Das neue Datenschutzrecht

Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis

Bearbeitet von
Dr. Peter Schantz, Prof. Dr. Heinrich Amadeus Wolff

1. Auflage 2017. Buch. XL, 437 S. Kartoniert
ISBN 978 3 406 69649 7
Format (B x L): 14,1 x 22,4 cm

wendig ist. Der Grundsatz der Erforderlichkeit setzt eine rechtmäßige Datenverarbeitung und eine rechtmäßige Zweckbestimmung der Datenverarbeitung voraus und grenzt diese noch einmal ein. Er ist entwickelt worden für Datenverarbeitungen, die sich auf Rechtsnormen stützen. Dies ist der Grund, weshalb Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO die Erforderlichkeit nicht erwähnt.[606] Der Grundsatz der Erforderlichkeit ist nicht in Art. 5 DS-GVO als Grundsatz genannt, aber in Art. 6 Abs. 1 UAbs. 1 lit. b bis lit. f DS-GVO enthalten.

Es ist nicht abschließend geklärt, ob der Grundsatz der Erforderlichkeit **gleichgesetzt** werden kann mit der **Erforderlichkeitsstufe** des verfassungsrechtlichen Grundsatzes der **Verhältnismäßigkeit**. Es bestehen aber zumindest weitgehende Übereinstimmungen. Als geringfügige Abweichungen sind zu verzeichnen: Beim Grundsatz der Erforderlichkeit liegt der verfolgte Zweck nicht in einem Gemeinwohlzweck, sondern in einer Datenverarbeitung zu einem Gemeinwohlzweck, weiter bezieht der Grundsatz die Frage der Geeignetheit mit ein und ebenso eklatante Fälle der Unverhältnismäßigkeit, dh der sogenannten Angemessenheit und trennt daher die Stufen, anders als der Grundsatz der Verhältnismäßigkeit, nicht. **430**

Der Grundsatz der Erforderlichkeit besitzt im Abstrakten einen **klaren Kern,** im Grenzbereich kann seine Bestimmung schwierig sein.[607] Nach seinem Kern gestattet eine generelle Erlaubnis der Datenverarbeitung nicht, dass diese Daten immer und für jeden Zweck im Rahmen der generellen Erlaubnisnorm verwendet werden dürfen, sondern nur konkret, soweit dies zur Erreichung eines konkret festgelegten Zweckes geboten ist. Er kann dabei auch über die Verarbeitung personenbezogener Daten als solche entscheiden. So ist deren Verarbeitung nicht erforderlich, wenn der Zweck auch mit der Verarbeitung anonymisierter Daten erreichbar ist.[608] **431**

Der Grundsatz der Erforderlichkeit gemäß Art. 5 Abs. 1 lit. d DS-GVO besitzt **mehrere Bedeutungsebenen**. Die Datenverarbeitung muss objektiv tauglich sein, den festgelegten Zweck zu erreichen bzw. seine Zweckerreichung zu erleichtern. Der Grundsatz der notwendigen Beschränkung verlangt, dass keine alternative Form der Datenverarbeitung besteht, die die Zwecke in vergleichbarer Weise erreichen kann und zugleich als datenschutzschonender zu qualifizieren ist (Gebot der Alternative). **432**

(2) Objektive Gebotenheit – Kausalität. Zunächst enthält der Grundsatz ein Gebot des Erfordernisses einer kausalen Zweckförderung. Die Datenverarbeitung muss **objektiv tauglich** sein, den festgelegten Zweck zu erreichen bzw. seine Zweckerreichung zu erleichtern. Zwischen der beabsichtigten Datenverarbeitung und dem Datenverarbeitungszweck muss ein unmittelbarer sachlicher Zusammenhang bestehen.[609] Lehnt man sich an die übliche Kausa- **433**

---

[606] *Art. 29-Gruppe* Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Art. 7 der Richtlinie 95/46/EG, WP 217 v. 9.4.2014, S. 13.

[607] *Tiedemann* NJW 1981, 945 (946).

[608] EuGH NVwZ 2009, 389 Rn. 65 – Huber.

[609] BAG NZA 1987, 415 (416).

litätsprüfung an, gilt: Kann die Datenverarbeitung hinweggedacht werden, ohne dass die Zweckerreichung erschwert oder verhindert wird, ist die Datenverarbeitung nicht erforderlich.

