Datenschutz-Grundverordnung: DS-GVO

Bearbeitet von
Prof. Dr. Jürgen Kühling, Benedikt Buchner, Prof. Dr. Matthias Bäcker, Matthias Bergt, Prof. Dr. Franziska Boehm, Prof. Dr. Johannes Caspar, Dr. Alexander Dix, Dr. Jürgen Hartung, PD Dr. Tobias Herbst, Dr. Silke Jandt, Prof. Dr. Thorsten Kingreen, Dr. Manuel Klar, Prof. Dr. Frank Maschmann, Prof. Dr. Thomas Bernhard Petri, Johannes Raab, Dr. Christian Schröder, Prof. Dr. Marie-Theres Tinnefeld, Dr. Thilo Weichert

1. Auflage 2017. Buch. XVI, 1170 S. In Leinen

Format (B x L): 16,0 x 24,0 cm

Der Begriff und das Konzept der Offenlegung (einschließlich der Übermittlung) der DS-GVO (und schon nach der DSRL) **unterscheidet sich** insoweit von entsprechenden Begriffen und Konzepten des **BDSG**, als das BDSG nur den Begriff des „Übermittelns" kennt und ein „Übermitteln" außerdem nach § 3 Abs. 4 Nr. 3 BDSG nur dann vorliegt, wenn es **gegenüber Dritten** erfolgt.[10] Die Offenlegung iSd DS-GVO unterscheidet sich auch insoweit von der Übermittlung im Sinne des BDSG, als eine Offenlegung schon dann vorliegt, wenn Daten **bloß zum Abruf bereitgehalten** werden; nach § 3 Abs. 4 Nr. 3 lit. b BDSG liegt eine Übermittlung in diesem Fall erst dann vor, wenn ein Dritter die Daten tatsächlich abruft.

Der Begriff „**Übermittlung**" (transmission) im Sinne der DS-GVO ist ein Unterfall der Offenlegung. Er unterscheidet sich dadurch vom Übermittlungsbegriff des § 3 Abs. 4 Nr. 3 BDSG, dass er, wie gerade zur Offenlegung dargelegt, **nicht auf die Weitergabe an „Dritte" beschränkt** ist. Eine Parallele zum Übermittlungsbegriff des § 3 Abs. 4 Nr. 3 BDSG ist allerdings darin zu sehen, dass das **Bereithalten zum Abruf für sich genommen noch keine Übermittlung** darstellt; eine Übermittlung iSv Art. 4 Nr. 2 liegt vielmehr erst dann vor, wenn ein anderer (nicht notwendig ein Dritter) die Daten tatsächlich abruft. Dieses Verständnis des Übermittlungsbegriffs wird (im Kontext der DSRL) deutlich im **Lindqvist-Urteil** des EuGH;[11] der EuGH führt hier aus, dass das Hochladen von Daten einer Internetseite auf einen Server deswegen keine „Übermittlung in ein Drittland" darstellt, weil ein Internetnutzer erst noch „eigenhändig" Schritte unternehmen (nämlich die betreffende Seite aufrufen) muss, um den Inhalt der Internetseite einsehen zu können. Der EuGH versteht das Übermitteln hier als einen Vorgang, durch den Informationen an Personen gesendet werden, die zum Empfang nicht bestimmte Seiten bewusst aufsuchen müssen. **31**

„**Verbreitung**" (dissemination) ist ein Begriff, der in Bezug auf Informationen häufig iSv „Veröffentlichen" verwendet wird, auch etwa durch Ausstrahlung von Rundfunk- oder Fernsehprogrammen, die von jedermann empfangen werden können, oder durch Abdruck in einer Zeitung. Gemeint ist hier insbes. die Weitergabe von Daten an eine **unbestimmte Vielzahl von Empfängern**. **32**

Der Ausdruck „**andere Form der Bereitstellung**" (otherwise making available) verdeutlicht den Charakter der Offenlegung als „**Zugänglichmachen**". **33**

8. Der Abgleich oder die Verknüpfung. Beim **Abgleich** (alignment) personenbezogener Daten werden diese verglichen mit bestimmten Vorgaben; bei der **Verknüpfung** (combination) werden personenbezogene Daten zusammengeführt (zB Daten zum Kaufverhalten bestimmter Personen mit Daten zu ihrem Einkommen). **34**

