selbst dann gelten, „wenn ungeachtet aller Übermittlungsvorschriften und Maßnahmen (aufgrund unvorhersehbarer Umstände wie die zufällige Zuordnung von Eigenschaften, die die Identität einzelner Personen offenbaren) einzelne Personen identifiziert werden“.*¹³⁶

Wenn geprüft wird, welche Daten in einem zu beurteilenden Fall in personenbezogener Form vorliegen, ist nach diesen Kriterien zu verfahren. Um feststellen zu können, für welchen Verantwortlichen oder Auftragsverarbeiter und für welchen Datenverarbeitungsvorgang Datenschutzrecht anwendbar ist, ist differenziert zu untersuchen, bei welcher Stelle in welcher Phase der Datenverarbeitung Daten vorliegen, für die ein Personenbezug hergestellt werden kann.

133 Ziebarth, in: Sydow, Art. 4 Rn. 23, 37; Brink/Eckhardt, ZD 2015, 205 (211); Dammann, in: Simitis, § 3 Rn. 28; Meyerdierts, MMR 2009, 8 (11f.), und Krüger/Maucher, MMR 2011, 433 (437f.), nehmen die „Kosten“ illegalen Handelns in die Aufwand-Nutzen-Abwägung mit auf; s. auch Kroschwald 2015, 67.

134 Nicht durchsetzbare rechtliche Verbote in Drittstaaten reichen hierfür nicht aus – s. z.B. Kroschwald 2015, 68.

135 Weichert, in: Däubler u.a., § 3 Rn. 1.

136 Art. 29-Datenschutzgruppe, WP 136, 23, Hervorhebung im Original.

3.1.6 Ergebnis zum Personenbezug

Nur wenn ein Verantwortlicher personenbezogene Daten verarbeitet, untersteht er dem Datenschutzrecht. Sind die Daten nicht personenbezogen, greift Datenschutzrecht weder nach bisherigem noch nach zukünftigem Recht. Dementsprechend wichtig und umstritten ist der Begriff der personenbezogenen Daten.

Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, ... identifiziert werden kann“. Auch wenn sich der Wortlaut gegenüber Art. 2 lit. a DSRL und § 3 Abs. 1 BDSG a.F. unterscheidet, ist anerkannt, dass das Datenschutzrecht in der Datenschutz-Grundverordnung, in der Datenschutz-Richtlinie und im Bundesdatenschutzgesetz den gleichen Begriff verwendet.

Entscheidend ist die Frage, wie eine Person indirekt identifiziert werden kann – vor allem, welches Zusatzwissen dritter Personen für diese Feststellung zu berücksichtigen ist. Nach dem herrschenden und richtigen „relativen“ Verständnis des Personenbezugs ist nur das Wissen zu berücksichtigen, das der Verantwortliche mit verhältnismäßigem Aufwand mobilisieren kann. Daher kann der Personenbezug relativ und von Verantwortlichem zu Verantwortlichem unterschiedlich sein. Diese Sichtweise wurde durch die Entscheidung des Europäischen Gerichtshofs vom 19. Oktober 2016 bestätigt.

Das Zusatzwissen, das der Verantwortliche „nach allgemeinem Ermessen wahrscheinlich“¹³⁷ nutzen wird, ist für die praktischen Probleme des Datenschutzes aus einer Risikoprognose zu bestimmen. Danach sind alle relevanten objektiven Faktoren zu beachten: der zeitliche Aufwand, die finanziellen Mittel, verfügbare Technologien und technologische Entwicklungen sowie das Interesse an der Zuordnung und die Folgen für die betroffene Person. Die Prognose muss mindestens die Entwicklungsmöglichkeiten in dem Zeitraum berücksichtigen, für den die Daten verarbeitet werden sollen. Das Zusatzwissen Dritter ist dann relevant, wenn die Dritten die Daten vom Verantwortlichen erhalten (sollen) oder sich beschaffen (können), wenn sie mit dem Verantwortlichen in irgendeiner Weise zusammenarbeiten (können), um die Person zu identifizieren, oder wenn sie ihr Zusatzwissen auf andere Weise dem Verantwortlichen zur Verfügung stellen können oder müssen. Das Zusatzwissen Dritter ist aber nur zu berücksichtigen, soweit „nach allgemeinem Ermessen“ im konkreten Fall mit seinem Einsatz zu rechnen ist. Dies ist nicht der Fall, wenn die Verwendung des Zusatzwissens gesetzlich verboten ist und keine Anhaltspunkte für einen Rechtsbruch vorliegen. Ebenso sind gesetzliche Zugriffs-

¹³⁷ Erwägungsgrund 26 Satz 3 DSGVO.

kompetenzen staatlicher Behörden nur zu beachten, wenn es für deren konkrete Ausnutzung Hinweise gibt.

3.2 Anonymisierung personenbezogener Daten

Das folgende Kapitel beantwortet die Frage 4.3. Diese lautet:

Bitte vergleichen Sie die bisherige Definition des Anonymisierens nach BDSG mit dem Erwägungsgrund 26 der EU-DSGVO und führen Sie aus, wo aus Ihrer Sicht Unterschiede im Vergleich zur bisherigen Rechtslage bei der Nutzung anonymer Daten für die wissenschaftliche Forschung bestehen.

Eng mit dem Begriff der personenbezogenen Daten ist der Begriff der anonymen Daten verbunden. Diese sind Angaben zu einer betroffenen Person, die ihr nicht zugeordnet werden können. Sie fallen daher nicht unter den Begriff der personenbezogenen Daten und daher auch nicht unter das Datenschutzrecht.¹³⁸ Diese Daten können vom Zeitpunkt ihrer Entstehung her anonym sein, sie können aber auch aus personenbezogenen Daten entstehen, indem sie dadurch anonymisiert werden, dass ihnen alle potenziellen Zuordnungsmerkmale entfernt werden.

3.2.1 Anonymisierung nach der Datenschutz-Grundverordnung

Anonyme Daten und Anonymisierung werden in keiner Vorschrift der Datenschutz-Grundverordnung genannt, aber in vielen Vorschriften als existent unterstellt und in Erwägungsgrund 26 Satz 5 und 6 DSGVO erwähnt. Diese beiden Sätze in dem Erwägungsgrund zu personenbezogenen Daten lauten:

„Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.“

Sowohl in Satz 5 als auch in Satz 6 wird die Rechtsfolge festgehalten: Anonyme Daten unterfallen nicht der Datenschutz-Grundverordnung. Sie ergibt sich nicht aus dem Erwägungsgrund,¹³⁹ sondern aus der Definition personenbezogener Daten in Art. 4 Nr. 1 DSGVO. Die Rechtsfolge gilt auch, wenn die anonymen Daten für Forschungszwecke verarbeitet werden. Diese Rechtsfolge

¹³⁸ Roßnagel/Scholz, MMR 2000, 721 (723); Weichert, in: Däubler u.a., § 3 Rn. 49; Kroschwald 2015, 72.

¹³⁹ S. hierzu Kap. 3.1.5.2.

dürfte auch der Grund sein, warum die Datenschutz-Grundverordnung keine Regelung für anonyme Daten – auch keine Definition – enthält.

Satz 5 benennt anonyme Daten, für die diese Rechtsfolge gilt. Danach gibt es zwei Arten anonymer Daten. Zum einen können Daten deshalb anonym sein, weil sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Ihnen fehlen von Anfang an Merkmale, die es ermöglichen, sie einer bestimmten natürlichen Person zuzuordnen. Zum anderen können Daten anonym sein, weil sie in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. In dieser Alternative waren Daten personenbezogen, haben dann aber durch einen Anonymisierungsprozess die Merkmale verloren, die zuvor ermöglicht haben, die von ihnen betroffene Person zu identifizieren.¹⁴⁰ In beiden Varianten wird die Anonymität von ihrem Ergebnis her definiert und ist in beiden Varianten gleich: Die Daten sind deshalb anonym, weil sie keine Zuordnung zu einer bestimmten Person ermöglichen.¹⁴¹

Anonyme Daten sind das Gegenteil von personenbezogenen Daten.¹⁴² Sie grenzen sich definitorisch von diesen dadurch ab, dass sie gerade keine personenbezogenen Daten sind.¹⁴³ Anonymisierung und Personenbezug korrelieren insofern negativ. Daten sind anonym und damit nicht identifizierbar, wenn sie mit den verfügbaren Mitteln nach allgemeinem Ermessen nicht einer bestimmten Person zugeordnet werden können. Die Begriffe der anonymen Daten und nicht-personenbezogenen Daten weichen im Wesentlichen in einem Punkt voneinander ab: Soweit ein anderes Merkmal als die Bestimmbarkeit aus der Begriffsdefinition der personenbezogenen Daten zu verneinen ist und entsprechend kein Personenbezug vorliegt, sind die Daten nicht automatisch anonym. Handelt es sich beispielsweise um keine Einzelangaben, beschreiben die Informationen keine persönlichen oder sachlichen Verhältnisse oder beziehen sich diese Informationen nicht auf eine natürliche Person, kann auch nicht von anonymen Daten gesprochen werden.¹⁴⁴ Es sind vielmehr Informationen, die zu keiner (natürlichen) Person gehören.¹⁴⁵ Entscheidend ist, dass die Daten zwar Angaben zu einer bestimmten Person enthalten, dass mit ihnen aber kein Bezug zu einer identifizierten oder identifizierbaren natürlichen Person hergestellt werden kann. Da sie keiner natürlichen Person zugeordnet werden können, geht von ihnen auch kein Risiko aus. Das ist der inhaltliche Grund, warum sie von der Datenschutz-Grundverordnung nicht erfasst werden.

140 Roßnagel/Scholz, MMR 2000, 721 (723).

141 Forgó/Krügel, MMR 2010, 19; Meyerdierks, MMR 2009, 10; Kroschwald 2015, 57f.

142 S. z.B. Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 31.

143 S. Hofmann/Johannes, ZD 2017, 223.

144 S. z.B. Kroschwald 2015, 71f.

145 Roßnagel/Scholz, MMR 2000, 721 (723).

Die Datenschutz-Grundverordnung hat anonyme Daten – im Gegensatz zu § 3 Abs. 6 BDSG a.F. und § 67 Abs. 8 SGB X a.F. – nicht definiert. Ebenso haben das neue Bundesdatenschutzgesetz und das neue Sozialgesetzbuch wie die Datenschutz-Grundverordnung auf eine Definition verzichtet. Daher kann ihr auch keine ausdrückliche Antwort auf die Frage entnommen werden, mit welcher Wahrscheinlichkeit der Personenbezug der Daten ausgeschlossen sein muss. Diese Antwort bietet auch Erwägungsgrund 26 DSGVO nicht. Dort heißt es nur, dass sich die Daten „nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen“ und dass „die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Da diese Frage nur die nach personenbezogenen Daten umkehrt, kann auf die Ausführungen zu personenbezogenen Daten¹⁴⁶ Bezug genommen werden. Entsprechend den Ausführungen in Kapitel 3.5 ist diese Frage nach dem dort beschriebenen pragmatischen Konzept zu beantworten.¹⁴⁷

Ob die Daten anonym sind und einen Personenbezug ausschließen, ist – ausgehend von einem relativen Konzept¹⁴⁸ – nach einer Risikoprognose zu bestimmen, die sowohl das Interesse möglicher Datenverarbeiter als auch die von ihnen mobilisierbaren Mittel der Zuordnung berücksichtigt. Diese Sichtweise liegt der Definition des § 3 Abs. 6 BDSG a.F. und des § 67 Abs. 8 BDSG X a.F. zugrunde, nach der die Daten dann anonym sind, wenn „sie nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können“. Nach dieser im geltenden Recht zu findenden pragmatischen Sichtweise kann für die Bewertung als anonym die Zuordnung zwar theoretisch möglich sein, muss aber mit einer jeweils ausreichenden Wahrscheinlichkeit ausgeschlossen sein. Die Zuordnung muss im Verhältnis zu dem dazu notwendigen Aufwand so unverhältnismäßig sein, dass eine Identifizierung nach allgemeiner Lebenserfahrung oder dem Stand der Wissenschaft und Technik nicht zu erwarten ist.¹⁴⁹ Zu berücksichtigen sind dabei das vorhandene oder erwerbbar Zusatzwissen des Verantwortlichen, aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit.¹⁵⁰ In diese Betrachtung müssen aber zusätzlich zur Verhältnismäßigkeit des Aufwands für den jeweiligen Datenverarbeiter auch die möglichen Folgen für die jeweils betroffene Person eingehen. Danach wären die Daten dann anonym, wenn die Wahrscheinlichkeit der Zuordnung zu einer betroffenen Person angesichts des Verhältnisses von Nutzen und Aufwand für den jeweiligen Datenverarbeiter und angesichts der jeweiligen Gefährdung der Grundrechte der betroffenen Person ausreichend gering ist. Ein absoluter Ausschluss der

146 S. insb. Kap. 3.1.5.

147 Nach *Laue/Nink/Kremer* 2016, § 1 Rn. 19 ist davon auszugehen, dass die bisherigen Definitionen von anonymen und anonymisierten Daten ihre Gültigkeit behalten.

