Die „neuen" personenbezogenen Daten in der DSGVO – Kontinuität und Änderungen

Corinna Bernauer, Regensburg*

Der Begriff der „personenbezogenen Daten" entscheidet darüber, ob das Datenschutzrecht überhaupt Anwendung findet. Trotz dieser wichtigen Aufgabe ist immer noch sehr unklar, was „personenbezogene Daten" überhaupt sind und ob sich durch die DSGVO etwas daran ändert. Klar ist, dass Literatur und Rechtsprechung zur alten Rechtslage weitgehend anwendbar bleiben. Eine wichtige Änderung ergibt sich jedoch: Die EuGH-Rechtsprechung zu Breyer/Deutschland, nach der illegale Methoden zur Identifizierbarkeit außer Acht bleiben, ist mit Erwägungsgrund 26 der DSGVO nicht mehr haltbar.

I. Das „personenbezogene Datum" als Eingangstor ins Datenschutzrecht

Daten sind überall. Jedes Tier, jeder Mensch und jede Maschine bringt eine schier unübersichtliche Flut von Daten mit sich. Es wäre ziemlich aussichtslos, generell alle Daten als gleich schutzwürdig zu betrachten. Daten an sich sind weder gefährlich noch schützenswert. Insofern will das Datenschutzrecht nur die Daten schützen, die für Menschen gefährlich werden können: Dass beispielsweise Passwörter oder die eigene Telefonliste sensibler sind als Wetterdaten, wird niemand bezweifeln. Entscheidend für die rechtliche Schutzwürdigkeit ist daher die Frage, ob es sich um ein personenbezogenes Datum handelt oder nicht: Nur personenbezogene Daten sind schützenswert genug, um überhaupt vom Datenschutzrecht erfasst zu werden. Zu entscheiden, ob ein Datum Personenbezug hat, steht deswegen als „Eingangstor" in das Datenschutzrecht am Anfang jeder Auseinandersetzung mit der Anwendbarkeit der Datenschutzgrundverordnung (VO (EU) 2016/679 – im Folgenden: DSGVO) sowie weiterer Datenschutznormen in anderen Gesetzen. Was ein Personenbezug genau voraussetzt, ist jedoch trotz Legaldefinitionen in Art. 2 lit. a) der alten Datenschutzrichtlinie (RL 95/46/EG – im Folgenden: DS-RL), § 3 Abs. 1 des Bundesdatenschutzgesetzes (im Folgenden: BDSG-alt) und Art. 4 Nr. 1 DSGVO heftig umstritten.

II. „Personenbezogenen Daten" in der DSGVO – Kontinuität und Änderung

Zur DSGVO, die gem. Art. 94 Abs. 1, 99 Abs. 2 DSGVO am 25. Mai 2018 die DS-RL ersetzen wird, gibt es zwar schon umfangreiche Literatur, jedoch naturgemäß noch keine Rechtsprechung. Die bisherige juristische Auseinandersetzung mit dem Begriff der „personenbezogenen Daten" basiert daher primär auf der DS-RL und deren Umsetzung in deutsches Recht, dem BDSG-alt. Dabei wurden zwar die Normtexte weitgehend übernommen, jedoch gab es eine wichtige Änderung in den für die Interpretation relevanten Erwägungsgründen. Dieser Artikel legt dar, warum deswegen wesentliche Einschränkungen des EuGH-Urteils Breyer/Deutschland nicht auf die neue Rechtslage unter der DSGVO übertragbar sind.

1. Kontinuität im Normtext

Außer Frage steht, dass die DSGVO keine radikale Änderung des Verständnisses von „personenbezogenen Daten" mit sich bringen wird. Dafür ist schon der Wortlaut der Normtexte zu ähnlich. In Nuancen weichen diese allerdings voneinander ab. Dort, wo Abweichungen vorhanden sind, sind diese inhaltlich so geringfügig, dass die Unterschiede übersetzungsbedingt erklärt werden können.

In Art. 2 lit. a DS-RL waren „personenbezogene Daten" definiert als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"). Etwas anders formuliert war die Definition in § 3 Abs. 1 BDSG-alt, die „personenbezogene Daten" als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)" definierte.