9. Die Einschränkung. Die **Einschränkung** (restriction) der Verarbeitung entspricht dem in der DSRL und im BDSG verwendeten Begriff der **Sperrung** von Daten. Der Begriff ist in Art. 4 Nr. 3 näher definiert (→ Art. 4 Nr. 3 Rn. 6 ff.). **35**

10. Das Löschen oder die Vernichtung. Der Begriff „**Löschen**" (erasure) wird in § 3 Abs. 4 Nr. 5 BDSG definiert als „Unkenntlichmachen gespeicherter personenbezogener Daten"; der Sache nach handelt es sich im BDSG um denselben Begriff wie in der DS-GVO. Das Löschen kann auf unterschiedliche Weise erfolgen, etwa durch Überschreiben von Daten auf einem Datenträger durch andere Daten; maßgeblich ist das Ergebnis der Löschungshandlung, nämlich die (faktische) **Unmöglichkeit, die zuvor in den zu löschenden Daten verkörperte Information wahrzunehmen**.[12] Nach dem Löschen **36**

[10] Eine interne Bekanntgabe an einen Adressaten, der nicht „Dritter" ist, kann aber eine durch § 4 BDSG grundsätzlich verbotene Nutzung iSv § 3 Abs. 5 BDSG darstellen; dazu *Dammann* in Simitis BDSG § 3 Rn. 158.

[11] EuGH Urt. v. 6.11.2003 – C-101/01, Slg. 2003, I-12992 Rn. 56 ff. (insbes. Rn. 60).

[12] Ähnlich *Dammann* in Simitis BDSG § 3 Rn. 175, allerdings mit dem Unterschied, dass Dammann es offenbar genügen lässt, dass die Informationswahrnehmung lediglich für die verantwortliche Stelle unmöglich gemacht wird.

darf es niemandem mehr ohne unverhältnismäßigen Aufwand möglich sein, die betreffende Information wahrzunehmen.[13] Zu den Anforderungen an das Löschen im Zusammenhang mit der Löschungspflicht aus Art. 17 vgl. näher → Art. 17 Rn. 37 ff.

37 „**Vernichtung**" (destruction) meint die **physische Zerstörung** des Datenträgers; sie stellt zugleich eine Form des Löschens dar.

C. DS-GVO und nationales Recht

38 Wie dargelegt (→ Rn. 3), weicht die Definition des „Verarbeitens" in § 3 Abs. 4 BDSG vor allem insofern von der Verarbeitungsdefinition in Art. 4 Nr. 2 DS-GVO ab, als das BDSG das Erheben und das Nutzen (§ 3 Abs. 3 und 5 BDSG) vom Verarbeitungsbegriff ausnimmt. Jedenfalls in den Bereichen, in denen dem nationalen Gesetzgeber keine Regelungsmöglichkeiten durch Öffnungsklauseln der DS-GVO eröffnet sind, hat die **Definition in Art. 4 Nr. 2 DS-GVO Vorrang gegenüber einer nationalen Regelung**, so dass § 3 Abs. 4 BDSG zu streichen sein wird; Gleiches gilt für § 3 Abs. 5 BDSG, weil hier das Nutzen ausdrücklich als nicht zur Verarbeitung gehörig definiert wird. § 3 Abs. 3 BDSG könnte als konkretisierende Definition des Erhebens für die Bereiche erhalten bleiben, in denen die Mitgliedstaaten Konkretisierungsbefugnisse haben (so etwa aufgrund von Art. 6 Abs. 2), wobei dann das Erheben als ein Teil der Verarbeitung anzusehen wäre.

39 Soweit Normen des deutschen Rechts bestehen bleiben können, in denen der **Begriff „Verarbeitung"** verwendet wird, kann im Fall der Aufrechterhaltung einer solchen Norm dieser Begriff ersetzt werden durch eine Aufzählung der sich aus § 3 Abs. 4 BDSG ergebenden **fünf Teilaspekte** des Speicherns, Veränderns, Übermittelns, Sperrens und Löschens.[14]

Nr. 3 Einschränkung der Verarbeitung

„Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

A. Allgemeines

I. Überblick

1 Art. 4 Nr. 3 definiert den in Art. 4 Nr. 2 schon als eine Verarbeitungsart erwähnten Begriff der „Einschränkung" bzw. der „Einschränkung der Verarbeitung". Die Definition ist in engem Zusammenhang mit den detaillierten Regelungen zu Voraussetzungen und Rechtsfolgen der Einschränkung der Verarbeitung in **Art. 18** zu sehen.