148 S. Kap. 3.1.3 bis 3.1.5.

149 *Roßnagel/Scholz*, MMR 2000, 721 (724); *Härting*, NJW 2013, 2065 (2066); *Laue/Nink/Kremer* 2016, § 1 Rn. 21.

150 *Roßnagel/Scholz*, MMR 2000, 721 (724); *Laue/Nink/Kremer* 2016, § 1 Rn. 21

Zuordnung ist nicht erforderlich. In der Literatur wird diese pragmatische Sichtweise¹⁵¹ als faktische Anonymität bezeichnet.¹⁵²

Diese Bestimmungen einer ausreichenden Anonymität entsprechen den Argumenten für die Abgrenzung von personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO.¹⁵³ Hier wie dort geht es um die Bestimmung des relevanten Zusatzwissens für die Definition personenbezogener Daten. Allerdings ist die Argumentation durch eine fehlende Definition anonymer Daten in der Datenschutz-Grundverordnung erschwert.

Es ist daher ergänzend zu prüfen, ob andere Vorschriften der Datenschutz-Grundverordnung als Art. 4 DSGVO andere Hinweise auf das Verständnis von anonymen Daten liefern. Einen solchen Hinweis könnte Art. 89 Abs. 1 DSGVO bieten. Diese Öffnungsklausel für die Regelung verschiedener Verarbeitungszwecke, u.a. Forschungszwecke, fordert in Satz 4, die Daten nur noch ohne Personenbezug weiterzuverarbeiten, wenn der Forschungszweck den Personenbezug nicht mehr erfordert. Die Verordnung fordert somit eine Anonymisierung von Daten, ohne diesen Begriff ausdrücklich zu benennen. Diese Vorschrift beinhaltet keine ausdrückliche Erklärung für das geforderte Maß an Anonymisierung. Sie führt aber zu folgender Überlegung:¹⁵⁴ Wollte die Verordnung einen absoluten Ausschluss der Zuordnung, also auf die Möglichkeiten aller Menschen zur Identifizierung abstellen, bestünde die Möglichkeit zur Anonymisierung kaum mehr und würde die Weiterverarbeitung von Daten für viele Forschungsinstitutionen ausgeschlossen. Angesichts des Grundrechts auf Forschung in Art. 13 GRCh (und Art. 5 Abs. 3 GG) sprechen die besseren Argumente dafür, dass die Verordnung auf das Potenzial des Verantwortlichen zur Re-Identifizierung abstellt, auf die er oder ein Dritter „nach allgemeinem Ermessen wahrscheinlich“ zurückgreifen kann. Das Gleiche gilt für jene Dritte, die „nach allgemeinem Ermessen“ die Identifizierung der betroffenen Person betreiben könnten. Das können wissenschaftliche Kooperationspartner, interessierte Unternehmen, aber auch staatliche Stellen mit Zugriffsrechten sein, nicht aber alle Dritte weltweit. Für staatliche Stellen genügt jedoch nicht die abstrakte gesetzliche Möglichkeit, sondern es muss „nach allgemeinem Ermessen“ damit gerechnet werden können, dass sie auf die (scheinbar) anonymen Daten zugreifen und mit diesen die betroffene Person identifizieren.¹⁵⁵

Im Ergebnis ist daher festzuhalten: Erwägungsgrund 26 Satz 5 und 6 DSGVO erläutert den Begriff der personenbezogenen Daten in Art. 4 Nr. 1 DSGVO durch den Rückgriff auf den Begriff der anonymen oder anonymisierten Daten.

151 S. z.B. *Dammann*, in: *Simitis*, § 3 Rn. 23; *Gola/Schomerus*, § 3 Rn. 43f.; *Hornung*, DuD 2004, 429; *Roßnagel/Scholz*, MMR 2000, 721 (724ff.); *Buchner*, in: *Taeger/Gabel*, § 3 Rn. 44.

152 S. z.B. *Härting*, NJW 2013, 2065; *Laue/Nink/Kremer*, § 1 Rn. 21; *Ziebarth*, in: *Sydow*, Art. 4 Rn. 98.

153 S. Kap. 3.1.5.

154 S. zu dieser *Hofmann/Johannes*, ZD 2017, 223.

155 S. z.B. *Brink/Eckhardt*, ZD 2015, 211;

Er verwendet dabei diesen Begriff in einer Weise, die dem bisherigen Verständnis der pragmatischen Sichtweise einer faktischen Anonymität¹⁵⁶ entspricht.¹⁵⁷

3.2.2 Anonymisierung nach § 27 Abs. 3 BDSG-neu

§ 27 BDSG-neu enthält in Ausfüllung der Öffnungsklausel in Art. 89 Abs. 1 DSGVO besondere Regelungen für die Datenverarbeitung zu Forschungs- und Statistikzwecken. Abs. 3 enthält Vorgaben zu geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person für den Fall, dass der Verantwortliche besondere Kategorien personenbezogener Daten verarbeitet. § 27 Abs. 3 BDSG-neu lautet:

„Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.“

Der amtlichen Begründung zu § 27 Abs. 1 BDSG-neu kann entnommen werden, dass die gesamte Vorschrift des § 27 BDSG für „die öffentliche und private Forschung durch öffentliche und nicht-öffentliche Stellen gilt“.¹⁵⁸ Abs. 3 wird in der amtlichen Begründung nur mit dem Hinweis erläutert, dass diese Regelung § 40 Abs. 2 BDSG a.F. „entlehnt“ ist.¹⁵⁹

Sie ist jedoch nicht mit § 40 Abs. 2 BDSG a.F. identisch. Denn dessen Satz 1 lautet:

„Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist.“

§ 40 Abs. 2 Satz 1 BDSG a.F. ist auf Forschungsinstitutionen beschränkt und bezieht sich auf alle personenbezogenen Daten, die zu Forschungszwecken verarbeitet werden. Die Vorschrift fordert, diese zu anonymisieren, sobald dies möglich ist. § 27 Abs. 3 Satz 1 BDSG-neu gilt dagegen auch für Statistik-

156 S. Fn. 149f.

157 S. z.B. Laue/Nink/Kremer, § 1 Rn. 21; Gola, in: Gola, Art. 4 Rn. 40; Ziebarth, in: Sydow, Art. 4 Rn. 98; Schantz, in: Schantz/Wolff, Rn. 297ff.; Husemann, in: Roßnagel 2018, § 3 Rn. 7.

158 BT-Drs. 18/11325, 98; Greve, NVwZ 2017, 737 (739).

159 BT-Drs. 18/11325, 98.

zwecke und schränkt die Forderung nach Anonymisierung auf besondere Kategorien personenbezogener Daten ein.¹⁶⁰

Mit § 27 Abs. 3 BDSG-neu setzt der deutsche Gesetzgeber Art. 9 Abs. 2 lit. j DSGVO in Bezug auf Gesundheitsdaten um. Art. 9 Abs. 2 lit. j DSGVO erlaubt dem Mitgliedstaat jedoch nicht, Regelungen zu Daten zu treffen, die nicht Gesundheitsdaten sind. Auch ist er nach dieser Öffnungsklausel nicht befugt, Regelungen zur Datenverarbeitung in der Forschung zu treffen. Für die Datenverarbeitung in der Forschung ist – auch wenn es um medizinische Forschung geht – Art. 89 DSGVO die speziellere Norm. Daher muss der deutsche Gesetzgeber sowohl zur Forschung mit Gesundheitsdaten als auch zur Forschung mit anderen Daten Art. 89 Abs. 1 DSGVO beachten.

Art. 89 Abs. 1 DSGVO fordert in Satz 1, dass „die Verarbeitung zu ... Forschungszwecken ... geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung“ unterliegt. Nach Satz 2 soll „mit diesen Garantien ... sichergestellt (werden), dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird“. Hierzu sollen nach der missglückten Formulierung in Satz 4 „in allen Fällen, in denen diese Zwecke durch die Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, erfüllt werden können, ... diese Zwecke auf diese Weise erfüllt“ werden. Die Anonymisierung der Daten, die nicht mehr als personenbezogene Daten für Forschungszwecke benötigt werden, ist eine gesetzlich vorgesehene Garantie, die Art. 89 Abs. 1 Satz 1 DSGVO fordert. Die englische Fassung des Art. 89 Abs. 1 Satz 4 DSGVO lautet:

“Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.”

Sie wird durch die deutsche Sprachfassung korrekt wiedergegeben. Das in der englischen Fassung verwendete Wort „shall“ bedeutet im Deutschen kein „soll“, sondern – wie in allen anderen Regelungen der Verordnung, in denen das Hilfsverb „shall“ genutzt wird – ein „muss“.

Diesen Anforderungen des Art. 89 Abs. 1 DSGVO wird § 27 Abs. 3 BDSG-neu nicht gerecht. Weder die Garantien nach Art. 89 Abs. 1 Satz 1 DSGVO noch die Pflicht zur Anonymisierung nach Art. 89 Abs. 1 Satz 4 DSGVO sind auf besondere Kategorien personenbezogener Daten beschränkt. Indem § 27 Abs. 3 Satz 1 BDSG-neu – im Gegensatz zu § 40 Abs. 2 Satz 1 BDSG a.F. – diese Einschränkung vornimmt, verstößt die Vorschrift gegen Art. 89 Abs. 1 Satz 1 und 4 DSGVO und ist unionsrechtswidrig.¹⁶¹ In dieser Hinsicht greift der Anwendungsvorrang

¹⁶⁰ Johannes/Richter, DuD 2017, 300 (304).

¹⁶¹ Johannes/Richter, DuD 2017, 300 (302).

der Unionsverordnung und es gilt allein Art. 89 Abs. 1 Satz 4 DSGVO für alle personenbezogenen Daten.¹⁶²

Außerdem kann nach Art. 89 Abs. 1 Satz 4 DSGVO von der Anonymisierung nur abgesehen werden, wenn dies zu Forschungszwecken zwingend erforderlich ist. Daher ist auch die Ausnahme in § 27 Abs. 3 Satz 1 BDSG-neu unionsrechtswidrig, nach der die Anonymisierung entfallen kann, wenn „berechtignte Interessen der betroffenen Person ... dem entgegen“ stehen.¹⁶³ Die Ausnahme kann nicht angewendet werden.¹⁶⁴

Soweit § 27 Abs. 3 Satz 1 BDSG-neu eine Anonymisierung vorsieht, entspricht dies der „Weiterverarbeitung, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist“, in Art. 89 Abs. 1 Satz 4 DSGVO und der Beschreibung der Anonymisierung in Erwägungsgrund 26 Satz 5 DSGVO. Auch § 27 Abs. 3 Satz 1 BDSG-neu erwähnt die zwei Entstehungsmöglichkeiten anonymer Daten, die in Erwägungsgrund 26 Satz 5 DSGVO genannt sind. Insofern ergibt sich aus § 27 Abs. 3 Satz 1 BDSG-neu kein anderer Bedeutung Gehalt als der in Erwägungsgrund 26 Satz 5 DSGVO.¹⁶⁵

3.2.3 Anforderungen an die Anonymisierung für die wissenschaftliche Forschung

Die Datenschutz-Grundverordnung gibt keine Verfahren zur Anonymisierung vor. Vielmehr muss der Datenverarbeiter im Ergebnis die in Art. 4 Nr. 1 DSGVO niedergelegten Kriterien erfüllen, die eine Einordnung der Daten als personenbezogen ausschließen.¹⁶⁶ Ob ein Personenbezug ausgeschlossen ist, richtet sich nicht nach der Einhaltung eines bestimmten Verfahrens, sondern nach dem Erreichen des notwendigen Ergebnisses: Eine Identifizierbarkeit der betroffenen Person muss mit den verfügbaren Mitteln nach allgemeinem Ermessen ausgeschlossen sein.

