Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG

Kommentar

Bearbeitet von
Herausgegeben von Prof. Dr. Jürgen Kühling, LL.M., und Prof. Dr. Benedikt Buchner, LL.M. (UCLA),
Bearbeitet von Prof. Dr. Matthias Bäcker, LL.M., Matthias Bergt, Rechtsanwalt, Prof. Dr. Franziska Boehm, Prof. Dr. Johannes Caspar, Dr. Alexander Dix, LL.M., Dr. Sebastian Golla, Dr. Jürgen Hartung, Rechtsanwalt, PD Dr. Tobias Herbst, PD Dr. Silke Jandt, Dr. Manuel Klar, Rechtsanwalt, Prof. Dr. Frank Maschmann, Prof. Dr. Thomas Petri, Dr. Johannes Raab, Rechtsanwalt, Florian Sackmann, Rechtsanwalt, Dr. Christian Schröder, Rechtsanwalt, Simon Schwichtenberg, Prof. Dr. Marie-Theres Tinnefeld, Dr. Thilo Weichert, und Dr. Mirko Wieczorek

2. Auflage 2018. Buch. XXII, 1624 S. In Leinen
ISBN 978 3 406 71932 5
Format (B x L): 16,0 x 24,0 cm

Übersicht

A. Allgemeines

Der Anwendungsbereich der DS-GVO ist nur eröffnet, wenn personenbezogene Daten iSv Art. 4 Nr. 1 verarbeitet werden. Damit kommt dem Begriff des personenbezogenen Datums eine **Schlüsselrolle** zu. Das Gegenstück zum personenbezogenen Datum bildet das anonyme Datum. Dieses wird in EG 26 erläutert (→ Rn. 31). Die Definition des Personenbezugs in Art. 4 Nr. 1 sowie die zugehörigen EG haben im Rechtssetzungsverfahren nur marginale Änderungen erhalten. **1**

Nach Art. 4 Nr. 1 sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Formulierung führt im Vergleich zur bisherigen Rechtslage unter der DSRL und dem BDSG aF zu **keiner grundlegenden Änderung** im Verständnis des Personenbezugs von Daten.[1] So ist die Definition des personenbezogenen Datums in der englischsprachigen Version der DS-GVO sogar identisch mit der englischen Fassung von Art. 2 lit. a DSRL. Auch soweit die DS-GVO nunmehr die Begriffe „identifiziert" und „identifizierbar" sowie die Formulierung „Informationen, die sich […] beziehen" verwendet, statt wie die DSRL und das BDSG aF von „bestimmt" und „bestimmbar" sowie von „Informationen über" bzw. „Einzelangaben über" zu sprechen, ändert sich hierdurch an der Reichweite des Personenbezugs nichts. Dasselbe gilt mit Blick auf den Umstand, dass es nunmehr nicht mehr auf die zusätzlichen Merkmale („Einzelangabe", „persönliche oder sachliche Verhältnisse") ankommt, die noch das BDSG aF in dessen § 3 Abs. 1 gefordert hatte.[2] **2**

B. Personenbezogene Daten

I. Persönlicher Schutzumfang

1. Betroffene Person. Personenbezogene Daten sind nur solche Informationen, die sich auf eine natürliche Person beziehen. Die DS-GVO nennt diese Personen „betroffene Personen" (zum Vorliegen mehrerer betroffener Personen → Rn. 15 f.). Auch Nicht-EU-Bürger fallen hierunter, wenn ihre Daten durch Verantwortliche oder Auftragsverarbeiter im Geltungsbereich von Art. 3 verarbeitet werden (vgl. → Art. 3 Rn. 36). **3**

[1] Ebenso *Karg* DuD 2015, 520 (521); *Krügel* ZD 2017, 455.
[2] *Krügel* ZD 2017, 455; kritisch zu den teils redundanten Merkmalen *Klar,* Datenschutzrecht und die Visualisierung des öffentlichen Raums, 167.

4 **2. Natürliche versus juristische Personen.** Juristische Personen, Personenmehrheiten und -gruppen sind aus dem Schutzbereich **ausgenommen**. Soweit Informationen über die Personengruppe aber auf ein identifiziertes oder identifizierbares Mitglied „durchschlagen", handelt es sich bei der Information um ein personenbezogenes Datum.[3] Dies kann etwa der Fall sein, wenn eine Angabe zur finanziellen Situation einer Personengesellschaft oder einer „Ein-Mann-GmbH" gemacht wird (zur Abgrenzung zu Sachdaten → Rn. 12 ff.).