2 Die wesentliche Bedeutung des Begriffs besteht darin, dass die Verarbeitung personenbezogener Daten nach der Einschränkung **nur noch für bestimmte wichtige Zwecke** zulässig ist. Die Einschränkung kann **an die Stelle einer eigentlich vorgesehenen Löschung** treten, wenn ein bestimmtes Interesse am Erhalt der Daten besteht. Der Begriff „Einschränkung der Verarbeitung" entspricht dem vom BDSG und von der DSRL verwendeten Begriff der „**Sperrung**".

3 Die Einschränkung als Verarbeitungsvorgang besteht in der entsprechenden **Markierung** der betreffenden Daten; die damit bewirkte Reduzierung der Verarbeitungsmöglichkeiten für die markierten Daten ergibt sich als Rechtsfolge aus Art. 18 Abs. 2.

---

[13] Ähnlich *Eßer* in Auernhammer BDSG § 3 Rn. 62: Verhinderung des Zugriffs auf Dauer (unaufhebbar) und gegenüber jedermann.

[14] Vgl. *Kühling/Martini et al.,* 309 f.

II. Entstehungsgeschichte

1. Richtlinie. Dem in Art. 4 Nr. 3 DS-GVO legaldefinierten Begriff der „Einschränkung der Verarbeitung" entspricht der in der DSRL verwendete Begriff des „**Sperrens**" (zur Umbenennung → Rn. 5). Das „Sperren" wird in **Art. 2 lit. b DSRL** als eine Art der Verarbeitung personenbezogener Daten genannt, aber **nicht weiter definiert**. **4**

2. Entwürfe zur DS-GVO. Im **Kommissionsvorschlag** findet sich die „Einschränkung der Verarbeitung" weder als Beispiel für eine Verarbeitungsart in der Legaldefinition der Verarbeitung (Art. 4 Abs. 3 des Kommissionsvorschlags) noch in Gestalt eines in Art. 4 legaldefinierten Begriffs; auch der in der DSRL verwendete Begriff des „Sperrens" findet sich hier nicht. Der Kommissionsvorschlag enthält in Art. 17 Abs. 4 bis 6 Regelungen zur „Beschränkung der Verarbeitung", die inhaltlich dem Art. 18 der finalen Fassung entsprechen, in dem von der „Einschränkung der Verarbeitung" die Rede ist (→ Art. 18 Rn. 6 ff.); auch der Begriff der „Beschränkung" findet sich in Art. 4 des Kommissionsvorschlags allerdings nicht. Aus Punkt 3.4.3.3. der Begründung des Kommissionsvorschlags wird jedenfalls deutlich, dass es sich bei dem Wort „Beschränkung" um eine neue und nun nicht mehr mehrdeutige Bezeichnung der aus der DSRL bekannten „Sperrung" handeln soll. Der Parlamentsentwurf brachte in Bezug auf den Begriff der „Beschränkung" keine Änderung. Erst im **Ratsentwurf** wurde die Bezeichnung „Beschränkung" durch „Einschränkung" ersetzt (wodurch auch eine Verwechslung mit den „Beschränkungen" nach Art. 23 vermieden wird), und die Einschränkung erfuhr eine gewisse Aufwertung dadurch, dass sie eine eigene Legaldefinition (im Ratsentwurf zunächst in Art. 4 Abs. 3a) und eine Regelung in einem eigenen Artikel (im Ratsentwurf zunächst in Art. 17a) erhielt. Art. 4 Abs. 3a des Ratsentwurfs findet sich nun unverändert als Art. 4 Nr. 3 der finalen Fassung. **5**