Für eine Anonymisierung muss der Personenbezug für alle Beteiligten irreversibel entfernt sein.¹⁶⁷ Nach dem Maßstab der faktischen Anonymität¹⁶⁸ ist auszuschließen, dass diese nicht oder nur unter unverhältnismäßigem Aufwand in der Lage sind, die Daten einer natürlichen Person zuzuordnen. Nur soweit eine Zuordnung der anonymen Daten nach der allgemeinen Lebenserfahrung oder – in Ermangelung entsprechender Erfahrungswerte – auf Grundlage einer

162 Im Ergebnis ebenso Greve, NVwZ 2017, 737 (739), der die Datenschutz-Grundverordnung für die Daten, die nicht besonderen Kategorien unterfallen, ergänzend anwenden will.

163 Johannes/Richter, DuD 2017, 300 (304).

164 Lebenswichtige Interessen der betroffenen Person können nach Art. 6 Abs. 1 UAbs. 1 lit. d DSGVO berücksichtigt werden.

165 S. hierzu Kap. 3.1.5.2.

166 S. z.B. Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 33; Klabunde, in: Ehmann/Selmayr, Art. 4 Rn. 16.

167 Dammann, in: Simitis, § 3 Rn. 200.

168 S. Kap. 3.2.1 und insb. Fn. 149f. und 155.

Risikoprognose auf dem Stand der Wissenschaft nicht zu erwarten ist,¹⁶⁹ ist ein ausreichendes Maß der Anonymisierung erreicht.¹⁷⁰ Dabei sind nach Erwägungsgrund 26 Satz 4 DSGVO auch zukünftige „technologische Entwicklungen“, die gegebenenfalls eine Re-Identifikation ermöglichen, zu berücksichtigen.¹⁷¹

Die Methode der Anonymisierung hängt vom Aufbau und Inhalt des jeweiligen Datenbestands ab.¹⁷² Unerlässlich ist wohl die irreversible Entfernung und Löschung der expliziten oder direkten Identifikationsmerkmale wie Namen und Anschriften, Personenkennzeichen, Kontonummern.¹⁷³ Dies kann aber in vielen Fällen unzureichend sein, insbesondere wenn der Verantwortliche Zusatzwissen mobilisieren kann, das dann auch ohne direkte Identifikationsmerkmale eine Identifizierung ermöglicht. Weitere Maßnahmen¹⁷⁴ sind etwa die Merkmalsaggregation, also das Ersetzen konkreter Angaben durch allgemein gehaltene Ersatzangaben,¹⁷⁵ oder auch der kontrollierte Einbau von Zufallsfehlern.¹⁷⁶ Stärken und Schwächen von Anonymisierungstechniken hat die Art. 29-Datenschutzgruppe analysiert.¹⁷⁷

Nach Erwägungsgrund 26 Satz 4 DSGVO sind bei der Feststellung des Personenbezugs von Daten „alle objektiven Faktoren, wie ... die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen“. Daraus folgt, dass die eingesetzten Anonymisierungsverfahren dem aktuellen Stand der Technik¹⁷⁸ und den absehbaren technischen Entwicklungen im Zeitraum der Datenspeicherung entsprechen müssen.

Ist das Risiko einer Re-Identifizierung entscheidendes Differenzierungsmerkmal zwischen anonymen und personenbeziehbaren Daten, erfordert die Dynamik der Risikoentwicklung zwei Reaktionen: Zum einen ist bei der Festlegung der Anonymisierungsverfahren eine „Schutzreserve“ vorzusehen, die zukünftigen Risiken vorbeugt.¹⁷⁹ Zum anderen ist eine einmalige Risikoanalyse unzureichend. Insbesondere wenn die anonymen Daten zur Datenanalyse (etwa im Zusammenhang mit „Big Data-Anwendungen“ oder bei „Web-tracking Tools“) genutzt werden, ist regelmäßig zu prüfen, ob im Laufe der

169 Roßnagel/Scholz, MMR 2000, 724.

170 Kroschwald 2015, 72f.

171 Für die DSGVO z.B. Marnau, DuD 2016, 428, (429); Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 24; Kühling/Klar, NJW 2013, 3611 (3613); Schantz, in: Schatz/Wolf 2017, Rn. 283. Hofmann/Johannes, ZD 2017, 221 (224f.); Krügel, ZD 2017, 455 (456); für die DSRL bereits z.B. Art. 29-Datenschutzgruppe, WP 136, 18; Kroschwald 2015, 60; Weichert, in: Däubler u.a., § 3 Rn. 47.

172 Dammann, in: Simitis, § 3 Rn. 205.

173 S. zu diesen z.B. Dammann, in: Simitis, § 3 Rn. 206.

174 Verfahren der Anonymisierung – Dammann, in: Simitis § 3 Rn. 209

175 Z.B. indem bei einer Altersangabe der Wert „103 Jahre“ durch die Gruppierung „Alter über 80 Jahre“ ersetzt wird, Dammann, in: Simitis, § 3 Rn. 207.

176 Dammann, in: Simitis, § 3 Rn. 207ff.

177 Art. 29-Datenschutzgruppe, Stellungnahme 5/2014, WP 216, 13ff. und Anhang, 33ff.

178 So Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 1 Rn. 33.

179 Schaar, ZD 2016, 224 (225).

Zeit erworbenes Zusatzwissen, etwa durch verbesserte Analyse- und Verknüpfungsmöglichkeiten, nicht zwischenzeitlich eine Identifizierung der ursprünglich anonymen Daten ermöglicht.¹⁸⁰

3.2.4 Vergleich mit der Rechtslage nach der Datenschutz-Richtlinie und dem geltenden Bundesdatenschutzgesetz

Die Datenschutz-Richtlinie kennt ebenfalls keine Regelung zur Anonymisierung. Sie wird lediglich in Erwägungsgrund 26 Satz 3 DSRL erwähnt.¹⁸¹ Dieser ist im Wesentlichen identisch mit der Erwähnung der Anonymisierung in Erwägungsgrund 26 Satz 5 DSGVO. Wie nach der Datenschutz-Grundverordnung ergibt sich das Verständnis der anonymen Daten und der Anonymisierung aus der Umkehr der Definition personenbezogener Daten in Art. 2 lit. a DSRL. Insofern können alle Erkenntnisse zur Anonymisierung nach der Datenschutz-Richtlinie auch auf die Datenschutz-Grundverordnung übertragen werden.

Dagegen hat das Bundesdatenschutzgesetz a.F. „Anonymisieren“ in § 3 Abs. 6 wie folgt definiert:

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Die Definition in § 67 Abs. 8 SGB X a.F. ist bis auf den Austausch der Worte „personenbezogener Daten“ durch „Sozialdaten“ mit der Definition in § 3 Abs. 6 BDSG a.F. identisch.

Danach sind Daten „anonym“ und damit nicht personenbezogen,¹⁸² wenn sie nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können. Für diese faktische Anonymität ist ein vollständiger Ausschluss der Zuordnung der Daten zu einer bestimmten Person nicht erforderlich. Dies entspricht auch dem Erwägungsgrund 26 Satz 5 DSGVO. Sowohl nach diesem Erwägungsgrund als auch nach § 3 Abs. 6 BDSG a.F. und § 67 Abs. 8 SGB X a.F. genügt eine faktische Anonymisierung.¹⁸³

Daher ist festzustellen, dass die Datenschutz-Grundverordnung weder für den Begriff noch für die Funktion für die Rechtsfolgen der Anonymisierung und

¹⁸⁰ Laue/Nink/Kremer 2016, § 1 Rn. 22.

¹⁸¹ S. den Text des Erwägungsgrunds 26 in Kap. 3.1.3.

¹⁸² S. z.B. Gola/Schomerus, § 3 Rn. 11, 43; Buchner, in: Taeger/Gabel, § 3 Rn. 44f.; 9; Roßnagel/Scholz MMR 2000, 723f.; Roßnagel, digma 2011, 161; Schaar, ZD 2016, 224 (225); dagegen Verwirrung suchend Härting, NJW 2013, 2066.

¹⁸³ Schaar, ZD 2016, 224 (225).

anonymer Daten gegenüber der Rechtslage unter dem bisherigen Bundesdatenschutzgesetz und dem bisherigen Sozialgesetzbuch wesentliche Änderungen gebracht hat.

Zur Erläuterung dieses Ergebnisses sei noch einmal darauf hingewiesen, dass die Datenschutz-Grundverordnung weder eine Definition noch eine Regelung zur Anonymität von Daten und ihrer Rechtsfolgen enthält. Der Begriff der Anonymität von Daten muss aus dem Begriff des Personenbezugs von Daten als dessen Gegenteil erschlossen werden. Hierzu hält die Erläuterung von personenbezogenen Daten in Erwägungsgrund 26 Satz 5 und 6 DSGVO nur fest, dass anonyme Daten, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen“, nicht dem Datenschutzrecht unterfallen. Da Art. 4 Nr. 1 DSGVO den Begriff der personenbezogenen Daten in den wesentlichen Aspekten identisch mit den Definitionen in Art. 2 lit. a DSGVO und § 3 Abs. 1 BDSG a.F. definiert, muss diese Identität auch für anonyme Daten als ihr Gegenteil gelten.

3.2.5 Ergebnis zur Anonymisierung

Anonyme Daten sind Angaben zu einer betroffenen Person, die ihr nicht zugeordnet werden können. Sie sind daher keine personenbezogenen Daten. Sie können von Anfang an anonym sein, aber auch aus personenbezogenen Daten entstehen, indem sie dadurch anonymisiert werden, dass aus ihnen alle potenziellen Zuordnungsmerkmale entfernt werden.

Anonyme Daten und Anonymisierung werden in keiner Vorschrift der Datenschutz-Grundverordnung genannt oder geregelt, aber in vielen Vorschriften als existent unterstellt und in Erwägungsgrund 26 Satz 5 und 6 DSGVO erwähnt. Das aus beiden Sätzen erkennbare Verständnis entspricht dem des § 3 Abs. 6 BDSG a.F.

§ 27 Abs. 3 BDSG-neu fordert eine Anonymisierung nur von besonderen Kategorien personenbezogener Daten, sobald dies nach dem Forschungszweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Diese Regelung verstößt insofern gegen die Datenschutz-Grundverordnung, als Art. 89 Abs. 1 Satz 4 DSGVO die Anonymisierung aller Forschungsdaten fordert und die Einschränkung wegen berechtigter Interessen der betroffenen Person nicht vorsieht. In beiden Fällen besteht ein Anwendungsvorrang der Verordnung.

Die Datenschutz-Grundverordnung gibt keine Verfahren zur Anonymisierung vor. Vielmehr muss der Datenverarbeiter im Ergebnis die in Art. 4 Nr. 1 DSGVO niedergelegten Kriterien erfüllen, die eine Einordnung der Daten als personenbezogen ausschließen.

3.3 Pseudonymisierung personenbezogener Daten

Das folgende Kapitel beantwortet die Fragen 4.1 Satz 1 bis 3. Diese lauten:

Vergleichen Sie bitte den Pseudonymisierungsbegriff aus den bisherigen Vorschriften des BDSG mit jenen aus der EU-Datenschutzgrundverordnung. Sind diese gleichbedeutend oder ergeben sich unterschiedliche Anforderungen an den Pseudonymisierungsprozess? Gehen Sie in Bezug auf die bisherige Rechtslage bei der Nutzung pseudonymer Daten auch auf das EUGH-Urteil vom 19.10.2016 (Patrick Breyer gegen Bundesrepublik Deutschland, Aktz. C – 582/14) ein.