5 **3. Verstorbene.** Daten Verstorbener stellen nach EG 27 **keine personenbezogenen Daten** dar. Allerdings können bestimmte Daten eines Verstorbenen einen Bezug zu einer lebenden Person haben und insoweit einen Personenbezug aufweisen.[4] So ist beispielsweise die Information, der Verstorbene habe an einer Erbkrankheit gelitten, im Verhältnis zu diesem kein geschütztes Datum. Im Verhältnis zu seinem lebenden Nachkommen kann es jedoch einen Personenbezug aufweisen, sofern die Information nahe legt, dass auch dieser von der Erbkrankheit betroffen ist.

6 EG 27 enthält eine **Öffnungsklausel**, wonach die Mitgliedstaaten Vorschriften für die Verarbeitung personenbezogener Daten Verstorbener vorsehen können. Soweit ersichtlich hat Deutschland bislang weder Regelungen getroffen, die aufgrund der Öffnungsklausel weitergelten könnten, noch neue Regelungen auf Grundlage der Öffnungsklausel geschaffen.

7 **4. Ungeborene.** Ob Daten, die sich auf ein noch ungeborenes Kind (Nasciturus) beziehen, einen Personenbezug aufweisen können, wird von der DS-GVO **nicht eindeutig** beantwortet. Die Art.-29-Datenschutzgruppe hatte dies unter der DSRL noch offengelassen und die Frage dem allgemeinen Standpunkt der jeweiligen nationalen Rechtssysteme überantwortet.[5] In der deutschen datenschutzrechtlichen Literatur zum BDSG aF war diese Frage seitdem umstritten.[6] Da EG 27 jedenfalls Daten Verstorbener ausdrücklich anspricht und von der DS-GVO ausnimmt, könnte im Umkehrschluss angenommen werden, dass Daten Ungeborener unter die DS-GVO fallen sollen. In Anbetracht der Tatsache, dass die DS-GVO der betroffenen Person spezielle Rechte (Auskunft, Löschung, Berichtigung etc) einräumt, die nur eine lebende Person ausüben kann, dürfte aber ein Verständnis näher liegen, wonach Daten ungeborener Kinder keinen Personenbezug aufweisen. Unabhängig davon kann parallel zur Argumentation bei Daten Verstorbener angenommen werden, dass sich die Daten Ungeborener jedenfalls auch auf die Mutter des Ungeborenen beziehen und insoweit ein Personenbezug vorliegen kann.

II. Sachlicher Schutzumfang

8 **1. Informationen.** Art. 4 Nr. 1 umfasst ohne Einschränkung „alle Informationen", die sich auf eine Person beziehen und ist daher **grundsätzlich weit** zu verstehen. Unter die Vorschrift fallen sowohl im Kontext verwendete persönliche Informationen wie Identifikationsmerkmale (zB Name, Anschrift und Geburtsdatum), äußere Merkmale (wie Geschlecht, Augenfarbe, Größe und Gewicht) oder innere Zustände (zB Meinungen, Motive, Wünsche, Überzeugungen und Werturteile), als auch sachliche Informationen wie etwa Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen und alle sonstigen Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt.

---

[3] *Art.-29-Datenschutzgruppe,* Stellungn. 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2007, 27; so zum BDSG aF *Dammann* in Simitis BDSG § 3 Rn. 19; *Gola/Schomerus* BDSG § 3 Rn. 11a.

[4] *Art.-29-Datenschutzgruppe,* Stellungn. 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2007, 26.

[5] *Art.-29-Datenschutzgruppe,* Stellungn. 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2007, 26 f.

[6] Dagegen für das BDSG aF *Gola/Schomerus* BDSG § 3 Rn. 12.

Nach Auffassung des BVerfG, der auch auf europäischer Ebene gefolgt wird, gibt es unter den Bedingungen der automatisierten Datenverarbeitung **kein belangloses Datum.**[7] Daher kommt es auf den Aussagegehalt und die persönlichkeitsrechtliche Implikation der Information nicht an. Bei der Beurteilung des Personenbezugs ist daher anders als etwa im Rahmen der Zulässigkeitstatbestände (vgl. etwa Art. 6 Abs. 1 S. 1 lit. f) keine Interessenabwägung vorzunehmen. Selbst die Information, dass Person X zwei Arme hat, stellt ein personenbezogenes Datum iSv Art. 4 Nr. 1 dar. Unerheblich ist auch die **Herkunft und Ausgestaltung** der Information. Umfasst sind demnach alle Informationen, seien sie in Form von Sprache, Schrift, Zeichen, Bild oder Ton, digital oder analog. **9**