B. Einschränkung der Verarbeitung

Die Legaldefinition der „Einschränkung der Verarbeitung" in Art. 4 Nr. 3 muss als **semantisch misslungen** bezeichnet werden, weil sie, indem sie diesen Begriff (wenn man es leicht umformuliert) als „Markierung mit dem Ziel der Einschränkung der Verarbeitung" definiert, diesen Begriff mit einem anderen Begriff erläutert, der dieselbe Bezeichnung trägt und selbst nicht erläutert wird. **Der Sinn des Ganzen ergibt sich erst aus Art. 18**, der die Voraussetzungen und die Rechtsfolgen einer Einschränkung der Verarbeitung regelt. Demnach handelt es sich bei der in Art. 4 Nr. 3 legaldefinierten Einschränkung der Verarbeitung um eine **Markierung** gespeicherter personenbezogener Daten; diese Markierung hat aufgrund der Regelung in Art. 18 Abs. 2 zur Folge, dass die markierten Daten – abgesehen von der Speicherung – in der Zukunft bzw. für einen bestimmten Zeitraum **nur noch für die in Art. 18 Abs. 2 genannten Zwecke** (→ Art. 18 Rn. 34 ff.) verarbeitet werden dürfen. **6**

Die Einschränkung der Verarbeitung findet dann Anwendung, wenn Daten – entsprechend dem Willen des Verantwortlichen oder auch wegen einer Verpflichtung des Verantwortlichen – **eigentlich gelöscht werden sollen**, aber bestimmte, in Art. 18 Abs. 1 genannte Gründe (näher dazu → Art. 18 Rn. 9 ff.) dafür sprechen, die Daten zunächst weiter aufzubewahren. Die Einschränkung der Verarbeitung bewirkt, dass die Daten weiterhin gespeichert bleiben müssen; sie dürfen dann aber grundsätzlich nicht mehr (über die Speicherung hinaus) verarbeitet werden. Eine Verarbeitung ist vielmehr nur möglich mit Einwilligung der betroffenen Person oder zu bestimmten wichtigen Zwecken, die in Art. 18 Abs. 2 abschließend aufgezählt werden. **7**

Zu den **technischen Möglichkeiten der Markierung** und den Anforderungen an sie vgl. → Art. 18 Rn. 30 f. **8**

C. DS-GVO und nationales Recht

9 **§ 3 Abs. 4 Nr. 4 BDSG** definiert den Begriff des „**Sperrens**" als „das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken". Der Sache nach entspricht dieser Begriff der „Einschränkung der Verarbeitung" nach Art. 4 Nr. 3 DS-GVO. Die zusätzliche Erwähnung der Nutzung erklärt sich daraus, dass nach der Begrifflichkeit des BDSG – anders als in der DS-GVO – die Nutzung nicht unter den Begriff der Verarbeitung fällt (→ Art. 4 Nr. 2 Rn. 3).

10 Grundsätzlich hat die Legaldefinition des Art. 4 Nr. 3 **Anwendungsvorrang** vor einer nationalen Regelung wie § 3 Abs. 4 Nr. 4 BDSG. Schon aus **Gründen der Begriffsklarheit** empfiehlt es sich, auf die Bezeichnung „**Sperrung**" im nationalen Recht (und damit auch auf die entsprechende Legaldefinition) **künftig zu verzichten** und stattdessen in den Bereichen, in denen dem nationalen Gesetzgeber eigene Regelungsmöglichkeiten durch Öffnungsklauseln der DS-GVO eröffnet sind, den in Art. 4 Nr. 3 definierten Begriff der „Einschränkung" zu verwenden.

Nr. 4 Profiling

„Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

Literatur *Britz,* Einzelfallgerechtigkeit versus Generalisierung, 2008; *Weichert,* Scoring in Zeiten von Big Data, ZRP 2014, 168.

I. Überblick

1 Art. 4 Nr. 4 definiert Profiling als automatisierte Datenverarbeitung zu Zwecken der Persönlichkeitsbewertung. Vom Profiling **zu unterscheiden** ist die sog **automatisierte Entscheidung** bzw. Entscheidungsfindung, auch wenn diese in der DS-GVO mehrmals im selben Atemzug mit dem Profiling genannt wird (s. vor allem die Überschrift bei Art. 22: „Automatisierte Entscheidungen im Einzelfall einschließlich Profiling"[1]). Ungenau ist diese Vermengung insoweit, als Profiling und Entscheidung (bzw. Entscheidungsfindung) auf zwei verschiedenen Ebenen anzusiedeln sind. Profiling – als automatisierte Datenverarbeitung – bildet die Grundlage, auf der eine Entscheidung des Verantwortlichen aufsetzt, die für die betroffene Person dann eine rechtliche Wirkung oder sonstige Konsequenz mit sich bringt. Profiling ist also ein Prozess der **Datenverarbeitung**, der sich nach den allgemeinen datenschutzrechtlichen Vorgaben richtet, die automatisierte Entscheidung beschränkt sich hingegen auf die Nutzung bestimmter Ergebnisse einer Datenverarbeitung (sa → Art. 22 Rn. 11).