Im Gegensatz zur Datenschutz-Richtlinie, die Pseudonymisierung gar nicht ausdrücklich berücksichtigt, und zum Bundesdatenschutzgesetz a.F., das Pseudonymisierung zwar in § 3 Abs. 6a BDSG a.F. definiert, aber nur in § 3a BDSG a.F. als eine beispielhafte Maßnahme der Datensparsamkeit erwähnt,¹⁸⁴ etabliert die Datenschutz-Grundverordnung Pseudonymisierung als den „Kernpfeiler“ der technisch-organisatorischen Maßnahmen des Datenschutzes.¹⁸⁵

3.3.1 Pseudonymisierung nach der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung nennt in vielen Vorschriften die Pseudonymisierung als zentrales Mittel, um die Rechte und Freiheiten der betroffenen Person zu wahren und ihr ausreichende Garantien zu bieten. So ist Pseudonymisierung in Art. 6 Abs. 4 lit. e DSGVO als angemessene Garantie bei der Bestimmung der Vereinbarkeit von Zwecken zu berücksichtigen.¹⁸⁶ Ebenso wird Pseudonymisierung in Art. 25 Abs. 1 DSGVO als ein Weg genannt, Privacy by Design umzusetzen.¹⁸⁷ Art. 32 Abs. 1 lit. a DSGVO nennt Pseudonymisierung als ein Instrument technisch-organisatorischer Sicherung des Datenschutzes.¹⁸⁸ Verhaltensregeln können nach Art. 40 Abs. 2 lit. d DSGVO Anforderungen an personenbezogene Daten branchenspezifisch konkretisieren. Art. 89 Abs. 1 Satz 3 DSGVO bietet Pseudonymisierung als eine der technisch-organisatorischen Maßnahmen an, um die von Art. 89 Abs. 1 Satz 1 DSGVO geforderten Garantien bei der Verarbeitung personenbezogener Daten für wissenschaftliche, statistische und archivarische Zwecke zu gewährleisten.¹⁸⁹

Pseudonymisierung ist in Art. 4 Nr. 5 DSGVO folgendermaßen definiert:

184 S. Scholz, in: Simitis, § 3a Rn. 45ff.

185 Marnau, DuD 2016, 428 (430); Albrecht/Jotzo 2017, Teil 3 Rn. 4: „besonderer Stellenwert der Pseudonymisierung“; Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 5 Rn. 4: „leicht gesteigerte Bedeutung“.

186 S. z.B. Buchner/Petri, in: Kühling/Buchner, Art. 6 Rn. 191.

187 Erwägungsgrund 78 DSGVO; s. z.B. Barlag, in: Roßnagel 2017, § 3 Rn. 225.

188 S. z.B. Barlag, in: Roßnagel 2017, § 3 Rn. 197.

189 S. hierzu auch Erwägungsgrund 156 DSGVO; s. hierzu z.B. Johannes, in: Roßnagel 2017, § 4 Rn. 63.

„Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“

Aufgrund dieser Definition in der Datenschutz-Grundverordnung haben das neue Bundesdatenschutzgesetz und das neue Sozialgesetzbuch auf eine eigene Definition der Pseudonymisierung verzichtet.

Im Rahmen des Erwägungsgrunds 26 DSGVO zur Definition personenbezogener Daten widmet sich Satz 2 der Pseudonymisierung und stellt fest:

„Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.“

Die Literatur zur Datenschutz-Grundverordnung orientiert sich überwiegend am Wortlaut des Erwägungsgrunds und stellt ohne weitere Differenzierung fest, dass pseudonyme Daten personenbezogene Daten sind.¹⁹⁰

Zwischen der Definition in Art. 4 Nr. 5 DSGVO und dem Erwägungsgrund 26 Satz 2 DSGVO besteht jedoch ein Widerspruch, den es aufzulösen gilt.¹⁹¹ Nach Art. 4 Nr. 5 DSGVO können die pseudonymen Daten ohne zusätzliche Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden. Sie sind also für den Verantwortlichen, der keinerlei Möglichkeiten hat, die zusätzlichen Informationen zur Kenntnis zu nehmen, entsprechend der Definition in Art. 4 Nr. 1 HS 2 DSGVO keine personenbezogenen Daten. Dagegen sollen nach Erwägungsgrund 26 Satz 2 DSGVO genau diese Daten „als Informationen über eine identifizierbare natürliche Person betrachtet werden“, also als personenbezogene Daten gelten. Dieser Widerspruch kann nur dadurch aufgelöst werden, dass die jeweiligen Aussagen präzisiert und damit eingeschränkt werden. Dabei sind die allgemeinen Regeln für die Feststellung personenbezogener Daten zu berücksichtigen.

Als identifizierbar wird eine natürliche Person nach Art. 4 Nr. 1 HS 2 DSGVO angesehen, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung ... identifiziert werden kann“. Dabei kommt es auf das vorhandene und in verhältnismäßiger Weise mobilisierbare Zusatzwissen des Verantwort-

190 S. z.B. Albrecht/Jotzo 2017, Teil 3 Rn. 4; Klabunde, in: Ehmann/Selmayr, Art. 4 Rn. 15; Gola, in: ders., Art. 4 Rn. 39, in Widerspruch zu Art. 4 Rn. 19f.; Laue/Nink/Kremer 2016, § 1 Rn. 26, in Widerspruch zu § 1 Rn. 29f.

191 Ein Problem sehen Klar/Kühling, in: Kühling/Buchner, Art. 4 Nr. 5 Rn. 12, ohne jedoch eine Lösung anzubieten.

lichen oder Auftragsverarbeiters an.¹⁹² Dieses Zusatzwissen kann auch bei Dritten vorhanden sein, wenn der Datenverarbeiter eine praktisch realisierbare Möglichkeit hat, dieses zur Kenntnis zu nehmen.¹⁹³ Dies muss auch für pseudonyme Daten gelten. Wenn es praktisch ausgeschlossen ist, dass der Datenverarbeiter die Zuordnungsregel für die pseudonymen Daten erlangen kann, dann können die Daten entsprechend der Definition des Art. 4 Nr. 5 DSGVO von ihm „nicht mehr einer spezifischen betroffenen Person zugeordnet werden“.¹⁹⁴

Da dies der Definition in Art. 4 Nr. 5 DSGVO widersprechen würde, kann Satz 2 des Erwägungsgrunds 26 DSGVO nicht absolut verstanden werden.¹⁹⁵ Vielmehr ist dieser Satz so zu verstehen, dass die „einer Pseudonymisierung unterzogene(n) personenbezogene(n) Daten“ dann „als Informationen über eine identifizierbare natürliche Person betrachtet werden“ sollen, wenn sie „durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten“. Dies ist dann der Fall, wenn der Datenverarbeiter irgendeine realistische Möglichkeit hat, die Zuordnungsregel für die pseudonymen Daten zu erlangen (oder auf andere Weise zuordnen kann). Dies ist immer dann der Fall, wenn die Zuordnungsregel beim Verantwortlichen oder Auftragsverarbeiter verbleibt (interne Pseudonymisierung). Dies gilt auch, wenn die Datenverarbeitung und die Aufbewahrung der Zuordnungsregel innerhalb des Verantwortlichen organisatorisch – etwa in unterschiedlichen Abteilungen – getrennt sind. Dies gilt schließlich auch dann, wenn zwar ein Dritter die Zuordnungsregel aufbewahrt, aber nicht sichergestellt ist, dass der Datenverarbeiter sie nicht erfahren kann.

Somit ist Erwägungsgrund 26 Satz 2 DSGVO mit der Definition in Art. 4 Nr. 5 DSGVO vereinbar, wenn in Satz 2 der Relativsatz als Bedingung verstanden wird. Umgekehrt ist Art. 4 Nr. 5 DSGVO mit Erwägungsgrund 26 Satz 2 DSGVO vereinbar, wenn durch die in Nr. 5 genannten Maßnahmen im Ergebnis sichergestellt ist, dass die pseudonymen Daten durch den Datenverarbeiter „nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ können.

Nach diesem Verständnis von Definition und Erwägungsgrund gibt es somit zwei Arten von pseudonymen Daten mit unterschiedlichen Voraussetzungen und unterschiedlichen Rechtsfolgen.

Die erste Art pseudonymer Daten bewirkt, dass für den Verantwortlichen die Zuordnung der Daten zu einer bestimmten Person ausgeschlossen ist. Diese pseudonymen Daten sind vom Ergebnis her zu bestimmen. Sie sind, weil eine

¹⁹² S. Kap. 3.1.5.6 und 3.1.5.7.

¹⁹³ S. näher Kap. 3.1.5.6 und 3.1.5.7.

¹⁹⁴ Im Ergebnis ebenso *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 49 – Breyer; *Gola*, in: ders., Art. 4 Rn. 19f.; *Ziebarth*, in: Sydow, Art. 4 Rn. 91, 97.

¹⁹⁵ So aber z.B. *Klabunde*, in: Ehmann/Selmayr, Art. 4 Rn. 15.

Identifizierung der betroffenen Person durch sie ausgeschlossen ist,¹⁹⁶ entsprechend der Definition in Art. 4 Nr. 1 DSGVO keine personenbezogenen Daten.¹⁹⁷ Insbesondere für den Gesundheitsbereich hat die Art. 29-Datenschutzgruppe festgestellt, dass pseudonyme Daten, wenn der Verantwortliche die Zuordnungsregel nicht kennen kann, keine personenbezogenen Daten sind.¹⁹⁸ Werden z.B. im Rahmen eines Forschungsprojekts mögliche Identifizierungsmerkmale ausreichend sicher von den erhobenen Nutzdaten getrennt und durch ein Pseudonym ersetzt und wird die Zuordnungsregel einer anderen unabhängigen Stelle übergeben (z.B. Notar), der sie den Forschenden nicht zugänglich machen darf, sind die Nutzdaten für die Forschenden anonym. Dies dürfte für die Nachnutzung der pseudonymen Nutzdaten durch andere Forscher aus einer anderen Forschungseinrichtung vielfach der Fall sein.

Die zweite Art pseudonymer Daten bewirkt, dass die Risiken der Datenverarbeitung für die betroffene Person vermindert werden.¹⁹⁹ Diese risikoreduzierende Wirkung erreichen sie dadurch, dass im Verarbeitungsprozess die zu verarbeitenden Daten und das Zusatzwissen, das die Identifizierung der betroffenen Person ermöglicht, sicher getrennt sind. Diese Sicherungen erreichen jedoch nicht das Niveau, dass eine Zuordnung der Daten durch den Datenverarbeiter ausreichend verlässlich ausgeschlossen ist. Diese zweite Art pseudonymer Daten sind für den Verarbeiter personenbezogen und unterfallen der Datenschutz-Grundverordnung.²⁰⁰ Mit dieser zweiten, risikomindernden Art pseudonymer Daten würden z.B. Forschende arbeiten, die zwar in der Regel nur das Pseudonym kennen, aber in einem Ausnahmefall bei dem Inhaber der Zuordnungsregel die Aufhebung der Pseudonymität fordern können, um Inkonsistenzen oder Unplausibilitäten aufzulösen. Für sie wären die Nutzdaten nicht anonym, sondern personenbezogen.