Auch statistische **Wahrscheinlichkeitsaussagen** und nicht lediglich völlig abstrakte **Prognose- oder Planungswerte**, die eine subjektive und/oder objektive Einschätzung zu einer identifizierten oder identifizierbaren Person liefern (zB Ausfallwahrscheinlichkeit eines Kredits), weisen einen Personenbezug auf.[8] Dies ist beispielsweise der Fall, wenn einer Person im Rahmen einer Bonitätsbewertung ein sog. Scorewert zugewiesen oder sie in eine Kaufkraftklasse eingeordnet wird.[9] Dasselbe gilt, wenn in Suchmaschinen als Ergänzung zu einer Namenssuchanfrage Vorschläge zum Namensträger eingeblendet werden (sog. Autovervollständigen).[10] **10**

2. Bezug zu Person. Ausweislich Art. 4 Nr. 1 muss sich die Information „auf eine natürliche Person beziehen". Dass sich die Information auf eine Person und nicht nur auf mehrere Personen oder eine Sache beziehen muss, ist **eigenständiges Merkmal** der Definition des personenbezogenen Datums.[11] Es ist losgelöst vom Kriterium der Identifizierbarkeit der Person (→ Rn. 19 ff.) zu prüfen. **11**

a) Abgrenzung zu Sachdaten. Keinen Bezug zu einer Person weisen sog. **Sachdaten** auf. Sie beziehen sich nicht auf eine Person, sondern ausschließlich auf eine Sache. Dies ist zB bei der Aussage „Der Mount Everest ist der höchste Berg der Erde" oder „Das Fertighaus X kostet 200.000 Euro" der Fall. Dies gilt selbst dann, wenn bei dem Verantwortlichen oder einem Dritten das Wissen vorhanden ist, dass Person A den Mount Everest bestiegen hat oder Eigentümerin des Fertighauses X ist. Denn in diesem Fall ist lediglich das Merkmal der Identifizierbarkeit erfüllt, nicht jedoch die Voraussetzung, dass sich die Information (von sich heraus) auf eine Person bezieht. **12**

Kein Sachdatum, sondern ein personenbezogenes Datum liegt vor, wenn in der Information über eine Sache aufgrund individualisierender Identifikationsmerkmale, des Detaillierungsgrads oder der Einzigartigkeit der Sache ein Bezug zu einer Person **angelegt** ist.[12] Dies ist etwa bei der Information der Fall, dass unter der Telefonnummer X zu einer konkreten Uhrzeit ein Anruf getätigt wurde. Durch die Angabe der Telefonnummer als eine einem konkreten Anschlussinhaber und damit einer natürlichen Person zugeordneten Kennziffer bezieht sich die Information nicht nur auf eine Sache (Telefonanschluss), sondern auch auf eine natürliche Person. Dasselbe gilt hinsichtlich der Information „In der Ludwigstraße 327 in Hannover befindet sich das Fertighaus X". Hier ist die grundsätzlich sachbezogene Information mit einer Kennziffer in Form der Georeferenzierung versehen, wodurch zugleich auch eine Information über den Lebensbereich einer konkreten Person vorliegt.[13] **13**

---

[7] BVerfG Urt. v. 15.12.1983 – 1 BvR 209/83 ua, BVerfGE 65, 1 (45).

[8] *Art.-29-Datenschutzgruppe,* Stellungn. 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2007.

[9] So für das BDSG aF *Gola/Schomerus* BDSG § 3 Rn. 3 ff.

[10] BGH Urt. v. 14.5.2013 – VI ZR 269/12, ZD 2013, 405 (405 f.).

[11] Vgl. für das BDSG aF *Dammann* in Simitis BDSG § 3 Rn. 59.

[12] Vgl. zu diesem Ansatz näher *Klar,* Datenschutzrecht und die Visualisierung des öffentlichen Raums, 139 ff.; ähnlich nun auch *Krügel* ZD 2017, 455 (457), wonach bestimmten Daten aus sich heraus ein „personenbezogener Verarbeitungszusammenhang" innewohnt.

[13] Insoweit von einem „personenbezogenen Sachdatum" sprechend *Karg* DuD 2015, 520 (522).

14 Dazwischen ist eine ganze Reihe von Streitfällen denkbar, die in jedem Einzelfall einer differenzierten Lösung zuzuführen sind. Abgrenzungsfragen stellen sich vor allem im Zusammenhang mit der sog. Machine-to-Machine-Kommunikation durch Alltagsgegenstände, die an das Internet angebunden sind, wie zB Fahrzeuge, Küchengeräte oder sog. Wearables („**Internet der Dinge**"). Insoweit ist idR nicht von Sachdaten auszugehen.[14] Die Abgrenzung vom Sachdatum zum personenbezogenen Datum kann hier nach dem kontextbezogenen Ansatz der Art.-29-Datenschutzgruppe erfolgen, den diese zum Begriff des personenbezogenen Datums aus Art. 2 lit. a DSRL entwickelt hatte. Danach bezieht sich eine Information dann auf eine natürliche Person (und nicht auf eine Sache),[15] wenn ein **Inhaltselement, ein Zweckelement oder ein Ergebniselement** vorhanden ist.[16] Ein Inhaltselement soll vorliegen, wenn unter Berücksichtigung aller Begleitumstände und unabhängig vom Zweck auf Seiten des Verantwortlichen oder eines Dritten oder von den Auswirkungen auf die betroffene Person Informationen über eine Person gegeben werden. Ein Zweckelement liegt vor, wenn es möglich ist, die Informationen zu dem Zweck der Beurteilung, Behandlung oder Beeinflussung einer Person zu verwenden. Auch ohne dass ein Inhalts- oder Zweckelement vorhanden ist, soll schließlich ein Ergebniselement immer dann vorliegen, wenn die Gefahr besteht, dass sich die Angabe unter Berücksichtigung aller Begleitumstände auf die Rechte und Interessen einer bestimmten Person auswirken kann. Dies kann etwa bei Informationen über die wirtschaftliche Nutzung und Verwertung von Immobilien der Fall sein.