2 Ob und wie personenbezogene Daten zu Zwecken des Profilings erhoben und genutzt werden dürfen, bestimmt sich nach den **allgemeinen Regeln der DS-GVO** zu Grundsätzen und Rechtmäßigkeit einer Datenverarbeitung (EG 72). Daneben sieht die DS-GVO für das Profiling eine Reihe von speziellen Regelungen vor, die teils allein das Profiling in seiner Ausprägung als automatisierte Datenverarbeitung betreffen, teils aber auch darüber hinausgehend automatisierte Entscheidungen, die auf solch einem Profiling beruhen. So sehen etwa Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g **Informationspflichten** des

[1] Ähnlich ist in den Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h von einer „automatisierten Entscheidungsfindung einschließlich Profiling" die Rede.

Verantwortlichen für den Fall einer „automatisierten Entscheidungsfindung einschließlich Profiling" vor. Korrespondierend dazu normiert Art. 15 Abs. 1 lit. h ein entsprechendes **Auskunftsrecht** der betroffenen Person. Gesondert erwähnt ist das Profiling[2] auch beim **Widerspruchsrecht** nach Art. 21 Abs. 1, das die betroffene Person aus Gründen, die sich aus ihrer besonderen Situation ergeben, ausüben kann. Noch weiter geht dieses Widerspruchsrecht der betroffenen Person für den Fall, dass das Profiling mit Direktwerbung in Verbindung steht (Art. 21 Abs. 2). Art. 22 Abs. 1 räumt der betroffenen Person das Recht ein, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden **Entscheidung** unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Und gem. Art. 35 Abs. 3 lit. a ist im Fall einer automatisierten Datenverarbeitung (einschließlich Profiling), die auf eine automatisierte Entscheidungsfindung abzielt, eine **Datenschutz-Folgenabschätzung** erforderlich.

II. Entstehungsgeschichte

Weder in der **DSRL** noch im **BDSG** taucht der Begriff „Profiling" auf. Art. 15 DSRL **3**
verwendet wie auch § 6a BDSG lediglich den allgemeineren Begriff der automatisierten Verarbeitung. Im BDSG erfährt darüber hinaus noch eine spezielle Ausprägung des Profilings, das Scoring, gesonderte Erwähnung – verstanden als mathematisch-statistisches Verfahren, um einen „Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen" (§ 28b BDSG) zu berechnen.[3]

Die Kommission verzichtete in ihrem Vorschlag zur **DS-GVO** noch auf eine eigen- **4**
ständige Definition des Profilings. Indirekt ergab sich das Verständnis von Profiling jedoch aus Art. 20 des Kommissionsvorschlags, welches im Wesentlichen der endgültigen Definition in Art. 4 Nr. 4 entspricht.[4] Eine eigenständige Definition des Profilings findet sich dann erstmals im Parlamentsentwurf, die als solche dann abgesehen von kleineren sprachlichen Änderungen auch in die endgültige Fassung der DS-GVO Eingang gefunden hat.

III. Profiling

Profiling setzt eine **automatisierte** Verarbeitung personenbezogener Daten voraus; die **5**
bloß manuelle Verknüpfung von Daten, um bestimmte Aspekte einer Person zu bewerten und zu analysieren, gehört nicht dazu, auch wenn die DS-GVO ansonsten nach Art. 2 Abs. 1 die nichtautomatisierte Datenverarbeitung ebenfalls erfasst, sofern die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Abgesehen von dieser Einschränkung einer automatisierten Datenverarbeitung knüpft **6**
Art. 4 Nr. 4 die weitere Definition des Profilings **allein an das mit der Datenverarbeitung verfolgte Ziel:** die Bewertung bestimmter persönlicher Aspekte einer natürlichen Person.[5] Unerheblich ist dagegen, wie genau im Einzelnen der konkrete Verarbeitungsvorgang bei einem Profiling ausgestaltet ist. Die Definition des Profiling ist damit offen für alle denkbaren technischen Varianten und Entwicklungen einer automatisierten Datenverarbeitung und es können ganz vielfältige Formen der Verarbeitung unter das Profiling fallen, solange der jeweilige Datenverarbeitungsprozess nur auf den von der Definition vorgegebenen Zweck einer Persönlichkeitsbewertung abzielt.