434 *(3) Die Frage der datenschutzschonenden Alternative.* Der Grundsatz der Erforderlichkeit verlangt nach zutreffender Auffassung aber nicht nur, dass eine Datenverarbeitung unterbleibt, die für die Zwecke überhaupt keinen Vorteil bringt. Er verlangt auch, dass keine alternative Form der Datenverarbeitung besteht, welche die Zwecke in vergleichbarer Weise erreichen kann und zugleich als datenschutzschonender zu qualifizieren ist (Gebot der **datenschutzschonenderen** oder datenschutzintensiveren **Alternative**). Die Frage, wie plausibel oder wie geboten die Datenverarbeitung für die Zweckerreichung ist, beruht (anders als die Prüfung des objektiven Kausalitätsverhältnisses) auf einem Werturteil. Die Datenverarbeitung ist zumindest dann gerechtfertigt, wenn diese ein geeignetes Mittel ist, für das es keine zumutbare Alternative gibt. Nicht notwendig ist, dass die Datenverarbeitung aus technischen, wirtschaftlichen, organisatorischen oder sonstigen Gründen schlechterdings unverzichtbar ist. Der Grundsatz der Erforderlichkeit kann **nicht** im Sinne einer **absolut zwingenden Notwendigkeit** oder einer bestmöglichen Effizienz verstanden werden. Entscheidend ist, ob nach den Gesamtumständen die Wahl einer anderen Informationsmöglichkeit oder der Verzicht hierauf nicht sinnvoll oder nicht zumutbar wäre und für dieses Werturteil dabei die grundsätzliche Organisationsform und Arbeitsweise des Verantwortlichen zugrunde gelegt wird. Komplizierte Formen der Arbeitsabläufe, die unsinnige Mengen von personenbezogenen Daten anhäufen, genügen dem Datenminimierungsgrundsatz auch dann nicht, wenn sie der Zweckerreichung objektiv gesehen noch dienen.

435 Die Frage, welche Datenverarbeitung im Vergleich zu einer anderen datenschutzschonender oder datenschutzintensiver ist, richtet sich nach allgemeinen Kriterien. Entscheidend ist, welche Datenverarbeitung, sofern sie auf einer gesetzlichen Grundlage beruhen würde, als der schwerere Eingriff zu qualifizieren ist. Nicht immer ist die Rangfolge klar zu benennen, oftmals werden die Varianten jeweils spezifische Vor- und Nachteile aufweisen. Die entscheidenden Maßstäbe für die Bewertung der Schwere wären: Art der Daten (sensible oder nicht sensible), Art der Datenverarbeitung, Missbrauchsgefahren, Verwendungsmöglichkeiten, Verknüpfungsmöglichkeiten, Verfahrensabsicherungen, Transparenzgebote, Gebote der Datensicherheit, Datenmenge, Anzahl der betroffenen Personen usw.

436 Das Gebot der datenschutzmilderen Alternative ist **mit Vorsicht** anzuwenden, da der Grundsatz der Erforderlichkeit der verarbeitenden Stelle vorschreiben darf, wie sie die Datenverarbeitung selbst zu organisieren hat, aber nicht in einer Weise, die ihr jeweiliges Selbstorganisationsrecht über Gebühr beeinträchtigt. Man kann der verantwortlichen Stelle keine Umorganisation vorschreiben mit der Folge, dass auf diese Weise die Datenverarbeitung dem Sinn des allgemeinen Persönlichkeitsrechts besser gerecht würde, wenn nicht sicher ist, dass alle anderen Faktoren, die für den Verantwortlichen zentral sind, gleich bleiben. Der Grundsatz der Erforderlichkeit verlangt nicht, dass die Ziele, die innerhalb der rechtlichen Grundlage der Datenverarbeitung liegen,

aufgegeben werden, nur weil es andere Möglichkeiten gäbe, die ein ähnliches Ergebnis erzielten und datenschutzmilder erreichbar wären. Der **Datenminimierungsgrundsatz** bezieht sich auf die **Datenverarbeitung** und nicht auf die **Zweckbestimmung**. Will beispielsweise ein Unternehmen werben und dafür auf die Werbung per Brief zurückgreifen, darf der Grundsatz der Erforderlichkeit vorschreiben, welche Daten verwendet werden dürfen, um die Briefwerbung durchzuführen; nicht zulässig wäre es aber, die Briefwerbung als solche zu untersagen mit dem Hinweis, eine Werbung mit einem großen Plakat am Firmensitz sei deutlich datenschutzfreundlicher und für die Zweckerreichung gleich wirksam. Den Zweck, der erreicht werden soll, darf der Verantwortliche selbst bestimmen. Dient die Datenverarbeitung objektiv dem konkret von der verantwortlichen Stelle festgelegten Zweck, müssen besondere Umstände hinzukommen, weshalb die Erforderlichkeit dennoch verneint werden kann.