15 **b) Aggregierte, statistische und mehrrelationale Daten.** Aggregierte und statistische Daten weisen in der Regel ebenfalls **keinen Personenbezug** auf, sofern sie sich nicht auf eine Person, sondern auf eine Personengruppe beziehen. So stellt etwa die Information, dass der Krankenstand der Mitarbeiter des Unternehmens A um X % zugenommen hat, kein personenbezogenes Datum dar, wenn das Unternehmen eine Vielzahl von Mitarbeitern beschäftigt. Anders kann dies zu beurteilen sein, wenn dem Unternehmen A nur wenige Mitarbeiter angehören. Wie hoch das Aggregationsniveau bzw. die Gruppengröße sein muss, damit kein Personenbezug anzunehmen ist, ist in jedem Einzelfall zu bestimmen. Leitgedanke bei der Beurteilung muss sein, ob die Information **Rückschlüsse auf eine einzelne Person** zulässt, dh auf diese „durchschlägt". Dies kann zB bei der Veröffentlichung von Ergebnissen eines Gruppenakkords wegen der Tendenzaussage der Fall sein.[17]

16 Wird eine **Aussage zu allen Personen** getroffen, die einer Gruppe angehören, bezieht sich die Information gleichzeitig auf jede einzelne identifizierte oder identifizierbare Person und es liegt folglich insoweit ein Personenbezug vor. Dies ist etwa der Fall bei der zusammenfassenden Information, dass A, B und C Mitarbeiter eines bestimmten Unternehmens sind oder dass alle Teilnehmer einer bestimmten klinischen Studie eine bestimmte Blutgruppe aufweisen. Dasselbe gilt hinsichtlich der Telefonverbindungsdaten zweier Kommunikationspartner.

17 **3. Identifiziertheit und Identifizierbarkeit der Person.** Die Informationen müssen sich auf eine identifizierte oder identifizierbare Person beziehen. Ob die betreffende Person identifiziert oder lediglich identifizierbar ist, spielt in rechtlicher Hinsicht keine Rolle, da hieran jeweils keine unterschiedlichen gesetzlichen Voraussetzungen geknüpft werden. Bei einer Interessenabwägung (zB im Rahmen von Art. 6 Abs. 1 S. 1 lit. f) kann dieser Umstand ggf. aber von Bedeutung sein.

---

[14] Hierzu etwa *Buchner* DuD 2015, 372 (373 f.); *Grünwald/Nüßing* MMR 2015, 378 (382); *Kinast/Kühnl* NJW 2014, 3057 (3058); *Lüdemann* ZD 2015, 247 (249 f.); *Weisser/Färber* MMR 2015, 506 (508); *Wilmer* K&R 2016, 382 (385).

[15] Die RL sprach insoweit zwar noch von Informationen „über" eine bestimmte oder bestimmbare natürliche Person. Die Formulierungen in der englischen Fassung der DSRL und der jetzigen DS-GVO sind indes identisch („any information relating to an identified or identifiable natural person").

[16] *Art.-29-Datenschutzgruppe,* Stellungn. 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2017, 10 ff.

[17] KSS DatenschutzR Rn. 216; für das BDSG aF *Dammann* in Simitis BDSG § 3 Rn. 14.