---

[2] Und zwar nur das Profiling in seiner Ausprägung als automatisierte Datenverarbeitung (nicht auch die automatisierte Entscheidung).

[3] Vgl. BT-Drs. 16/10529, 9.

[4] Art. 20 Abs. 1 des Kommissionsentwurfs: „Auswertung bestimmter Merkmale" einer Person oder „Analyse beziehungsweise Voraussage etwa ihrer beruflichen Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens".

[5] *Martini* in Paal/Pauly Art. 22 Rn. 21.

7 Zu den Persönlichkeitsaspekten, auf deren Bewertung ein Profiling abzielen kann, zählt Art. 4 Nr. 4 beispielhaft („insbesondere") die Arbeitsleistung einer natürlichen Person, deren wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort und Ortswechsel. Die Weite und Breite dieser – beispielhaft aufgezählten – Persönlichkeitsaspekte legen es nahe, dass die Definition von Profiling **umfassend** die Bewertung sämtlicher Aspekte einer Persönlichkeit erfassen soll. Eines der bekanntesten und praktisch bedeutsamsten Beispiele für ein Profiling ist das sog **Credit Scoring**, das darauf gerichtet ist, auf Grundlage mathematisch-statistischer Berechnungsverfahren die in Art. 4 Nr. 4 genannten Aspekte der wirtschaftlichen Lage und Zuverlässigkeit einer Person zu analysieren und vorherzusagen.

8 Ob die im Zuge eines Profilings vorgenommene Persönlichkeitsbewertung im konkreten Fall tatsächlich der betroffenen Person gerecht wird, hängt von der Genauigkeit des automatisierten Verfahrens ab. Üblicherweise liegen dem Profiling statistisch-mathematische Verfahren zugrunde, denen stets die Gefahr eines „Generalisierungsunrechts"[6] innewohnt. Verstärkt wird diese Problematik vor allem dadurch, dass Bewertungen beim Profiling regelmäßig nur auf Korrelationen und Wahrscheinlichkeiten beruhen, hinter denen keine Kausalitäten stehen müssen.[7] Umso wichtiger ist es daher, dass die Rechtmäßigkeitsanforderungen an das Profiling hoch angesetzt werden, etwa wenn die Zulässigkeit eines Profilings auf Grundlage einer allgemeinen Interessenabwägung nach Art. 6 Abs. 1 lit. f zu beurteilen ist. Von zentraler Bedeutung ist hier insbes. der Aspekt der **Datenqualität**: Nur wenn im Ausgangspunkt die Richtigkeit und Vollständigkeit in den Datenbeständen gewährleistet ist, kann der Verantwortliche für das Profiling überhaupt ein berechtigtes Interesse anführen. Ebenso kann die bisherige Wertung des § 28b BDSG zum Scoring ganz allgemein für jede Art des Profilings übernommen werden: Die Zulässigkeit eines Profilings kommt danach stets nur dann in Betracht, wenn der Verantwortliche auf Basis eines **wissenschaftlich anerkannten** mathematisch-statistischen Verfahrens **nachweisen** kann, dass die von ihm verarbeiteten Daten für die Bewertung eines bestimmten Persönlichkeitsaspekts **erheblich** sind.

Nr. 5 Pseudonymisierung

„Pseudonymisierung" 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;

Literatur *Art.-29-Datenschutzgruppe,* Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216; *Dammann,* Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307; *Härting,* Datenschutz-Grundverordnung – Anwendungsbereich, Verbotsprinzip, Einwilligung, ITRB 2016, 36; *ders.,* Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065; *Karg,* Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520; *Piltz,* Die Datenschutz-Grundverordnung – Teil 1: Anwendungsbereich, Definitionen und Grundlagen der Daten-verarbeitung, K&R 2016, 557.

I. Überblick

1 Art. 4 Nr. 5 definiert das Pseudonymisieren von personenbezogenen Daten. Eine Pseudonymisierung bietet sich in der Praxis immer dann an, wenn die jederzeitige Kenntnis der

[6] S. dazu ausf. *Britz* Einzelfallgerechtigkeit versus Generalisierung, passim.
[7] *Weichert* ZRP 2014, 168 (170).