Bereits hier fallen Gemeinsamkeiten und Unterschiede auf: Das Paar „bestimmt/bestimmbar" findet sich in beiden Normtexten. Die Formulierung „Informationen" der Datenschutzrichtlinie wurde aber im BDSG-alt durch „Einzelangaben" ersetzt. Ein Unterschied erschließt sich daraus allerdings schon linguistisch nicht und konnte sich aus der Pflicht zur richtlinienkonformen Auslegung auch nicht ergeben.[1] Zu Recht wurde daher ein Bedeutungsunterschied zwischen den beiden Formulierungen mehrheitlich abgelehnt.[2] Dieser Wortlautunterschied beruht daher allein auf der Übersetzung des Normtexts.

Der neue Art. 4 Nr. 1 DSGVO definiert ebenfalls, was personenbezogene Daten sein sollen, nämlich „alle Informationen, die sich auf eine identifizierte oder identifizierbare na-

* Die Autorin studiert Rechtswissenschaft mit Schwerpunkt Recht der Informationsgesellschaft an der Universität Regensburg.

1 *Schild*, in: Wolff/Brink, BeckOK Datenschutzrecht, 22. Edition, Stand: 01.11.2017, BDSG § 3 Rn. 1.

2 *Dammann*, in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 5; Gola/Klug/Körffer, in: *Gola/Schomerus*, Bundesdatenschutzgesetz, 12. Auflage 2015, § 3 Rn. 3.

türliche Person (…) beziehen." Änderungen im Wortlaut im Vergleich zur DS-RL finden sich nur darin, dass „bestimmt/bestimmbar" durch „identifiziert/identifizierbar" ersetzt wurde. Dies wird – insbesondere mit Blick auf die Nähe zu anderen Sprachfassungen – zutreffend ebenfalls als inhaltsgleich interpretiert.[3] Trotz des unterschiedlichen Wortlauts sind also die wesentlichen Inhalte der Definition der „personenbezogenen Daten" gleich geblieben.

Ebenfalls völlig unproblematisch sind identifizierte Daten – „identifiziert" bedeutet dabei unstrittig, dass die Daten unmittelbar einer individualisierten natürlichen Person zugeordnet werden können.[4] Das war schon nach alter Rechtslage unproblematisch und wird sich mit der DSGVO nicht ändern.

2. Änderung in der Norminterpretation

Seit langem strittig ist dagegen das Kriterium der Identifizierbarkeit. Auch dazu gibt es zwar eine Legaldefinition, nämlich wird gem. Art. 4 Nr. 1 Halbs. 2 DSGVO „als identifizierbar (…) eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind." Kurz gesagt, ist eine Person identifizierbar, wenn ihr die zugehörigen Daten aufgrund von zusätzlicher Information zugeordnet werden können. So ist eine IP-Adresse für den Telekommunikationsanbieter identifizierbar, weil er selbst weiß, welche IP-Adresse welchem Nutzer zugeordnet ist.

Strittig ist aufgrund des passiven Satzbaus jedoch nach wie vor, ob und inwieweit dabei auch das Wissen Dritter zu berücksichtigen ist. Die bisherigen Meinungen zur alten Rechtslage werden in zwei größere Theorien zusammengefasst: Die Theorie des relativen Personenbezugs, und die des absoluten bzw. objektiven Personenbezugs.

a) Theorie des relativen Personenbezugs

Eine zur alten Rechtslage in Deutschland vielfach vertretene Ansicht ging davon aus, dass ein Datum nur dann für eine Stelle identifizierbar ist, wenn diese selbst über das zur Identifizierung erforderliche Zusatzwissen verfügt.[5] Eine dynamische IP-Adresse wäre damit für die meisten Stellen, die nicht über die Zuordnung des Anschlussnutzers zur IP-Adresse verfügen, nicht personenbezogen, da sie keine Möglichkeit haben, den Nutzer ohne zusätzliches Wissen von dritter Stelle zu identifizieren. Für den Internetzugangsanbieter dagegen, der zu Abrechnungszwecken über die Zuordnung auch dynamischer IP-Adressen zum Klarnamen des Nutzers verfügen muss, wäre die Adresse personenbezogen. Somit kann dasselbe Datum für eine Stelle personenbezogen sein und für eine andere nicht.[6] Personenbezug wird somit nicht als einem Datum eigen, sondern in Abhängigkeit des Wissens des Verarbeiters bestimmt.