Diese Unterscheidung kennen auch die Definitionen des § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F., wenn sie Pseudonymisieren definieren als „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“. „Die Bestimmung des Betroffenen auszuschließen“, entspricht der anonymisierenden Wirkung der Pseudonymisierung für den Verantwortlichen, der die Zuordnungsregel nicht kennen kann. „Die

196 S. zu den Anforderungen an diese Art der Pseudonymisierung Kap. 3.3.3.

197 S. *EuGH*, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 47–49 – Breyer; *Ziebarth*, in: *Sydow*, Art. 4 Rn. 25, 91, 98; *Ziebarth*, CR 2015; 687 (691); *Laue/Nink/Kremer*, § 1 Rn. 29f.; *Knopp*, DuD 2015, 527 (528); *Kroschwald* 2015, 74; *Buchner*, in: *Taege/Gabel*, § 3 Rn. 47f.; *Scholz*, in: *Simitis*, § 3 Rn. 217a; *Gola/Schomerus*, § 3 Rn. 46; *Tinnefeld*, in: *Roßnagel* 2003, Kap. 4.1 Rn. 30; grundsätzlich *Roßnagel/Scholz*, MMR 2000, 721 (724f.); *Roßnagel/Pfitzmann/Garstka* 2002, 103; *Stiernerling/Hartung*, CR 2012, 60 (63). Unklar *Karg*, DuD 2015, 520 (524): „wirkt ... anonym, ohne es ggfs. rechtlich zu sein“; a.A. z.B. *Schaar* 2002, 74.

198 Art. 29-Datenschutzgruppe, WP 136, 20.

199 S. hierzu auch *Gola*, in: *ders.*, Art. 4 Rn. 41.

200 S. zu den Anforderungen an diese Art der Pseudonymisierung Kap. 3.3.3.

Bestimmung des Betroffenen zu erschweren“, entspricht der zweiten, der risikomindernden Art pseudonymer Daten. Diese pseudonymen Daten sind aber weiterhin personenbezogene Daten.²⁰¹

Zwar unterscheidet sich der Wortlaut²⁰² der Definition von Pseudonymisierung in Art. 4 Nr. 5 DSGVO, die lautet

„Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“,

vom Wortlaut der Definition in § 3 Abs. 6a BDSG a.F., die deutlich kürzer gefasst ist als

„Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“

Bezogen auf die Nutzdaten fordern beide Definitionen, dass diese nach der Pseudonymisierung nicht mehr ohne die Zuordnungsregel einer spezifischen betroffenen Person zugeordnet werden können. Nach beiden Definitionen muss dadurch der Personenbezug der Nutzdaten ausgeschlossen sein. Im Gegensatz zu Art. 4 Nr. 1 DSGVO differenziert § 3 Abs. 6a BDSG a.F. diese Folge dahingehend, dass die Bestimmung des Betroffenen ausgeschlossen oder wesentlich erschwert sein kann. Diese zweite Alternative entsteht für die Datenschutz-Grundverordnung aber ebenfalls, wenn der Widerspruch zwischen Art. 4 Nr. 1 DSGVO und Erwägungsgrund 26 Satz 2 DSGVO durch ein Nebeneinander zweier möglicher Folgen aufgelöst wird.²⁰³ In dieser Interpretation sind die Anforderungen an die Nutzdaten in beiden Definitionen identisch.²⁰⁴

Bezogen auf die Zuordnungsregel geht Art. 4 Nr. 1 DSGVO jedoch über die Definition in § 3 Abs. 6a BDSG hinaus. Während das Bundesdatenschutzgesetz a.F. den Umgang mit der Zuordnungsregel nur implizit durch die beiden Folgen regelt, nach denen die Zuordnung ausschließt oder erschwert, stellt die Datenschutz-Grundverordnung explizite Forderungen: Sie muss gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen

201 S. hierzu auch *Tinnefeld*, in: Roßnagel 2003, Kap. 4.1 Rn. 30; *Knopp*, DuD 2015, 527 (528).

202 Zum Vergleich des Wortlauts des Art. 4 Nr. 5 und § 3a BDSG a.F. und § 67 Abs. 8a SGB X a.F. s. auch Kap. 3.3.4.

203 S. hierzu oben.

204 So z.B. auch *Gola*, in: Gola, Art. 4 Rn. 36.

unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können. Diese Forderung gilt für beide möglichen Folgen gleichermaßen – können sich aber danach unterscheiden, dass sie den Personenbezug der Nutzdaten ausschließen oder erschweren. Insofern enthält die Definition in Art. 4 Nr. 1 präzisere Vorgaben als die Definition in § 3 Abs. 6a BDSG a.F., ist aber auch wie diese am Erfolg orientiert.

Für den Inhaber der Zuordnungsregel sind beide Arten pseudonymer Daten personenbezogen. Dies ist der entscheidende Unterschied zur Anonymisierung. Während eine wirksame Anonymisierung die Identifizierung der betroffenen Person auch für denjenigen ausschließt, der sie durchführt, behält derjenige, der eine Pseudonymisierung durchführt, zusätzliche Informationen (Zuordnungsregel), die ihm ermöglichen ein Pseudonym einer betroffenen Person zuzuordnen.²⁰⁵

Diese zweite Art risikomindernder pseudonymer Daten wird von Erwägungsgrund 28 DSGVO angesprochen:

„Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der ‚Pseudonymisierung‘ in dieser Verordnung ist nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen.“

Für die erste Art der Pseudonymisierung besteht der Anreiz darin, dass der Datenverarbeiter, der die Zuordnungsregel nicht kennen kann, keine personenbezogenen Daten verarbeitet und damit aus dem Anwendungsbereich der Datenschutz-Grundverordnung herausfällt. Die Anreize für die zweite Art der Pseudonymisierung, die nur risikomindernd, aber nicht anonymisierend wirkt, sind Thema des Erwägungsgrunds 29 DSGVO:

„Um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um – für die jeweilige Verarbeitung – die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden. Der für die Verarbeitung der personenbezogenen Daten Verantwortliche, sollte die befugten Personen bei diesem Verantwortlichen angeben.“

²⁰⁵ S. hierzu Roßnagel/Scholz, MMR 2000, 721ff.

Für die Pseudonymisierung der zweiten Art liegt der Anreiz für den Verantwortlichen in der Erleichterung der Datenverarbeitung. Mit der Verwendung pseudonymer Daten kann er

- eher eine für sich günstige Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO durchführen,
- eher eine mit dem Primärzweck vereinbare Weiterverarbeitung nach Art. 6 Abs. 4 DSGVO annehmen,
- seiner Pflicht zu einer datenschutzfreundlichen Systemgestaltung nach Art. 25 Abs. 1 DSGVO genügen,
- sich seine Aufgabe der Datensicherung nach Art. 32 Abs. 1 DSGVO erleichtern,
- allgemein seiner Verantwortung nach Art. 5 Abs. 2 und 24 DSGVO gerecht werden,
- sich Benachrichtigungen bei Datenschutzverletzungen gemäß Art. 34 Abs. 3 lit. a DSGVO ersparen,
- leichter eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO bestehen und
- seiner Pflicht, ausreichende Garantien für eine Datenverarbeitung für statistische, wissenschaftliche und archivarische Zwecke nach Art. 89 Abs. 1 Satz 1 und 3 DSGVO zu bieten, genügen.

Wie Erwägungsgrund 29 Satz 1 DSGVO ausdrücklich festhält, sollten durch risikomindernde Pseudonymisierung – gemäß Art. 6 Abs. 1 UAbs. 1 lit. f und Abs. 4 DSGVO – mit den pseudonymen Daten allgemeine Analysen bei demselben Verantwortlichen zulässig sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 4 Nr. 5 DSGVO getroffen hat. Dadurch sollen statistische Untersuchungen und ähnliche Maßnahmen in Unternehmen, Unternehmensgruppen²⁰⁶ und Behörden, insbesondere aber auch in der Forschung möglich sein, obwohl es sich bei diesen pseudonymen Daten um personenbezogene Daten entsprechend Erwägungsgrund 26 Satz 2 DSGVO handelt. Die Pseudonymisierung kann der Verantwortliche in diesem Fall selbst vornehmen.²⁰⁷

3.3.2 Bewertung der Pseudonymisierung durch den Europäischen Gerichtshof

Das Urteil des Europäischen Gerichtshofs vom 19. Oktober 2016²⁰⁸ befasst sich zwar nicht ausdrücklich mit dem Thema der Pseudonymisierung, sondern mit der Frage des Personenbezugs von IP-Adressen, wenn ein Dritter über die relevanten Zusatzinformationen verfügt. Genau diese Konstellation kann aber auch bei pseudonymen Daten vorliegen. Von manchen werden IP-Adressen auch als

206 S. Laue/Nink/Kremer 2016, § 1 Rn. 31.

207 S. z.B. Albrecht/Jotzo 2017, Teil 3 Rn. 4

208 EuGH, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Breyer.

pseudonyme Daten angesehen. Insofern können aus dem Urteil Schlussfolgerungen abgeleitet werden, wenn es um die Frage geht, ob die pseudonymen Daten für einen Verantwortlichen personenbezogen sind, wenn die Zuordnungsregel ihm unbekannt ist, aber bei einem Dritten liegt. Diese Frage bezieht sich nur auf die erste Art pseudonymer Daten, die die Wirkung anonymer Daten haben können. Folgende Erkenntnisse aus dem Urteil sind übertragbar:

Der Europäische Gerichtshof geht zwar von einem relativen Personenbezug aus. IP-Adressen stellen isoliert betrachtet kein personenbezogenes Datum dar.²⁰⁹ Das muss auch für pseudonymisierte Daten gelten. Er hat aber festgestellt, dass nicht allein auf das Zusatzwissen des Verantwortlichen abzustellen ist, sondern dass unter bestimmten Bedingungen auch das Zusatzwissen eines Dritten relevant sein kann.²¹⁰ Dieses Zusatzwissen Dritter ist dem Verantwortlichen dann zurechenbar, wenn das Zusatzwissen des Dritten „ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann“.²¹¹ Der Gerichtshof nennt zwei Gründe, nach denen dies nicht der Fall ist. Erstens ist die Berücksichtigung des Zusatzwissens Dritter dann ausgeschlossen, „wenn die Identifizierung der betreffenden Person gesetzlich verboten“ ist. Zweitens bleibt das Zusatzwissen Dritter unberücksichtigt, wenn die Identifizierung „praktisch nicht durchführbar“ ist, „z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften“ erfordert, sodass das Risiko einer Identifizierung de facto vernachlässigbar ist.²¹² Dabei sind auch mögliche Umwege, auf denen das Zusatzwissen zum Verantwortlichen gelangen kann, zu berücksichtigen. Auch wenn es nicht erlaubt ist, die Daten direkt zu übermitteln, kann es – wie im zu entscheidenden Fall – möglich sein, das Zusatzwissen über Akteneinsicht bei einer zuständigen Behörde zu erlangen.²¹³ In diesem Fall verfügt der Verantwortliche über vernünftigerweise einsetzbare rechtliche Mittel.²¹⁴

Der Europäische Gerichtshof stellt letztlich auf das Risiko der Identifizierung ab. Dies entfällt, wenn die Preisgabe des Zusatzwissens und die Identifizierung der betroffenen Person „gesetzlich verboten“ ist. Der Gerichtshof musste in dem zu entscheidenden Fall nicht darüber entscheiden, wie wahrscheinlich die Verwendung nur rechtswidrig zu erlangender Zusatzinformationen sein muss. So bleibt nach dem Urteil offen, ob die Risikoprognose auch den Anreiz rechtswidrigen Verhaltens, die Leichtigkeit der Grenzübertretung und Anhaltspunkte für die Gefahr eines nicht rechtskonformen Zugriffs auf das Zusatzwissen berücksichtigen muss.²¹⁵

209 S. Moos/Rothkegel, MMR 2016, 845 (846).

210 EuGH, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 43, Breyer.

211 EuGH, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 44, Breyer.

212 EuGH, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 46, Breyer.

213 S. hierzu ausführlich Moos/Rothkegel, MMR 2016, 845 (846).

214 EuGH, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779, Rn. 47–49, Breyer.

215 Dafür wohl Kühling/Klar, ZD 2017, 28.

3.3.3 Anforderungen an den Pseudonymisierungsprozess

Die Datenschutz-Grundverordnung gibt keine Verfahren zur Pseudonymisierung vor. Sie erkennt jedoch die verwendeten Verfahren nur dann als Pseudonymisierung nach Art. 4 Nr. 5 DSGVO an, wenn sie zwei Voraussetzungen erfüllen. Sie müssen erstens die Daten so verarbeiten, dass sie „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“. Zweitens müssen die „zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

Allerdings fordert die Datenschutz-Grundverordnung – jedoch nicht ausdrücklich – ein bestimmtes Maß an Qualität der Pseudonymisierung.²¹⁶ Solche Qualitätsanforderungen ergeben sich aber indirekt durch die Einordnung der pseudonymen Daten in den Begriff der personenbezogenen Daten.²¹⁷ Je nach intendiertem Charakter der pseudonymen Daten sind unterschiedliche Anforderungen an den Pseudonymisierungsprozess zu stellen:

Sollen die pseudonymen Daten der ersten Art unterfallen und für den sie nutzenden Verantwortlichen die Eigenschaft anonymer Daten haben, dürfen sie im Ergebnis keine personenbezogenen Daten sein. Sie müssen also ausschließen, dass der Verantwortliche durch sie bestimmte natürliche Personen identifizieren kann. Hierfür gelten die gleichen Anforderungen wie für die Anonymisierung.²¹⁸ Ob ein Personenbezug ausgeschlossen ist, richtet sich nicht nach der Einhaltung eines bestimmten Verfahrens. Auch die gesonderte und gesicherte Aufbewahrung der „zusätzlichen Informationen“ garantiert keine Anonymität. Vielmehr muss eine Identifizierbarkeit der betroffenen Person mit den verfügbaren Mitteln nach allgemeinem Ermessen ausgeschlossen sein.