Identität einer Person verzichtbar ist, die Daten jedoch gleichzeitig unter bestimmten Bedingungen mit einer bestimmten Person verknüpfbar bleiben sollen.

Charakteristisch für pseudonyme Daten ist – im Unterschied zu anonymen Daten – das Bestehen einer **Zuordnungsregel,** welche den unter einem Pseudonym erfassten Daten ein Identifikationsmerkmal einer Person zuweist. Eine Pseudonymisierung stellt daher **keine Anonymisierung,** sondern – wie Art. 32 Abs. 1 lit. a verdeutlicht – eine bloße Sicherungsmaßnahme dar.[1] **2**

Nach EG 28 besteht das **Ziel der Pseudonymisierung** darin, die Risiken für betroffene Personen zu senken und den Verantwortlichen und Auftragsverarbeiter bei der Einhaltung der Datenschutzpflichten zu unterstützen. Zugleich stellt der Verordnungsgeber klar, dass die Pseudonymisierung nur eine von mehreren in Betracht kommenden Möglichkeiten darstellen soll, betroffenen Personen Schutz zu gewähren und dass durch die ausdrückliche Einführung der Pseudonymisierung andere Datenschutzmaßnahmen nicht ausgeschlossen werden sollen. **3**

Der Pseudonymisierung kommt in der DS-GVO eine im Vergleich zur DSRL **leicht gesteigerte Bedeutung** zu. Eine ausdrückliche Privilegierung der Verarbeitung pseudonymisierter Daten enthält aber auch die DS-GVO nicht (zu den Anreizen für eine Pseudonymisierung → Rn. 13).[2] **4**

II. Anforderungen an Pseudonymisierung

Die DS-GVO definiert in Art. 4 Nr. 5 das Pseudonymisieren als die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen **nicht mehr einer spezifischen betroffenen Person zugeordnet** werden können. **5**

In Abgrenzung zur Anonymisierung (→ Art. 4 Nr. 1 Rn. 31) sind die zusätzlichen Informationen aber nicht zu löschen, sondern zu ersetzen und **gesondert aufzubewahren.** Gemeint ist hierbei eine technisch/räumlich getrennte Aufbewahrung.[3] **6**

Die personenbezogenen Daten sind zudem besonderen **technischen und organisatorischen Maßnahmen** zu unterwerfen, die gewährleisten, dass die Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. In Betracht kommen insoweit die Maßnahmen nach Art. 32. Diese müssen sicherzustellen, dass der Nutzer der pseudonymisierten Daten keinen Zugang zur Zuordnungsregel hat. Ausweislich EG 29 sollte der Verantwortliche die insoweit zur Nutzung befugten Personen angeben. **7**

III. Arten und Verfahren der Pseudonymisierung

Eine Pseudonymisierung personenbezogener Daten kann auf verschiedene Arten vorgenommen werden. So kann die Zuweisung des Pseudonyms durch die betroffene Person selbst erfolgen, etwa indem sie unter einer frei gewählten Nutzer-ID auftritt. Denkbar ist es auch, dass ein Dritter, zB eine Zertifizierungsstelle oder Datentreuhänder, das Pseudonym zuweist. Schließlich kann die Zuweisung des Pseudonyms **durch den Verantwortlichen** erfolgen (beispielsweise durch Zuweisung einer Kennziffer), dem die Identität der betroffenen Person bekannt ist. Von diesem Fall scheint Art. 4 Nr. 5 primär auszugehen. **8**

Für den Vorgang der Pseudonymisierung kommen verschiedene Möglichkeiten in Betracht, etwa die logische Trennung der Information, die Implementierung eines Rechte- und Rollenkonzepts, oder die Erzeugung von Zufallswerten und die Zuordnung zur **9**

[1] Ebenso bereits *Art.-29-Datenschutzgruppe* Stellungn. 5/2014 zu Anonymisierungstechniken, WP 216, 3 und 12.

[2] *Piltz* K&R 2016, 557 (562); krit. hierzu *Härting* ITRB 2016, 36 (38).