Problematisch ist dabei zunächst die daraus resultierende Rechtsunsicherheit für die Betroffenen, denn ob Wissen bei einer bestimmten Stelle vorhanden ist, ist ungleich schwerer zu bestimmen, als ob Wissen generell vorhanden ist. Deutlich wird das in Fällen, bei denen die Kenntnisnahme auf informellen oder sogar illegalem Wege vorhanden ist – in diesen Fällen wäre das Datenschutzrecht überhaupt nicht anwendbar, weil schon der Personenbezug fehlt, obwohl gerade durch die illegale Kenntnisnahme genau der Fall eingetreten ist, vor dem das Datenschutzrecht schützen soll.

Der Wortlaut der Norm ist, wie oben dargelegt, mehrdeutig.[7] Allerdings ist eine tatsächliche Kenntnisnahme auf informellem oder illegalem Weg immer möglich, und der Wortlaut keiner der Normen schränkt die bloße Möglichkeit der Kenntnisnahme noch weiter ein.[8] Auch systematisch sprach bereits nach alter Rechtslage die explizite Formulierung „oder einem Dritten" in Erwägungsgrund 26 DS-RL,[9] sowie der Sinn und Zweck des Datenschutzes als Missbrauchsvorbeugung dagegen.[10] Auch wird eine Zusammenführung durch Vernetzung verschiedener Stellen immer realistischer.[11] Zu guter Letzt ist zu sagen, dass ja erst der Personenbezug überhaupt den Schutzbereich des Datenschutzrechts eröffnet, was ebenfalls für eine weite Auslegung des Begriffs spricht. Innerhalb des Datenschutzrechts sind feine Abstufungen verschiedener Schutzgrade möglich – lässt man Daten jedoch schon aus dessen Schutzbereich völlig herausfallen, so fehlt diese Interessenabwägung.

b) Theorie des absoluten Personenbezugs

Die andere Ansicht sieht ein Datum als objektiv bzw. absolut personenbezogen an, sobald irgendeine Stelle über das zur Identifizierung erforderliche Zusatzwissen verfügt.[12] Die oben als Beispiel genannten dynamischen IP-Adressen sind daher personenbezogen, weil sie der Telekommunikationsanbieter dem Klarnamen des Nutzers zuordnen kann. Dementsprechend sind deutlich mehr Daten vom Personenbezug betroffen als nach der relativen Theorie.

Kritiker lehnen den absoluten Personenbezug mit Verweis auf den ihrer Ansicht nach unklaren Wortlaut daher aus systematischen und teleologischen Gründen ab: Schon dass das Datenschutzrecht selbst nur auf personenbezogene Daten anwendbar sei, spräche dafür, nicht alle Daten zu erfassen. Nach der relativen Theorie wäre praktisch jedes Datum ein personenbezogenes und somit der Datenschutz so allumfas-

---

3 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), DSGVO, 2017, Art. 4 Rn. 2; ebenso *Ernst*, in: Paal/Pauly (Hrsg.), DSGVO, 2017, Art. 4 Rn. 3; a.A. *Klabunde*, in: Ehmann/Selmayr (Hrsg.), DSGVO, 2017, Art. 4 Rn. 12.

4 Für viele: *Klar/Kühling*, (Fn. 3), Art. 4 Nr. 1 Rn. 18.

5 *Gola/Klug/Körffer*, (Fn. 2), § 3 Rn. 10; differenzierter *Dammann*, (Fn. 2), § 3 Rn. 5.

6 *Brink/Eckhardt*, ZD 2015, 205 (206).

7 *Brink/Eckhardt*, (Fn. 7), S. 207; a.A. *Breyer*, ZD 2017, 400 (403).

8 *Breyer*, (Fn. 8), S. 402.

9 *Herbst*, NVwZ 2016, 902 (904).

10 *Breyer*, (Fn. 8), S. 403.

11 *Breyer*, (Fn. 8), S. 402.

12 *Schild*, (Fn. 1), § 3 Rn. 17.