a) Identifizierte Person. Wann eine Person iSd Art. 4 Nr. 1 „identifiziert" ist, wird in der DS-GVO nicht näher erläutert. Von einer identifizierten Person ist auszugehen, wenn die Identität der Person **unmittelbar aus der Information selbst folgt**.[18] Dies ist beispielsweise der Fall, wenn die Information ein Identifikationsmerkmal (zB Name, Anschrift und Geburtsdatum) der Person beinhaltet oder wenn der Inhalt der Information oder der Kontext eine eindeutige Identifikation erlaubt, ohne dass auf weitere Informationen zurückgegriffen werden muss. **18**

b) Identifizierbare Person. Dagegen ist eine Person identifizierbar, wenn die Information zwar für sich genommen nicht ausreicht, um sie einer Person zuzuordnen, dies aber gelingt, sobald die Information **mit weiteren Informationen verknüpft** wird. So bestimmt Art. 4 Nr. 1, dass eine Person dann identifizierbar ist, wenn sie 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. **19**

aa) Maßgebliches Wissen und Mittel. Nach EG 26 sind bei der Frage, ob eine Person identifizierbar ist, **alle Mittel** zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach **allgemeinem Ermessen wahrscheinlich** genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Die englische Fassung dieser Formulierung („all the means reasonably likely to be used") fand sich in ähnlicher Form auch in der englischsprachigen Version der DSRL („all the means likely reasonably to be used").[19] Dort wurde sie in der deutschen Fassung allerdings schlicht mit „vernünftigerweise" wiedergegeben. Im Ergebnis lassen sich die insoweit zur DSRL vertretenen Auffassungen im Wesentlichen auf die DS-GVO übertragen. **20**

Bei der Frage, welche Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, sind nach EG 26 alle über die betreffende Person **bekannten oder ermittelbaren Informationen sowie alle objektiven Faktoren** heranzuziehen, wie zB die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand. Inwieweit auch das **Wissen und die Mittel Dritter** zu berücksichtigen sind, die diese zur Identifizierung einer Person verwenden können, ist umstritten (dazu unter → Rn. 25 ff.). **21**

Damit ist eine **Risikoanalyse** vorzunehmen, in deren Rahmen die Identifizierungswahrscheinlichkeit unter Verhältnismäßigkeitsgesichtspunkten zu evaluieren ist.[20] Nach Ansicht des EuGH sollen solche Mittel außer Betracht bleiben, mithilfe derer eine Identifizierung praktisch nicht durchführbar wäre, zB weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, sodass das Risiko einer Identifizierung „de facto vernachlässigbar" erschiene.[21] Insoweit muss im Grundsatz gelten, dass je größer die Persönlichkeitsrelevanz der Daten ist, desto geringere Anforderungen an die Wahrscheinlichkeit einer Zuordnung zu stellen sind. **22**

Bei der Beurteilung der Wahrscheinlichkeit ist ein **objektiver Maßstab** anzulegen: es kommt nicht auf die Motivation oder Intention an, sich das Mittel zu verschaffen oder es in einem konkreten Fall tatsächlich zu nutzen. Liegen solche subjektiven Faktoren vor, sind sie aber zu berücksichtigen. Im Übrigen ist ausreichend, dass die Nutzung des fraglichen Mittels unter rein abstrakt zu beurteilenden Gesichtspunkten wahrscheinlich ist. Dies folgt aus EG 26, wonach es insoweit auf „objektive Faktoren" ankommen soll. Die Nutzung **23**

---

[18] EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 38 – Breyer, mAnm *Kühling/Klar* ZD 2017, 24, zur insoweit vergleichbaren Formulierung („bestimmte natürliche Person") der DSRL.

[19] *Krügel* ZD 2017, 455 (459) sieht hierin eine Änderung des Bezugsobjekts und deshalb eine Änderung in der Bedeutung.

[20] Dazu *Nink/Pohle* MMR 2015, 563 (564 f.).

[21] EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 46 – Breyer, mAnm *Kühling/Klar* ZD 2017, 24.

allgemein auf dem Markt verfügbarer Mittel wird man hiernach nach allgemeinem Ermessen als wahrscheinlich ansehen können.

24 Maßgeblicher **Zeitpunkt** für die Bewertung ist stets der Zeitpunkt der Verarbeitung. So bestimmt EG 26, dass die zum Zeitpunkt der Verarbeitung jeweils verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Gleichwohl sind zumindest absehbare oder zu erwartende technologische Entwicklungen einzukalkulieren.[22] Da es auf eine Wahrscheinlichkeitsbetrachtung ankommt, liegt ein Personenbezug in zeitlicher Hinsicht nicht erst ab einer tatsächlich erfolgten Identifizierung vor, sondern bereits zu dem Zeitpunkt, ab dem die Nutzung entsprechender Mittel nach allgemeinem Ermessen wahrscheinlich ist.[23] Folglich stellt beispielsweise eine mit einer Telefonnummer verknüpfte Information (wie etwa der Zeitpunkt eines Anrufs) auch schon vor dem Zeitpunkt, zu dem der Verantwortliche die Telefonnummer – etwa mittels eines Telefonverzeichnisses mit Inverssuche – einer Person zuweist, ein personenbezogenes Datum dar. Dasselbe gilt mit Blick auf Videoüberwachungen, die zum Zwecke der späteren Identifikation von Personen vorgenommen werden. Auch hier liegt ein Personenbezug der Aufnahmen bereits bei deren Erstellung und nicht erst ab dem Zeitpunkt der tatsächlichen Identifizierung vor.[24]