Um ausreichend sicherzugehen, dass eine Identifizierung der betroffenen Person ausgeschlossen ist, muss neben einem guten Verfahren zum Ersetzen der identifizierenden Merkmale²¹⁹ auch die besondere Schwachstelle, das Vorhandensein zusätzlicher identifizierender Informationen, ausreichend abgesichert werden.

Die Wiederherstellbarkeit des Personenbezugs führt daher zu einem fortdauernden Schutzbedarf der betroffenen Person. Es muss dauerhaft sichergestellt sein, dass nur der berechtigte Inhaber der Zuordnungsregel über diese verfü-

²¹⁶ Marnau, DuD 2016, 428 (430).

²¹⁷ S. hierzu Roßnagel/Scholz, MMR 2000, 721 (723f.).

²¹⁸ S. Kap. 3.2.3.

²¹⁹ Art. 29-Datenschutzgruppe, Stellungnahme 5/2014, WP 216, 13ff.

gen kann und alle anderen sicher davon ausgeschlossen sind.²²⁰ Dies kann zum einen dadurch gewährleistet werden, dass die Pseudonymisierung von einem vertrauenswürdigen unabhängigen Dritten durchgeführt wird, der auch die Zuordnungsregel aufbewahrt. Dieser muss ausreichende Garantien dafür bieten, dass er die Zuordnungsregel keinem anderen zur Kenntnis kommen lässt. Hier können die Kriterien des Europäischen Gerichtshofs für die Bestimmung personenbezogener Daten unter Zurechnung des Wissens Dritter²²¹ in umgekehrter Weise zur Anwendung kommen. Für den Verantwortlichen darf es keinen rechtlich möglichen Weg geben, die Zuordnungsregel zu erfahren, und auch keinen anderen praktisch gangbaren Weg, mit verhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskräften an die Zuordnungsregel zu gelangen.

Um besonders sicherzugehen, dass die pseudonymen Daten nur in den wenigen vorgesehenen Fällen (z.B. bei der medizinischen Forschung Kontakt mit der betroffenen Person in deren Interesse) zugeordnet werden können, kann eine mehrfache Pseudonymisierung erfolgen. Werden z.B. Daten in einem Krankenhaus gewonnen, kann dieses die erste Pseudonymisierung vornehmen, bevor die pseudonymen Daten an ein Forschungsprojekt weitergegeben werden. Dort kann dann ein Treuhänder die pseudonymen Daten ein zweites Mal pseudonymisieren und die Zuordnungsregel aufbewahren. Das Forschungsprojekt arbeitet dann mit faktisch anonymen Daten, da es selbst keine Möglichkeit hat, die betroffene Person zu identifizieren. Das Pseudonym kann nur aufgedeckt werden (und die betroffene Person kontaktiert werden), wenn zwei Stellen zusammenarbeiten, nämlich der Treuhänder und das Krankenhaus. Sollen die Daten aus dem Forschungsprojekt weitergegeben werden, empfiehlt sich eine dritte Pseudonymisierung durch das Forschungsprojekt.²²²

Sollen die pseudonymen Daten für den sie nutzenden Verantwortlichen die Eigenschaft von risikomindernden zusätzlichen Garantien für betroffene Personen haben, bleiben sie personenbezogene Daten. Sie sind allerdings in besonderer Weise gesichert, sodass von ihnen ein erheblich geringeres Risiko für die betroffenen Personen ausgeht als von sonstigen personenbezogenen Daten. Für diese zweite Art pseudonymer Daten genügt ein Pseudonymisierungsverfahren, das die Anforderungen der gesonderten und gesicherten Aufbewahrung der „zusätzlichen Informationen“ gemäß Art. 4 Nr. 5 DSGVO erfüllt. Für diese Art pseudonymer Daten ist keine Pseudonymisierung durch einen Dritten notwendig. Nach Erwägungsgrund 29 DSGVO ist für sie sogar eine interne Pseudonymisierung möglich, wenn der Verantwortliche „die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um – für die jeweilige Verarbeitung – die Umsetzung dieser Verordnung zu gewährleisten“. Hierfür hat er „sicherzustellen ..., dass zusätzliche Informationen, mit denen die

220 Knopp, DuD 2015, 527 (529).

221 S. Kap. 3.3.2.

222 S. hierzu Herbst, DuD 2016, 371 (375).

personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden“. In diesem Fall hat der Verantwortliche die bei ihm für die gesonderte Aufbewahrung „befugten Personen“ anzuweisen. Diese Personen sind in die Dokumentation nach Art. 30 DSGVO aufzunehmen. Die Sicherungsmaßnahmen für die gesondert aufbewahrte Zuordnungsregel müssen den Vorgaben des Art. 32 DSGVO entsprechen. Diese müssen sicherstellen, dass der Verantwortliche, der die pseudonymen Daten nutzt, keinen Zugang zu der Zuordnungsregel hat.

3.3.4 Vergleich mit der Rechtslage nach der Datenschutz-Richtlinie und dem geltenden Bundesdatenschutzgesetz

Der Begriff „Pseudonymisieren“ wurde erst im Jahr 2001 im Bundesdatenschutzgesetz und im Sozialgesetzbuch X legaldefiniert. Nach § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. ist Pseudonymisieren „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“. ²²³ Obwohl Art. 4 Nr. 5 DSGVO einen anderen Wortlaut hat, enthält er keine andere inhaltliche Aussage als § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. ²²⁴

Wie für Art. 4 Nr. 5 und Erwägungsgrund 26 Satz 2 DSGVO analysiert, kennen auch die Definitionen des § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. zwei Arten von pseudonymen Daten, nämlich solche, die in der Lage sind, „die Bestimmung des Betroffenen auszuschließen“, und solche, die die Identifizierung wesentlich erschweren sollen. Dementsprechend ist auch für das Bundesdatenschutzgesetz und für das Sozialdatenschutzrecht anerkannt, dass es pseudonyme Daten geben kann, die für den Verantwortlichen, der ihre Aufdeckungsregel nicht kennen kann, anonyme Daten sein können, ²²⁵ und dass es pseudonyme Daten gibt, die personenbezogene Daten sind, weil sie die Identifikation des Betroffenen nur erschweren, aber nicht ausschließen. Wie für Art. 4 Nr. 5 DSGVO gibt es auch Gegenmeinungen, die dem Konzept einer absoluten Bestimmung personenbezogener Daten anhängen. ²²⁶

Die Anforderung der gesicherten und getrennten Aufbewahrung der Zuordnungsregel, die in Art. 4 Nr. 5 DSGVO ausdrücklich aufgenommen ist, ist auch für § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. eine ungeschriebene, aber notwendige Voraussetzung, um von Pseudonymisieren und pseudonymen Daten reden zu können. ²²⁷

²²³ Zum Vergleich des Wortlauts des Art. 4 Nr. 5 und § 3a BDSG a.F. s. auch Kap. 3.3.1.

²²⁴ S. Kap. 3.3.1 sowie aus der Literatur z.B. Gola, in: ders., Art. 4 Rn. 36.

²²⁵ Scholz, in: Simitis, § 3 BDSG, Rn. 217a ff.; Roßnagel/Scholz, MMR 2000, 721 (724); Stiernerling/Hartung, CR 2012, 60 (63); Kroschwald 2015, 74.

²²⁶ S. z.B. Schaar 2002, 74, Rn. 218; Pahlen-Brandt, DuD 2008, 34 (35).

²²⁷ Roßnagel/Scholz, MMR 2000, 721 (724); Scholz, in: Simitis, § 3 BDSG, Rn. 217a ff.

Das Urteil des Europäischen Gerichtshofs vom 19. Oktober 2016²²⁸ hat der absoluten Bestimmung des Personenbezugs eine klare Absage erteilt und im Rahmen des Konzepts eines relativen Personenbezugs Fragen zur Zuordnung von Zusatzwissen bei Dritten geklärt. Diese von ihm gegebenen Feststellungen gelten für die Datenschutz-Richtlinie und damit auch für § 3 Abs. 6a BDSG a.F. und § 67 Abs. 8a SGB X a.F. Sie entsprechen der von der herrschenden Meinung vertretenen Auffassung. Diese Feststellungen sind auch auf Pseudonyme nach Art. 4 Nr. 5 DSGVO übertragbar.²²⁹

Im Ergebnis ändert sich durch den Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25. Mai 2018 für den Begriff, die Funktion und die Rechtswirkungen der Pseudonymisierung nichts Wesentliches.

3.3.5 Ergebnis zur Pseudonymisierung

Pseudonymisierung wird – im Gegensatz zur Anonymisierung definiert – und zwar in Art. 4 Nr. 5 DSGVO. Trotz eines unterschiedlichen Wortlauts ist der Begriff in Art. 4 Nr. 5 DSGVO mit dem in § 3 Abs. 6a BDSG a.F. identisch. Im Unterschied zur Anonymisierung gibt es bei der Pseudonymisierung eine Stelle, die eine Re-Identifizierung vornehmen kann. Daher ist zwischen dem Inhaber der Zuordnungsregel und allen anderen, die die Zuordnungsregel nicht kennen, zu unterscheiden.

Von der Rechtsfolge her können in beiden Vorschriften zwei Arten von pseudonymen Daten unterschieden werden, je nachdem, ob sie die Zuordnung zu einer bestimmten Person für alle, die die Zuordnungsregel nicht kennen, ausschließen oder nur erschweren. Im ersten Fall sind pseudonyme Daten für den Verantwortlichen keine personenbezogenen Daten, im zweiten Fall bleiben sie es. Nicht personenbezogen sind pseudonyme Daten nach dem Urteil des Europäischen Gerichtshofs vom 19. Oktober 2016, wenn die Identifizierung der betroffenen Person gesetzlich verboten ist oder wenn die Identifizierung „praktisch nicht durchführbar“ ist, „z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften“ erfordert, sodass „das Risiko einer Identifizierung de facto vernachlässigbar“ ist. Für den Kenner der Zuordnungsregel sind die Daten immer personenbezogen.

Die Datenschutz-Grundverordnung gibt keine spezifischen Verfahren zur Pseudonymisierung vor. Sie erkennt jedoch die verwendeten Verfahren nur dann als Pseudonymisierung nach Art. 4 Nr. 5 DSGVO an, wenn sie zwei Voraussetzungen erfüllen. Sie müssen erstens die Daten so verarbeiten, dass sie „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können“. Zweitens müssen die

²²⁸ EuGH, Urteil vom 19.10.2016, C-582/14, ECLI:EU:C:2016:779 – Breyer.

²²⁹ S. hierzu Kap. 3.3.2.

„zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

3.4 Löschung durch Anonymisierung?

Das folgende Kapitel beantwortet die Frage 4.4. Diese lautet:

Kann eine wirksame Anonymisierung von Daten als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 EU-DSGVO angesehen werden? Gehen Sie bitte auch darauf ein, ob eine wirksame Anonymisierung ausreichend ist, wenn die Löschung im Rahmen einer Einwilligung vereinbart wurde.

Art. 17 Abs. 1 DSGVO sieht in sechs Fällen ein Recht und eine Pflicht zur Löschung vor. Um die Daten weiterhin nutzen zu können, stellt sich die Frage, ob in diesen sechs Fällen eine wirksame Anonymisierung von Daten als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 DSGVO angesehen werden kann.

Für die Beantwortung der Frage ist jedoch immer zu beachten, dass eine Löschung personenbezogener Daten voraussetzt und keine Löschung erforderlich ist und eingefordert werden kann, wenn die Daten anonymisiert sind.²³⁰

3.4.1 Löschung nach der Datenschutz-Grundverordnung

Nach Art. 17 Abs. 1 DSGVO hat

„die betroffene Person ... das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.*
- b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.*
- c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.*

²³⁰ S. hierzu genauer Kap. 3.4.3.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.“

Der Begriff des Löschens ist in der Datenschutz-Grundverordnung im Gegensatz zu § 3 Abs. 4 Nr. 5 BDSG a.F. und § 67 Abs. 6 Nr. 5 SGB X a.F. nicht definiert. Er ist in Art. 4 Nr. 2 DSGVO nur als eine Form der Datenverarbeitung erwähnt.

Aus der funktionalen Verwendung des Begriffs „Löschen“ in Art. 17 Abs. 1 DSGVO und aus dem Wortsinn ist abzuleiten, dass „Löschen“ eine Handlungsform beschreibt, die dazu dient, dass Daten nicht mehr verwendet werden können.²³¹ Dem entsprechend ist „Löschen“ in § 3 Abs. 4 Nr. 5 als „das Unkenntlichmachen gespeicherter personenbezogener Daten“ definiert.²³² In diesem Sinn ist „Löschen“ auch in Art. 4 Nr. 1 DSGVO zu verstehen.²³³ Löschen ist nur auf einem elektronischen Datenträger möglich.²³⁴ Das Löschen kann auf unterschiedliche Weise erfolgen. Entscheidend ist, dass es unmöglich ist, die zuvor in den zu löschenden Daten erfassten Informationen wahrzunehmen.²³⁵ Unzureichend ist das schlichte Entfernen eines Verweises auf bestimmte Daten in einem Register oder das Überschreiben der Daten in einer Datei.²³⁶ Notwendig ist, dass die Daten nach dem „Löschen“ nicht wiederhergestellt und in irgendeiner sinnvollen Weise verwendet werden können.²³⁷ Das Löschen ist auf allen Datenträgern des Verantwortlichen vorzunehmen und muss auch alle Sicherungskopien erfassen.²³⁸ Eine „Vernichtung“ der Daten ist nicht gefordert. Diese Handlungsform ist neben dem Löschen in Art. 4 Nr. 2 DSGVO eigens erwähnt. Unter Vernichten ist im Unterschied zum Löschen die physische Beseitigung der Daten zu verstehen.²³⁹ Dies wäre etwa durch Zerstören der Datenträger möglich, wenn man sicher sein kann, dass die Daten nur auf den zerstörten Datenträgern gespeichert waren.

231 S. Herbst, in: Kühling/Buchner, Art. 4 Rn. 36; Reimer, in: Sydow, Art. 4 Rn. 75: das Datum soll „nicht mehr ausgelesen“ werden können.

232 Dammann, in: Simitis, § 3 Rn. 172ff.

233 Herbst, in: Kühling/Buchner, Art. 4 Nr. 2 Rn. 36 und Art. 17 Rn. 37; Reimer, in: Sydow, Art. 4 Rn. 75.

234 Ernst, in: Paal/Pauly, Art. 4 Rn. 34.

235 Herbst, in: Kühling/Buchner, Art. 4 Nr. 2 Rn. 36 und Art. 17 Rn. 37.

236 Sie hierzu das in Dammann, in: Simitis, § 3 Rn. 179 erwähnte Sonderproblem der Löschung eines zwei Datensätze verbindenden Elements.

237 Herbst, in: Kühling/Buchner, Art. 17 Rn. 38f.

238 Herbst, in: Kühling/Buchner, Art. 4 Nr. 2 Rn. 36 und Art. 17 Rn. 41f.

239 Ernst, in: Paal/Pauly, Art. 4 Rn. 34.

Genau genommen muss jede Anonymisierung auch eine Löschung enthalten, nämlich die der Identifizierungsmerkmale. Denn solange diese noch im Datensatz sind, können die Daten nicht anonym sein. Insofern ist Anonymisieren immer auch ein teilweises Löschen der personenbezogenen Daten (bis sie nicht mehr personenbezogen sind). Insofern ist zu fragen, ob die Löschpflicht bereits mit der Teillöschung durch Anonymisierung erfüllt werden kann.

Löschen soll jedoch dazu führen, dass gespeicherte personenbezogene Daten vollständig unkenntlich gemacht werden, sodass sie nicht mehr verarbeitet, ausgelesen oder wahrgenommen werden können. Dagegen verändert Anonymisieren nur die gespeicherten Daten. Dies erfolgt zwar auf eine Weise, dass die Daten nicht mehr einer betroffenen Person zugeordnet werden können. Die Daten sind aber weiterhin verarbeitbar, auslesbar und wahrnehmbar. Anonymisieren und Löschen führen somit zu unterschiedlichen Ergebnissen. Insofern kann eine Löschpflicht nicht durch Anonymisieren der Daten erfüllt werden.

Soweit der Unionsgesetzgeber für bestimmte Situationen das Löschen als Rechtsfolge vorschreibt, kann dem eine Anonymisierung der Daten nicht genügen. Dies ist auf jeden Fall anzunehmen, wenn nach Art. 17 Abs. 1 lit. e DSGVO die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, der der Verantwortliche unterliegt. Dies gilt aber auch, wenn nach lit. d die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder unrichtig sind.²⁴⁰ In diesem Fall sollen die Daten vollständig beseitigt werden. Dagegen könnte für Fälle der Zweckerreichung nach lit. a, des Widerrufs einer Einwilligung nach lit. b oder der Einlegung eines Widerspruchs nach lit. c eine Anonymisierung eventuell die Interessen der jeweils betroffenen Person ebenso erfüllen. Allerdings hat der Unionsgesetzgeber auch für diese Fälle eine andere Wertung und Entscheidung getroffen.²⁴¹

Löschen und Anonymisieren sind aber auch in diesen Fällen für die betroffenen Personen nicht gleichwertig, weil sie zu unterschiedlichen Risiken führen. Löschung heißt, dass das Risiko eines Missbrauchs der Daten vollkommen beseitigt ist. Eine faktische Anonymisierung, die nach Art. 4 Abs. 1 DSGVO für eine Aufhebung des Personenbezugs ausreichend ist,²⁴² bewirkt zwar, dass die Zuordnung der Daten zu einer betroffenen Person nach allgemeinem Ermessen ausgeschlossen ist, führt aber zu einem Restrisiko, das beim Löschen nicht mehr besteht.

Außerdem ist ergänzend zur Löschung in Art. 17 Abs. 2 DSGVO vorgesehen, dass ein zur Löschung verpflichteter Verantwortlicher vertretbare Schritte

240 S. Erwägungsgrund 39 DSGVO.

241 S. Erwägungsgrund 65 Satz 2 und 3 DSGVO.

242 S. Kap. 3.1.5.6 und 3.2.1.

unternehmen muss, um weitere Verantwortliche darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat.²⁴³ Diese Informationspflicht geht über die bisherige Löschpflicht hinaus.²⁴⁴ Diese wird durch eine Anonymisierung nicht erfüllt und ist auch nicht deren notwendige Folge.

Als Ergebnis ist festzuhalten, dass eine wirksame Anonymisierung von Daten nicht als Umsetzung der Löschpflicht nach Art. 17 Abs. 1 DSGVO angesehen werden kann.

3.4.2 Ausnahmen zur Löschpflicht

Nicht eine andere Form des Löschens, sondern Ausnahmen zur Löschpflicht und zum Löschanpruch²⁴⁵ regelt Art. 17 Abs. 3 DSGVO. Nach lit. d gelten die Absätze 1 und 2 dieser Vorschrift nicht, soweit die Verarbeitung erforderlich ist, „für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt“. Soweit die Ausnahme nach Abs. 3 gilt, beseitigt sie nicht nur Löschananspruch und Löschpflichten, sondern auch die Rechtsgrundlagen für ein Löschen der erfassten Daten als Form der Datenverarbeitung.²⁴⁶

Die Ausnahme nach Art. 17 Abs. 3 lit. d DSGVO setzt eine bestimmte Prognose der Folgen der Datenlöschung voraus. Bezogen auf die Forschung muss diese Prognose ergeben, dass durch die Löschung der spezifischen Daten der Zweck der Forschung zumindest ernsthaft gefährdet ist. Dies ist etwa anzunehmen, wenn eine bestimmte Erkenntnis nicht gewonnen, bestimmte Untersuchungen nicht durchgeführt oder die für den Forschungszweck notwendige Vollständigkeit des Datensatzes nicht erreicht werden kann.²⁴⁷

Der Bezug auf Art. 89 Abs. 1 DSGVO ist so zu verstehen, dass die Ausnahme nur dann greift, wenn die nach dieser Vorschrift erforderlichen geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person bestehen.²⁴⁸ Nach Art. 89 Abs. 1 Satz 2 DSGVO muss sichergestellt sein, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen

²⁴³ S. Erwägungsgrund 66 DSGVO.

²⁴⁴ S. Roßnagel/Geminn/Jandt/Richter 2016, 170.

²⁴⁵ Herbst, in: Kühling/Buchner, Art. 17 Rn. 70.

²⁴⁶ Herbst, in: Kühling/Buchner, Art. 17 Rn. 70.

²⁴⁷ Herbst, in: Kühling/Buchner, Art. 17 Rn. 82; Peucker, in: Sydow, Art. 17 Rn. 68; Nolte/Werkmeister, in: Gola, Art. 17 Rn. 43.

²⁴⁸ Herbst, in: Kühling/Buchner, Art. 17 Rn. 81.

Maßnahmen kann nach Satz 3 die Pseudonymisierung gehören, sofern es möglich ist, die Forschungszwecke auf diese Weise zu erfüllen.²⁴⁹ Soweit dies möglich ist, sind schließlich nach Art. 89 Abs. 1 Satz 4 DSGVO im Fall einer Weiterverarbeitung der Daten diese zu anonymisieren, soweit der Forschungszweck auch mit anonymisierten Daten erreicht werden kann.²⁵⁰

Soweit diese Ausnahme des Art. 17 Abs. 3 lit. d DSGVO greift, kann zwar nicht eine Löschpflicht oder ein Löschanspruch durch Anonymisierung der Daten erfüllt werden. Es kann jedoch die Löschpflicht oder der Löschanspruch entfallen und an seine Stelle kann eine Pflicht und ein Anspruch treten, die Daten zu anonymisieren.

3.4.3 Beseitigung des Personenbezugs durch Anonymisierung

Der Anspruch auf Löschung und die Pflicht zur Löschung gelten allerdings nur für personenbezogene Daten. Zum einen setzt die Anwendung der Datenschutz-Grundverordnung insgesamt nach Art. 3 Abs. 1 DSGVO die Verarbeitung personenbezogener Daten voraus. Zum anderen bestehen im Besonderen der Löschanspruch und die Löschpflicht nur für personenbezogene Daten. Drittens beziehen sich auch die Gründe für einen Löschanspruch und eine Löschpflicht in Art. 17 Abs. 1 lit. a, d und f ausdrücklich auf personenbezogene Daten.