send, dass dieser letztlich geschwächt würde. Auch sei dies für den Auftragsdatenverarbeiter mit größerer Rechtssicherheit verbunden, die relevanter sei als die Interessenabwägung der Datenschutzgesetze.[13]

c) Die EuGH-Entscheidung Breyer/Deutschland

In der Rechtssache Breyer/Deutschland[14] hat der EuGH entschieden, dass dynamische IP-Adressen nach bisheriger Rechtslage als personenbezogene Daten zu klassifizieren sind.[15] Bezugnehmend auf den Wortlaut der Norm, in der der Begriff „indirekt" verwendet wird, und Erwägungsgrund 26 der DS-RL geht der EuGH davon aus, dass es für den Personenbezug von Daten nicht erforderlich ist, dass die Informationen, die zur Identifizierung eines Nutzers benötigt werden, sich bei der verarbeitenden Stelle befinden.[16]
Das ist eine klare Absage an die reine relative Theorie: Der Gedanke, dass Informationen allein deswegen schon nicht personenbezogen – und somit nicht durch das Datenschutzrecht geschützt – sind, weil die verarbeitende Stelle selbst nicht über die Informationen verfügt, wird vom EuGH zu Recht abgelehnt.
Der EuGH schränkt diese begrüßenswerte Klarstellung entsprechend Erwägungsgrund 26 DS-RL allerdings wieder ein. Erwägungsgrund 26 DS-RL stellt darauf ab, welche Mittel „vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten." Im Urteil benennt der EuGH zwei Ausnahmen für den Personenbezug: wenn die Zusammenführung der Daten nicht legal oder wenn sie „praktisch nicht durchführbar wäre, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene".[17] Diese Kriterien entstammen den Schlussanträgen des Generalanwalts und wurden im vorliegenden Fall sehr knapp abgehandelt, wohl weil eindeutig eine rechtliche Möglichkeit zur Kombination von IP-Adressen und Namen durch Rechtsverfolgung bestand.[18] Als „rechtliches Mittel" zur Herstellung des Personenbezugs einer IP-Adresse lässt der EuGH genügen, dass ein Internetanbieter durch Strafanzeige eine Identifizierung und Verfolgung des Inhabers durch die Strafverfolgungsbehörden erreichen kann. Nicht gefordert wird, dass ein Anspruch der verarbeitenden Stelle auf Einsatz des rechtlichen Mittels besteht.[19] Allgemeine Kriterien, wann ein Mittel „vernünftig" ist, lassen sich daraus jedenfalls nicht ableiten.[20]

d) Änderung in Erwägungsgrund 26 DSGVO

Im Gegensatz zu den bis auf redaktionelle Änderungen nahezu identischen Normtexten (s.o.) gibt es in den Erwägungsgründen, die bei der Interpretation der Verordnung zu berücksichtigen sind, durchaus eine wesentliche Änderung: In Erwägungsgrund 26 der DSGVO wird nun auf diejenigen Mittel abgezielt, die von dem Verantwortlichen oder einer anderen Person zur Identifizierung „nach allgemeinem Ermessen wahrscheinlich" (reasonably likely, raisonnablement susceptible) eingesetzt werden, nicht mehr auf das Merkmal „vernünftig" (likely reasonably, susceptibles d'être raisonnablement mis en oeuvre) wie in Erwägungsgrund 26 DS-RL. Somit erscheint es sehr zweifelhaft, ob das vom EuGH formulierte Kriterium des rechtlich erlaubten Mittels zur Identifizierung Bestand haben kann.[21]

aa) Wortlaut

Wenn in einem für die Normauslegung relevanten Dokument Änderungen auftreten, ist davon auszugehen, dass auch Änderungen beabsichtigt sind, außer sie sind ganz klar nur durch Übersetzungen bedingt. Das ist hier aber nicht der Fall, der Wortlaut ist zwar spiegelbildlich, aber gerade in der englischen Fassung wird deutlich, dass sich der Schwerpunkt verschoben hat: Entscheidend für die Eigenschaften ist das Adjektiv („likely" bzw. früher „reasonably"), das Adverb soll nur wiederum das Adjektiv näher beschreiben.[22] Insofern spielt die Spiegelbildlichkeit von Adjektiv und Adverb von „likely reasonably" und „reasonably likely" in Erwägungsgrund 26 DSGVO in den beiden Wörtern keine Rolle, auch wenn manche darin gar keine Änderung sehen wollen:[23] In der ersten Fassung lag der Fokus auf dem Kriterium der „Vernunft", in der DSGVO auf der „Wahrscheinlichkeit". In den deutschen und französischen Fassungen wird dies durch die unterschiedlichen Formulierungen sogar noch deutlicher: Im Deutschen werden ganz unterschiedliche Adjektive benutzt, im Französischen jedenfalls die direkte Spiegelbildlichkeit der englischen Fassung aufgehoben.
Bezogen auf die Rechtsprechung des EuGH in Breyer/Deutschland, die illegale, aber tatsächliche Möglichkeiten der Identifizierung als unvernünftig i.S.d. Erwägungsgrunds 26 DS-RL außer Betracht für die Identifizierbarkeit lassen würde, ist dies eine Verschärfung.[24] Illegale Methoden mögen nicht vernünftig sein, generell unwahrscheinlich sind sie jedenfalls nicht.[25]

---

13 *Brink/Eckhardt*, (Fn. 7), S. 2017 m.w.N.