25 **bb) Wissen und Mittel Dritter.** Inwieweit auch das Wissen und die Mittel Dritter zur Identifizierung von Personen zu berücksichtigen sind, ist **umstritten**. Die Problematik betrifft die Frage, ob es bei der Herstellbarkeit des Personenbezugs auf den jeweils Verantwortlichen ankommt (relativer Personenbezug) oder ob es ausreicht, dass irgendein Dritter einen Personenbezug herstellen kann (absoluter Personenbezug). Zwischen beiden Extrempositionen findet sich eine Reihe von Mischformen.[25] Die Art.-29-Datenschutzgruppe[26] und auch die deutschen Gerichte[27] hatten sich zur Frage des absoluten oder relativen Personenbezugs nicht eindeutig geäußert. Mehrere deutsche Datenschutzbehörden sprachen sich entgegen der hM in der datenschutzrechtlichen Literatur[28] für ein absolutes Verständnis aus.[29] Der EuGH hat im Zusammenhang mit dem Personenbezug von IP-Adressen erste richtungsweisende Ausführungen dazu gemacht, welche Anforderungen an die Berücksichtigung des Wissens und die Mittel Dritter zu stellen sind.[30]

26 Die Frage, ob ein relativer oder absoluter Personenbezug gilt, wird auch durch die **DS-GVO nicht eindeutig beantwortet**. Der DS-GVO lassen sich sowohl Elemente entnehmen, die für eine absolute Sichtweise sprechen, als auch solche, die ein relatives Verständnis nahelegen.[31] So sind nach EG 26 bei der Beurteilung der Frage der Identifizierbarkeit ausdrücklich auch alle solchen Mittel zu berücksichtigen, die „von einer anderen Person"

---

[22] *Piltz* K&R 2016, 557 (561).

[23] So ausdrücklich *GA Sánchez-Bordona* SchlA v. 12.5.2016 – C-582/14, ECLI:EU:C:2016:339 Rn. 77 – Breyer; in der nachfolgenden Entsch. spart der EuGH diese Thematik allerdings aus, vgl. EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 31 ff. – Breyer, mAnm *Kühling/Klar* ZD 2017, 24; ebenso wohl *Brink/Eckhardt* ZD 2015, 205 (211); kritisch zu einer solchen frühen Anknüpfung *Klar,* Datenschutzrecht und die Visualisierung des öffentlichen Raums, 156; vgl. in diesem Zusammenhang zur Figur des „potentiellen" Personenbezugs für das BDSG aF *Dammann* in Simitis BDSG § 3 Rn. 36.

[24] Zur Videoüberwachung näher unter → Rn. 37 und → Art. 6 Rn. 172.

[25] Dazu *Bergt* ZD 2015, 365 ff.

[26] *Art.-29-Datenschutzgruppe,* Stellungn. 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2007, 18 ff.; *Art.-29-Datenschutzgruppe,* Stellungn. 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148, 4.4.2008, 9.

[27] Zul. BGH Beschl. v. 28.10.2014 – VI ZR 135/13, MMR 2015, 131 ff.; vgl. im Übrigen die Nachweise bei *Bergt* ZD 2015, 365 (367 f.); *Kühling/Klar* NJW 2013, 3611 (3614).

[28] Vgl. für das BDSG aF nur *Dammann* in Simitis BDSG § 3 Rn. 22 ff.; *Gola/Schomerus* BDSG § 3 Rn. 10 mwN.

[29] So etwa für das BDSG aF *Schaar,* Datenschutz im Internet, Rn. 175; *Pahlen-Brandt* K&R 2008, 288; *Pahlen-Brandt* DuD 2008, 34; *Weichert* in DKWW BDSG § 3 Rn. 13; *Düsseldorfer Kreis,* Beschl. der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27.11.2009 in Stralsund, 1, in Bezug auf IP-Adressen.

[30] EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 31 ff. – Breyer, mAnm *Kühling/Klar* ZD 2017, 24; nachfolgend BGH Urt. v. 16.5.2017 – VI ZR 135/13, Rn. 25 ff.