Allerdings wirkt sich der Erforderlichkeitsgrundsatz von seiner Ratio her **437**
mit einer gewissen **Vorwirkung** auch auf die Zweckbestimmung im Rahmen eines Zumutbarkeitsprinzips aus. Liegen daher zwei verschiedene Ziele, die mit der Datenverarbeitung erreicht werden sollen, der Sache nach nahe nebeneinander, rufen aber ganz unterschiedliche datenschutzrechtlich relevante Datenverarbeitungsvorgänge hervor, so wird man zutreffender Ansicht nach von der verantwortlichen Stelle verlangen können, das Ziel zu wählen, das deutlich datenschutzmilder erreicht werden kann, wenn keine erkennbaren Interessen der verarbeitenden Stelle für das andere Ziel bestehen, und die Pflicht, das datenschutzmildere Ziel zu wählen, im Einzelfall zumutbar ist.

cc) Unterschiede zum Grundsatz der Datenminimierung. Der Grund- **438**
satz der **Erforderlichkeit** ist eng mit dem Grundsatz der **Datenminimierung verbunden** aber **nicht identisch**. Das sieht man schon daran, dass der Grundsatz der Datenminimierung für alle Verarbeitungen gilt, der Grundsatz der Erforderlichkeit aber nicht bei einer Verarbeitung auf der Grundlage der Einwilligung gilt.

Weiter ist der **Ansatzpunkt** unterschiedlich. Die Datenminimierung bezieht **439**
sich auf das Verhältnis von personenbezogenen Daten zum Zweck und der Grundsatz der Erforderlichkeit bezieht sich auf die Verarbeitung personenbezogener Daten. Der Grundsatz der Datenminimierung ist daher mehr statusbezogen, gewissermaßen auf die Verfügbarkeit der personenbezogenen Daten abstellend, während der Grundsatz der Erforderlichkeit die Verarbeitungssituation in den Blick nimmt. Liegt eine nicht erforderliche Verarbeitung vor, dürfte in der Regel aber zugleich ein Verstoß gegen die Datenminimierung vorliegen, weil dann der Verantwortliche das relevante Datum kaum vorhalten muss. Umgekehrt dürfte die Verarbeitung eines Datums, das gegen den Grundsatz der Datenminimierung verstößt, den Grundsatz der Erforderlichkeit missachten. Dennoch leuchten beide Grundsätze unterschiedliche Aspekte aus, der eine ist datenbezogen und der andere verarbeitungsbezogen.

f) Anwendungsbereich der JI-RL (§ 45 BDSG nF). Auch dieser Grund- **440**
satz wird im BDSG nF wiederholt **(§ 47 Nr. 3 BDSG nF**). Sachlich gilt das Gleiche. Den Hintergrund bildet Art. 4 Abs. 1 lit. c JI-RL.

8. Datenrichtigkeit gem. Art. 5 Abs. 1 lit. d DS-GVO

441 Das Gebot der **Richtigkeit** besagt im Kern: Der Verantwortliche hat Sorge dafür zu tragen, dass personenbezogene Daten **sachlich richtig sind**. Dies ist wichtig, denn personenbezogene Daten sind die Basis für das Bild, das sich die Mitmenschen von einer Person machen und auf der sie Entscheidungen treffen. Schon das BVerfG hat in seinem Volkszählungsurteil darauf hingewiesen, dass der Betroffene unter den Bedingungen der modernen Datenverarbeitung die Richtigkeit der über ihn verarbeiteten Daten nur noch schwer kontrollieren kann.[610] Dies gilt umso mehr, weil durch das Internet die Verbreitung von Informationen immer leichter wird, aber zugleich immer schwerer korrigiert werden kann.

442 Der Grundsatz der Richtigkeit enthält unterschiedliche Gebote, je nachdem ob es um die Erhebung und Speicherung oder um die spätere Kontrolle geht.[611] Bei der **erstmaligen Speicherung** hat der Verantwortliche mit der üblichen Sorgfalt zu **prüfen**, ob Gesichtspunkte gegen die Richtigkeit der erhobenen Daten sprechen. Werden Unrichtigkeiten **später bekannt**, sind die Daten zu **korrigieren**. Gibt es Anzeichen für eine Unrichtigkeit, darf der Verantwortliche nicht die Augen verschließen, sondern muss ihnen nachgehen. Darüber hinaus verlangt Art. 5 Abs. 1 lit. d DS-GVO ausdrücklich, dass angemessene Mittel zu fassen sind, damit der Verantwortliche von diesen Anzeichen auch Kenntnis nimmt.

443 Für den Bereich des § 45 BDSG nF ist sachlich das Gleiche in § 46 Nr. 4 BDSG nF niedergelegt (vgl. Art. 4 Abs. 1 lit. d JI-RL).