14 *EuGH*, 19.10.2016, C-582/14 – Breyer/Deutschland = ZD 2017, 24 m. Anm. *Klar/Kühling* = NJW 2016, 3579 m. Anm. *Mantz/Spittka* = NVwZ 2017, 213 m. Anm. *Ziegenhorn* = MMR 2016, 842 m. Anm. *Flemming/Rothkegel* = EuZW 2016, 909 m. Anm. *Richter*.

15 *Klar/Kühling*, (Fn. 15), S. 28; a.A. *Hansen/Struwe*, GRUR-Prax. 2016, 503 (503).

16 *EuGH*, 19.10.2016, C-582/14 – Breyer/Deutschland, Rn. 41 ff.

17 *EuGH*, 19.10.2016, C-582/14 – Breyer/Deutschland, Rn. 46.

18 *Richter*, (Fn. 15). S. 913.

19 *Klar/Kühling*, (Fn. 15), S. 28; *Flemming/Rothkegel*, (Fn. 15), S. 846.

20 *Ziegenhorn*, (Fn. 15), S. 217.

21 *Ziegenhorn*, (Fn. 15), S. 217; a.A. *Herbst*, (Fn. 10), S. 903; *Flemming/Rothkegel*, (Fn. 15), S. 846; *Mantz/Spittka*, (Fn. 15), S. 3583.

22 *Alexander*, Longman English Grammar, S. 106, 122.

23 *Klar/Kühling*, (Fn. 3), Art. 4 Rn. 20;*Gola*, DSGVO, 2017, Art. 4 Rn. 15.

24 So auch *Krügel*, ZD 2017, 455 (460); a.A. *Klar/Kühling*, (Fn. 3), Art. 4 Nr. 1 Rn. 20.

25 *Krügel*, (Fn. 25), S. 459 m.w.N.

bb) Systematik

Eine derartige Änderung passt auch systematisch zu DS-GVO, da diese im Vergleich zur DS-RL den Datenschutz insgesamt eher stärken soll.[26] Beispielhaft seien nur die Bußgeldvorschriften der Art. 83 Abs. 4 DSGVO genannt, die Verstöße deutlich drastischer ahnden als es bisher der Fall war.[27] Das primäre Ziel des Verordnungsgebers mag zwar die Vereinheitlichung des Datenschutzes gewesen sein, aber durch die immer engere grenzüberschreitende Datenverarbeitung kommt diese Vereinheitlichung einem erhöhten Schutz gleich, auch wenn dieser in einzelnen Staaten auch eine Absenkung des Datenschutzniveaus mit sich bringt. Diese Tendenz entspricht auch der datenschutzfreundlichen Rechtsprechung des EuGH in Sachen Vorratsdatenspeicherung,[28] Safe Harbor und nicht zuletzt eben auch IP-Adressen.

cc) Telos

Auch teleologisch ist eine Verschärfung der Rechtslage durch das Kriterium der „Wahrscheinlichkeit" angemessen: In der Praxis kommen Datenschutzverstöße vielfach vor, gerade wenn sie profitabel sind. Die Wahrscheinlichkeit für Hackerangriffe ist in den letzten Jahren stets gestiegen und wird weiter steigen. Die Zahl der Pannen und Missbrauchsfälle wächst täglich. Insofern erscheint es realitätsfern, nur auf den Einsatz legaler Mittel abzustellen. Das Bundesverfassungsgericht hat zu Recht ausgesprochen, die Grundrechte schützten auch vor Missbräuchen, die von dem Betroffenen „nicht ohne Grund befürchtet" werden.[29] Dieser Maßstab muss auch für die unzulässige Heranziehung von Zusatzwissen gelten. Wie Herbst zutreffend ausführt, kommt es für die Wahrscheinlichkeit der Nutzung von Mitteln nicht nur auf deren Legalität an, sondern auf das „Verhältnis zwischen den zu erzielenden Vorteilen und den bei Entdeckung bzw. Bestrafung zu erwartenden Nachteilen" an, sodass es nicht unrealistisch schiene, dass diese Abwägung entscheidender ist als Rechtstreue.[30] Dem ist noch hinzuzufügen, dass die Wahrscheinlichkeit entdeckt und bestraft zu werden, nicht besonders hoch ist.[31] Datenschutz dient gerade dem präventiven Schutz vor Datenmissbrauch. Diese Schutzfunktion wird ihm genommen, wenn möglicher Datenmissbrauch von vornherein als zu vernachlässigend abgetan wird.