[31] *Härting* ITRB 2016, 36 (36 f.); *Brink/Eckhardt* ZD 2015, 205 (209).

genutzt werden können, „um die Person direkt oder indirekt zu identifizieren".[32] Hier mag zunächst eine absolute Betrachtung anklingen. Nach demselben EG muss die Nutzung dieser Mittel durch den Dritten aber nach „allgemeinem Ermessen wahrscheinlich" sein. Die Nutzung entsprechender Mittel durch den Dritten kann aber nur dann wahrscheinlich sein, wenn nicht ausgeschlossen ist, dass der Dritte mit den fraglichen Daten in Berührung kommt, etwa indem sie ihm übermittelt werden.[33] Insoweit ist eine irgendwie geartete Beteiligung des Dritten am Identifizierungsvorgang erforderlich.[34] Damit kommt es bei der Beurteilung letztlich auf die jeweils Daten haltende Stelle an, was **eher für ein relatives Verständnis spricht**. Jedenfalls lässt sich aus EG 26 nicht ableiten, dass bei der Frage der Identifizierbarkeit das Wissen eines beliebigen Dritten bzw. das gesamte „Weltwissen" zugrunde zu legen wäre.[35] Das hat auch der EuGH im Zusammenhang mit dem Personenbezug von IP-Adressen eindeutig festgestellt.[36]

Im Einklang mit der DS-GVO sind das Wissen und die Mittel Dritter jedenfalls dann zu berücksichtigen, wenn Daten, die für den Verantwortlichen keinen Personenbezug aufweisen, an einen **Dritten weitergegeben werden**, der nach allgemeinem Ermessen wahrscheinlich in der Lage ist, einen Personenbezug herzustellen.[37] Dies folgt aus EG 26. Der Übermittlungstatbestand des Art. 4 Nr. 2 ist in diesem Fall erfüllt. Dasselbe gilt, wenn Informationen über eine Person im **Internet veröffentlicht** werden sollen. Auch hier ist danach zu fragen, ob ein Dritter (dh mindestens ein Internetnutzer) nach allgemeinem Ermessen wahrscheinlich in der Lage ist, einen Personenbezug herzustellen. Dies dürfte in den meisten Fällen der Fall sein. **27**

In allen anderen Fällen kommt es darauf an, ob Mittel existieren, die vom Verantwortlichen nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die bei ihm befindlichen Daten mit den Zusatzinformationen des Dritten so zu verknüpfen, dass ihm eine Identifikation der Person gelingt. Nach Ansicht des EuGH ist dies dann der Fall, wenn der Verantwortliche über **rechtliche Mittel** verfügt, um sich die Daten des Dritten verfügbar zu machen.[38] Dabei soll unerheblich sein, ob dies über den Umweg staatlicher Behörden erfolgt. Der EuGH scheint unmittelbar aus dem Vorhandensein eines rechtlichen Mittels darauf zu schließen, dass dessen Einsatz auch „vernünftigerweise" – bzw. in der Terminologie des EG 26 der DS-GVO: „nach allgemeinem Ermessen wahrscheinlich" – erfolgt. Dem ist jedenfalls dann zuzustimmen, wenn der Verarbeitungszweck (zB Speicherung von IP-Adressen zur Ahndung von Urheberrechtsverletzungen) in einem funktionalen Zusammenhang mit dem rechtlichen Mittel (zB urheberrechtlicher Auskunftsanspruch) steht. Denn nur dann liegt es nahe, dass der Verantwortliche von dem rechtlichen Mittel nach allgemeinem Ermessen wahrscheinlich Gebrauch macht. Denkbar sind aber auch Fälle, bei denen der Verantwortliche zwar über entsprechende rechtliche Mittel verfügt, ihr Gebrauch aber nur unter unverhältnismäßig hohem Aufwand einen Zugriff auf die Daten des Dritten ermöglicht. Dies kann zB der Fall sein, wenn der Dritte einer anderen Rechtsordnung unterliegt als der Verantwortliche. **28**

Auch ob die Möglichkeit der Verwendung **rechtswidriger Mittel** zu berücksichtigen ist, um an das Wissen und die Mittel Dritter zu gelangen, hängt nach der Formulierung des EG 26 davon ab, wie wahrscheinlich deren Verwendung angesichts des zu erlangenden Informationswerts ist. Nach Ansicht des EuGH sollen gesetzlich verbotene Möglichkeiten **29**

[32] Eine ähnliche Formulierung fand sich bereits in EG 26 der DSRL.

[33] Ähnlich für das BDSG aF *Dammann* in Simitis BDSG § 3 Rn. 19; *Klar,* Datenschutzrecht und die Visualisierung des öffentlichen Raums, 145.

[34] Zutreffend *Nink/Pohle* MMR 2015, 563 (564 f.).

[35] IErg ebenso *GA Sánchez-Bordona* SchlA v. 12.5.2016 – C-582/14, ECLI:EU:C:2016:339 Rn. 67 – Breyer.

[36] EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 31 ff. – Breyer, mAnm *Kühling/Klar* ZD 2017, 24.

[37] Zutreffend für das BDSG aF *Gola/Schomerus* BDSG § 3 Rn. 10 und 44a; kritisch dazu *Bergt* ZD 2015, 365 (369).