[3] Vgl. *Ernst* in Paal/Pauly Art. 4 Rn. 43.

betroffenen Person mittels Referenzliste. Auch die **Verschlüsselung** von Daten kann eine Pseudonymisierung darstellen, obgleich Art. 6 Abs. 4 lit. e und Art 32 Abs. 1 lit. a „Verschlüsselung" und „Pseudonymisierung" als zwei unterschiedliche im Abwägungsprozess zu berücksichtigende Maßnahmen beschreiben. Denn die Daten können erst nach Hinzuziehung zusätzlicher Informationen (des Schlüssels) wieder lesbar gemacht werden. EG 83 sieht insoweit vor, dass Verschlüsselungsmaßnahmen unter Berücksichtigung des Stands der Technik erfolgen sollen.

10 Werden Pseudonymisierungsverfahren verwendet, sollte stets vorab **zwischen den Beteiligten geklärt** werden, wer das Pseudonym generiert, wer im Besitz der Zuordnungsregel sein soll und unter welchen Umständen diese weitergegeben und mit Identifikationsmerkmalen zusammengeführt werden darf.

IV. Pseudonymisierung und Personenbezug

11 EG 26 bestimmt, dass pseudonymisierte Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können, als Informationen über eine identifizierbare natürliche Person zu betrachten sind. Pseudonymisierte Daten weisen folglich einen **Personenbezug** auf. Dogmatisch gesehen handelt es sich bei pseudonymisierten Daten daher um einen Unterfall von personenbezogenen Daten (→ Art. 4 Nr. 1).[4] Dies hat zur Folge, dass die Regelungen der DS-GVO für die Verarbeitung pseudonymisierter Daten im vollen Umfang zu beachten sind.

12 Problematisch sind Fälle, in denen ein Verantwortlicher pseudonymisierte Daten selbst nicht durch Heranziehung zusätzlicher Informationen einer natürlichen Person zuordnen kann, aber ein **Dritter im Besitz einer Zuordnungsregel** ist. Virulent wird dies etwa dann, wenn ein Arzt pseudonymisierte Blutproben in ein Labor einschickt. Der Arzt kennt regelmäßig die Zuordnungsregel, wohingegen sie dem Labor unbekannt ist. Eine ähnliche Problematik besteht, wenn ein Treuhänder oder die betroffene Person selbst das Pseudonym verwaltet. Ob in diesen Fällen auch für den Verantwortlichen (und nicht bloß für den Dritten) ein Personenbezug vorliegt, ist vor dem Hintergrund der Ausführungen des EuGH zu beantworten, die dieser zur Frage der Maßgeblichkeit des Zusatzwissens Dritter aufgestellt hat (ausführlich → Art. 4 Nr. 1 Rn. 19 ff.).[5]

V. Anreize für eine Pseudonymisierung

13 Der praktische Anreiz, personenbezogene Daten zu pseudonymisieren, liegt auch unter der DS-GVO darin, dass eine **Interessenabwägung** eher zugunsten des Verantwortlichen ausfallen wird, der eine Pseudonymisierung vornimmt, als wenn es zu keiner Pseudonymisierung kommt.[6] Auch ist der technisch-organisatorische Schutzbedarf bei pseudonymen Daten geringer. Zudem besteht im Falle von Datenschutzverstößen nach Art. 34 Abs. 3 lit. a **keine Benachrichtigungspflicht** gegenüber der betroffenen Person, wenn Verschlüsselungsverfahren angewandt wurden (zur Verschlüsselung als Unterfall der Pseudonymisierung → Rn. 9). Kommt es zu einer **Zweckänderung** bei der Datenverarbeitung, fließt die Tatsache, dass die Daten pseudonymisiert verarbeitet werden, nach Art. 6 Abs. 4 lit. e in den Abwägungsprozess ein.[7] Überdies kann die privilegierte Verarbeitung von personenbezogenen Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken nach Art. 89 eine Pseudonymisierung erfordern.

---

[4] Ebenso *Karg* DuD 2015, 520 (524).

[5] EuGH Urt. v. 19.10.2016 – C-582/14, Rn. 31 ff. – Breyer mAnm *Kühling/Klar* ZD 2017 (im Erscheinen).

[6] *Härting* NJW 2013, 2067; *Karg* DuD 2015, 520 (524); *Scholz* in Simitis BDSG § 3 Rn. 219d.

[7] Diesen Mechanismus lobend *Dammann* ZD 2016, 307 (314).