Weder die Datenschutz-Grundverordnung noch Art. 17 Abs. 1 DSGVO gelten für anonyme Daten. Wenn die Daten anonymisiert worden sind, bevor der Löschanspruch oder die Löschpflicht entsteht, kommt die Datenschutz-Grundverordnung nicht zur Anwendung und es kann kein Löschanspruch geltend gemacht werden. Sind die Daten personenbezogen, wenn ein Löschanspruch gerichtlich geltend gemacht wird, kann eine Anonymisierung den entstandenen Löschanspruch nicht erfüllen.

3.4.4 Vereinbarung einer Löschung durch Anonymisierung

Sind der Löschanspruch und die Löschpflicht nicht durch Art. 17 DSGVO begründet, sondern Bedingung einer Einwilligung, kommt es auf den Inhalt der Bedingung in der Einwilligungserklärung an, ob eine Anonymisierung die Löschung ersetzen kann. Wenn die betroffene Person in die Datenverarbeitung nur eingewilligt hat, weil der Verantwortliche ihr ohne weitere Spezifizierung eine Löschung in bestimmten Situationen zugesagt hat, ist davon auszugehen, dass eine Löschung im Sinne des Art. 17 Abs. 1 DSGVO gemeint ist. In diesem Fall kann aus den genannten Gründen²⁵¹ die Anonymisierung die Löschung nicht ersetzen.

249 S. z.B. *Peucker*, in: *Sydow*, Art. 17 Rn. 67; *Nolte/Werkmeister*, in: *Gola*, Art. 17 Rn. 43.

250 S. Kap. 3.2.2.

251 S. Kap. 3.4.2.

Doch auch in diesem Fall gilt: Soweit die Daten anonymisiert worden sind, bevor der Löschanspruch und die Löschpflicht entstehen, kommen weder die Regelungen in der Datenschutz-Grundverordnung zur Einwilligung noch die Einwilligung in die Verarbeitung personenbezogener Daten selbst zur Anwendung und es kann auch kein Löschanspruch aus der bedingten Einwilligung geltend gemacht werden.

Wenn jedoch im Rahmen von AGB, in deren Geltung die betroffene Person eingewilligt hat, vereinbart wurde, dass eine Löschung auch durch eine Anonymisierung ersetzt werden kann, könnte die Einwilligung zulässig und wirksam sein. Jedenfalls gibt es in der Datenschutz-Grundverordnung keine Regelung mehr wie in § 6 Abs. 1 BDSG a.F. und § 84a SGB X a.F., nach der die Rechte der betroffenen Person unabdingbar sind und daher das Recht etwa auf Löschung nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden kann. Ob eine Einwilligung in die Datenverarbeitung unter Geltung solcher AGBs wirksam ist, hängt von den Voraussetzungen des Art. 4 Nr. 11 DSGVO sowie Art. 7 DSGVO ab, insbesondere davon, dass die betroffene Person nach Art. 7 Abs. 2 DSGVO ausreichend aufgeklärt und die Einwilligung gemäß Art. 7 Abs. 4 DSGVO freiwillig erteilt worden ist.²⁵²

3.4.5 Vergleich mit der Rechtslage nach der Datenschutz-Richtlinie und dem geltenden Bundesdatenschutzgesetz

Durch die Datenschutz-Grundverordnung ändern sich weder die Anforderungen an eine Löschung noch die Einschätzung des Verhältnisses von Löschung und Anonymisierung. Nach § 3 Abs. 4 Nr. 5 BDSG a.F. und § 67 Abs. 6 Nr. 5 SGB X a.F. ist Löschen „das Unkenntlichmachen gespeicherter personenbezogener Daten“. Diesem Verständnis des Löschens wird eine Anonymisierung der Daten nicht gerecht.

Die Gründe für einen Löschanspruch und eine Löschpflicht in Art. 17 Abs. 1 DSGVO haben sich leicht gegenüber den Gründen in §§ 20 und 35 BDSG a.F. und § 84 SGB X verändert. Dies ändert aber nichts an der Grundaussage, dass eine Anonymisierung eine Löschung nicht ersetzen kann.

Neu sind allerdings die Ausnahmen von der Löschpflicht und dem Löschanspruch nach Art. 17 Abs. 3 DSGVO. Dies kann im Fall der medizinischen Forschung dazu führen, dass Löschpflicht und Löschanspruch entfallen und dafür im Fall der Weiterverarbeitung von Forschungsdaten eine Pflicht und ein Anspruch auf Anonymisierung der Daten an deren Stelle treten.²⁵³

Die Anforderungen an eine Einwilligung in Art. 4 Nr. 11 und Art. 7 DSGVO haben sich gegenüber § 4a BDSG a.F. und § 67b Abs. 2 SGB X a.F. leicht verändert.

²⁵² S. hierzu z.B. Ernst, ZD 2017, 110; Buchner/Kühling, DuD 2017, 544.

²⁵³ S. Kap. 3.4.2.

Aber auch diese Änderungen sind für das Ergebnis irrelevant, dass bei der Vereinbarung einer Löschung, die zur Bedingung einer Einwilligung wird, eine Anonymisierung nicht ausreicht. Lediglich soweit in der bedingten Einwilligung ein gesetzlicher Anspruch auf Löschung durch einen Anspruch auf Anonymisierung ersetzt wird, greift für die Datenverarbeitung nach dem bisherigen deutschen Datenschutzrecht das Dispositionsverbot nach § 6 Abs. 1 BDSG a.F. und § 84a SGB X a.F. Dieses ist in der Datenschutz-Grundverordnung entfallen.

Für alle Erwägungen greift jedoch die Feststellung, dass eine Löschung immer personenbezogene Daten voraussetzt und keine Löschung erforderlich ist und eingefordert werden kann, wenn die Daten zuvor anonymisiert worden sind.

3.4.6 Ergebnis zur Löschung durch Anonymisierung

Eine wirksame Anonymisierung von Daten kann nicht als Umsetzung der Löschpflicht oder des Löschanpruchs nach Art. 17 Abs. 1 DSGVO angesehen werden, da beide unterschiedliche Wirkungen haben. Löschpflicht oder Löschananspruch entfallen jedoch nach Art. 17 Abs. 3 DSGVO. Im Fall der Forschung im öffentlichen Interesse besteht keine Löschpflicht und kein Löschananspruch, soweit voraussichtlich die Verwirklichung der Ziele der Datenverarbeitung unmöglich gemacht oder ernsthaft beeinträchtigt werden. Soweit die Ausnahme des Art. 17 Abs. 3 lit. d DSGVO greift, kann es sein, dass die Löschpflicht oder der Löschananspruch entfallen und an ihre Stelle eine Pflicht und ein Anspruch treten, die Daten zu anonymisieren. Weiterhin ist zu beachten, dass weder die Datenschutz-Grundverordnung noch Art. 17 Abs. 1 DSGVO für anonyme Daten gelten. Wenn die Daten anonymisiert sind, bevor der Löschananspruch oder die Löschpflicht entsteht, kommt die Datenschutz-Grundverordnung nicht zur Anwendung und es besteht weder eine Löschpflicht noch ein Löschananspruch.

3.5 Vereinbarkeit der Ergebnisse mit Art. 8 GRCh und Art. 16 AEUV

Art. 8 GRCh begründet ein Recht auf Schutz personenbezogener Daten. Die Grundrechte-Charta erlangte mit dem Inkrafttreten des Vertrags von Lissabon²⁵⁴ zum 1. Dezember 2009 Rechtskraft. Sie ist damit Teil des EU-Primärrechts.²⁵⁵ Nach Art. 8 Abs. 1 GRCh hat „jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten“. Art. 8 Abs. 2 Satz 1 GRCh enthält eine Präzisierung des Schutzes, wonach Daten „nur nach Treu und Glauben

²⁵⁴ Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13.12.2007, ABl. C 306, 1.

²⁵⁵ S. auch KOM (2010) 573 endg., 3: „Mit dem Vertrag von Lissabon wurden die in der Charta verankerten Rechte, Freiheiten und Grundsätze anerkannt und dieser dieselbe Rechtsverbindlichkeit wie den Verträgen verliehen.“



für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“ dürfen. Art. 8 Abs. 2 Satz 2 GRCh erweitert den Schutz noch um ein Auskunfts- und Berichtigungsrecht. Art. 8 Abs. 3 GRCh garantiert die Überwachung des Grundrechts durch eine unabhängige Stelle.

Art. 8 GRCh stützt sich auf das europäische Sekundärrecht zum Datenschutz, insbesondere die Datenschutz-Richtlinie von 1995.²⁵⁶ Demnach ist für das Verständnis der Begriffe und die Zulässigkeit eines Eingriffs in das durch Art. 8 Abs. 1 GRCh begründete Recht auf Datenschutz auf das europäische Sekundärrecht zum Datenschutz zu verweisen.²⁵⁷ Art. 8 GRCh kann als eine Zusammenfassung des geltenden europäischen Datenschutzrechts verstanden werden. Daher orientiert sich auch der Begriff der personenbezogenen Daten an Art. 2 lit. a DSRL.²⁵⁸ Damit orientiert sich auch Art. 8 Abs. 1 GRCh für die Abgrenzung der personenbezogenen Daten von anonymen Daten und für die rechtliche Einordnung pseudonymer Daten an den Vorgaben der Richtlinie.

Auch Art. 16 Abs. 1 AEUV enthält ein Grundrecht auf Datenschutz. Dieses ist als Wiederholung von Art. 8 GRCh zu verstehen, sodass die Ausführungen zu Art. 8 GRCh auch für Art. 16 AEUV gelten.²⁵⁹

Da die Definition personenbezogener Daten in Art. 4 Nr. 1 DSGVO identisch mit der Definition in Art. 2 lit. a DSRL ist und die Definition pseudonymer Daten in Art. 4 Nr. 5 DSGVO aus der Rechtsprechung und wissenschaftlichen Diskussion um den Begriff der personenbezogenen Daten in Art. 2 lit. a DSRL hervorgegangen ist, besteht kein Zweifel, dass die beiden Regelungen der Datenschutz-Grundverordnung mit dem Grundrecht auf Datenschutz in Art. 8 GRCh und in Art. 16 Abs. 1 AEUV vereinbar sind. Dies gilt auch für das hier referierte Verständnis der anonymen Daten. Ebenso ist der Begriff des Löschens in Art. 4 Nr. 2 DSGVO identisch mit dem gleichen Begriff des Löschens in Art. 2 lit. b DSRL und damit zusammen mit dem hier referierten Bedeutungsgehalt mit Art. 8 GRCh und Art. 16 Abs. 1 AEUV vereinbar. Wie der Vergleich zwischen der neuen Rechtslage nach der Datenschutz-Grundverordnung und der bisherigen Rechtslage nach der Datenschutz-Richtlinie und ihren deutschen Umsetzungsgesetzen gezeigt hat,²⁶⁰ sind die Unterschiede sehr gering. Daher stimmen die hier gefundenen Ergebnisse mit der Datenschutzrechtslage vor Erlass des Grundrechts auf Datenschutz in Art. 8 GRCh und in Art. 16 Abs. 1 AEUV überein, die als normativer Bezugsrahmen dem Grundrecht zugrunde liegt.

²⁵⁶ S. Charta-Erläuterungen, EU ABL. C 303 vom 14.12.2007, 20.

²⁵⁷ Bernsdorff, in: Meyer 2014, Art. 8 GRCh, Rn. 17; Kingreen, in: Callies/Ruffert, Art. 8 GRCh, Rn. 5ff.

²⁵⁸ EuGH, Urteil vom 9.11.2010, Rs. C-92/09 und C-93/09, ECLI:EU:C:2010:662, Rn. 52 – Schecke; Jarass 2016, Art. 8 Rn. 5; Kingreen, in: Callies/Ruffert, Art. 8 GRCh, Rn. 9.

²⁵⁹ Sobotta, in: Grabitz/Hilf/Nettesheim 2015, Art. 16 AEUV, Rn. 8; Kingreen, in: Callies/Ruffert, Art. 16 AEUV, Rn. 3.

²⁶⁰ S. Kap. 3.1.6, 3.2.4, 3.3.4 und 3.4.5.