dd) Gegenansicht

Doch selbst wenn man mit der Gegenansicht annähme,[32] dass mit der Änderung in den Erwägungsgründen keine Verschärfung beabsichtigt sei und damit der Rechtsprechung des EuGH zur unbeachtlichkeit illegaler Identifizierungsmöglichkeiten folgen wollte, so sind bei den maßgebenden „rechtlichen Möglichkeiten" der legalen Zuordnung deutlich mehr Vorschriften zu berücksichtigen, als zunächst scheint: Neben den Auskunftsansprüchen bei Internetkriminalität nach §§ 202a, 303a, 303b StGB[33] und Urheberrechtsverletzungen, namentlich § 101 UrhG,[34] benennt nämlich Richter etwa §§ 1 Abs. 1 Satz 1 IFG, § 44 ff. BMG und § 19 GWB[35] und Mantz/Spittka zusätzlich § 17 UWG.[36] Das sind rechtliche Mittel, die ein Zusammenführen ermöglichen, bei denen es zwar nicht gerade auf den Auskunftsanspruch über eine einzelne Person ankommt, jedoch trotzdem eine hohe Wahrscheinlichkeit besteht, dass diese identifiziert wird. Insofern ist auch nach dieser Ansicht ein Datum schon dann personenbezogen, wenn eine der genannten Anspruchsgrundlagen oder hoheitliche Möglichkeiten zur Identifikation in Frage kommen. Dies ist bereits dann der Fall, wenn ihre Anwendung nicht von vornherein auszuschließen ist. Somit wäre auch nach dieser Auffassung von einem umfangreichen Anwendungsbereich der DSGVO auszugehen.

III. Fazit

Im Ergebnis lässt sich festhalten, dass bei der Frage, was ein personenbezogenes Datum ist, die Rechtsprechung und Literatur zu weiten Teilen auf die neue Rechtslage übertragbar ist. Dies ist wichtig, da hierbei schon zahlreiche Unklarheiten, die sich im Verlauf der Anwendung der Datenschutzrichtlinie und des BSDG-alt entwickelt hatten, insbesondere durch den EuGH geklärt wurden. Ebenso wichtig ist jedoch, dass die Änderung in Erwägungsgrund 26 DSGVO nicht übersehen wird, denn darin liegt eine wesentliche Änderung im Zurechnungsmaßstab des Wissens Dritter: Die Änderung des allzu sehr auf Legalität abzielenden „likely reasonably" (vernünftig) in ein auf die bloße Möglichkeit abzielenden „reasonably likely" (wahrscheinlich) darf hier nicht ignoriert werden, denn sie führt zu einer Ausweitung der Anwendbarkeit des Datenschutzrechts. Ob und wie stark die betroffenen Daten dann tatsächlich zu schützen sind, ist eine Frage der inhaltlichen Regelungen der DSGVO sowie des deutschen Anpassungs- und Umsetzungsgesetzes. Doch jedenfalls ist die Tür ins Datenschutzrecht in der DSGVO deutlich weiter geöffnet als sie es noch bei der DS-RL und dem BDSG-alt war.

---

26 *Voßhoff/Hermerschmidt*, PinG 2016, 56 (57).

27 *Holländer*, (Rn. 1), Art. 83 Rn. 1.

28 *Klar/Kühling*, (Fn. 15), S. 29.

29 BVerfGE 100, 313 (376); 107, 299 (320).

30 *Herbst*, (Fn. 10), S. 905.

31 *BKA*, Cybercrime Bundeslagebild 2016, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html?nn=28110, Abruf v. 19.12.2017.

32 *Klar/Kühling*, (Fn. 3), Art. 4 Nr. 1 Rn. 20.

33 *Mantz/Spittka*(Fn. 15), S. 3583.

34 *Flemming/Rothkegel*, (Fn. 15), S. 846.

35 *Richter*, (Fn. 15), S. 913.

36 *Mantz/Spittka*, (Fn. 15), S. 3583.