[38] EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 47 ff. – Breyer, mAnm *Kühling/Klar* ZD 2017, 24; ebenso BGH Urt. v. 16.5.2017 – VI ZR 135/13, Rn. 26.

allerdings außer Betracht bleiben, da sie regelmäßig nicht „vernünftigerweise" iSv EG 26 der bisherigen DSRL – bzw. übertragen auf EG 26 der DS-GVO: nicht „nach allgemeinem Ermessen wahrscheinlich" – zur Bestimmung der betreffenden Person eingesetzt werden.[39] Dem ist entgegenzusetzen, dass es auf rechtliche Mittel dann weniger ankommen sollte, wenn die faktische Nähe zu den beim Dritten befindlichen Daten (zB bei Auftragsverarbeitungsverhältnissen) oder die Sensibilität der Daten (zB bei klinischen Studien) groß ist und ein nicht rechtskonformer Zugriff auf die Daten nicht abwegig erscheint. Ob der EuGH tatsächlich so weit gehen und derartige Risikofälle vom Personenbezug ausnehmen wollte, ist fraglich.

30 Das Wissen und die Mittel **staatlicher Stellen** wird man ebenfalls nur dann berücksichtigen können, wenn sich der Verantwortliche dieser nach allgemeinem Ermessen wahrscheinlich zur Informationserlangung bedient oder Anhaltspunkte dafür vorliegen, dass staatliche Stellen von ihrer Befugnis zur Datenerhebung Gebrauch machen. Dies wird man beispielsweise in Fällen annehmen können, in denen der Verantwortliche bei der KFZ-Behörde Auskunft über den Halter eines Fahrzeugs begehrt, von dem ihm lediglich das KFZ-Kennzeichen bekannt ist. Nicht zu berücksichtigen ist dagegen das Wissen und die Mittel, die bei Geheimdiensten und ähnlichen Stellen vorhanden sind. Denn an diese kann sich der Verantwortliche regelmäßig nicht wenden, um Informationen über eine Person zu erlangen.

31 **4. Anonyme Daten.** Nach EG 26 gelten die Grundsätze des Datenschutzrechts **nicht für anonyme Informationen**, dh für Informationen, die sich (von vornherein) nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die (nachträglich) in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Durch die Formulierung macht der Verordnungsgeber deutlich, dass das anonyme Datum die Kehrseite des personenbezogenen Datums darstellt und ein Datum entweder personenbezogen oder anonym ist.[40]

32 Ob eine natürliche Person nicht mehr identifizierbar und das Datum damit anonym ist, ist nach Maßgabe von EG 26 zu prüfen, dh es sind **alle Mittel zu berücksichtigen**, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, wobei insbesondere die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand zu berücksichtigen sind (hierzu näher → Rn. 20 ff.).

33 Die Verordnung macht **keine technischen Vorgaben** dazu, welche Anforderungen an eine Anonymisierung zu stellen sind. EG 26 bestimmt jedoch, dass im Rahmen der Feststellung der Identifizierbarkeit einer Person die zum Zeitpunkt der Verarbeitung jeweils verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Daraus folgt, dass eingesetzte Anonymisierungsverfahren zumindest dem aktuellen Stand der Technik entsprechen müssen.

34 Als **Verfahren der Anonymisierung** kommen in der Praxis eine Löschung von identifizierenden Merkmalen (zB Name, Anschrift, Kontodaten), eine Aggregation von Daten, die Bildung von Gruppen und/oder die kontrollierte Einbringung von Zufallsfehlern in Betracht.[41]

35 **5. Einzelfälle.** Bei dynamischen **IP-Adressen** verfügt prinzipiell nur der Internetzugangsanbieter des Nutzers über entsprechende Log-Dateien und Zuordnungsdateien, die erkennen lassen, welchem Nutzer er zu welcher Zeit welche IP-Adresse zugeordnet hat. Wie der EuGH in einer früheren Entscheidung festgestellt hat, ist die IP-Adresse daher für den Internetzugangsanbieter ein personenbezogenes Datum.[42] Nach einer jüngeren Ent-

[39] EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 46 – Breyer, mAnm *Kühling/Klar* ZD 2017, 24.
[40] Ebenso *Karg* DuD 2015, 520 (523).
[41] Ausf. für die DSRL und das BDSG aF *Art.-29-Datenschutzgruppe,* Stellungn. 5/2014 zu Anonymisierungstechniken, WP 216, 10.4.2014; *Schefzig* K&R 2014, 772 (776); s. auch *Dammann* in Simitis BDSG § 3 Rn. 209.
[42] EuGH Urt. v. 24.11.2011 – C-70/10, ECLI:EU:C:2011:771 Rn. 51 – Scarlet Extended.