9. Speicherbegrenzung gem. Art. 5 Abs. 1 lit. e DS-GVO

444 Das in Art. 5 Abs. 1 lit. e DS-GVO wortreich umschriebene Prinzip der **Speicherbegrenzung** enthält der Sache nach zwei Gebote. Zum einen verlangt es nach einer zeitlichen Begrenzung der Speichermöglichkeiten. Nur solange wie dies zur Erreichung der Zwecke erforderlich ist, dürfen die Daten gespeichert werden. Er bildet daher gewissermaßen einen Grundsatz der Datenminimierung aus zeitlicher Perspektive. Er bildet die objektive Grundlage für den Anspruch auf Vergessen gemäß Art. 17 DS-GVO. Weiter begründet er die Pflicht des Verantwortlichen, von sich aus personenbezogene Daten nicht mehr weiter zu verarbeiten, wenn es hierfür mangels Erforderlichkeit keine Rechtsgrundlage mehr gibt. Ew 39 DS-GVO spricht von einer Überprüfung zu vorher festgelegten Intervallen.

445 Darüber hinaus enthält das Gebot aber auch ein Gebot **der frühestmöglichen Anonymisierung.** Dem Gebot der Speicherbegrenzung wird auch dadurch genügt, dass die Daten, die länger gespeichert werden als für die Zweckerreichung erforderlich, nicht mehr einer Person zugerechnet werden können und daher keine personenbezogenen Daten mehr sind.

---

[610] BVerfGE 65, 1 (42) – Volkszählung.
[611] Vgl. *Frenzel* in Paal/Pauly DS-GVO Art. 5 Rn. 40.

Fraglich ist, ob man aus dem Grundsatz der Speicherbegrenzung das Gebot herleiten muss, Daten, die einer bestimmten Person zuzurechnen sind, soweit zu verallgemeinern, dass die Person gegebenenfalls nur noch bestimmbar ist. Der Wortlaut verlangt die Reduzierung der Bestimmbarkeit nicht ausdrücklich, vom Sinn her ist es aber nicht ausgeschlossen, auch ein Gebot der Reduzierung der Bestimmtheit herbeizuführen, wenn dies mit einem erheblichen Gewinn für den Datenschutz verbunden sein sollte. Ob der Gedanke sich durchsetzt, bleibt abzuwarten. **446**

Für den Bereich des § 45 BDSG nF ist sachlich das Gleiche, allerdings deutlich wortärmer, **in § 46 Nr. 5 BDSG nF** niedergelegt (vgl. Art. 4 Abs. 1 lit. e JI-RL). **447**

10. Integrität und Vertraulichkeit gem. Art. 5 Abs. 1 lit. f DS-GVO

Integrität meint der Sache nach **Unversehrtheit**, **Unverfälschtheit** und **Vollständigkeit**. **Vertraulichkeit** meint hingegen **Quantität** und **Qualität** der **Sicherung** vor einem **fremden Zugriff**. Der Grundsatz der Integrität und Vertraulichkeit besitzt eine erhebliche Sprengkraft. Er verlangt, dass eine angemessene technische Sicherheit für die personenbezogenen Daten durch den Verantwortlichen gewährleistet wird. Die Angemessenheit hängt von der Bedeutung der Daten, dem Interesse des Verantwortlichen, den Interessen der betroffenen Person und der Schutzgefährdung ab. Auch dieser Grundsatz wird nicht als reines Optimierungsgebot verstanden, sondern als bindendes Prinzip, dessen Verletzung durchaus Geldbußen hervorrufen kann. Dennoch ist der Grundsatz im Wesentlichen auf Konkretisierungen angelegt. Die DS-GVO enthält einige spezielle Normen zur Datensicherheit, die insofern diesen Grundsatz weiter konkretisieren. Innerhalb seiner Befugnisse kann auch der nationale Gesetzgeber den Grundsatz der Datensicherheit konkretisieren. So ist etwa das Recht auf IT-Sicherheit, das den Betreibern gefährlicher Infrastrukturen gewisse technische Sicherheitsstandards auferlegt, als eine Konkretisierung dieses Grundsatzes zu begreifen. Für den Bereich von § 45 BDSG nF eröffneten Verarbeitungsbereich s § 46 Nr. 6 BDSG nF. **448**

11. Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO

Gemäß Art. 5 Abs. 2 DS-GVO folgt aus der Verpflichtung, die Grundsätze einzuhalten, zugleich eine **Darlegungslast** für den Verantwortlichen. Wie er der Darlegungslast nachkommt, ist in der Norm nicht vorgegeben.[612] Auch diese Norm ist weitgehend konkretisierungsbedürftig, in Extremfällen ist aber ein Verstoß auch ohne Konkretisierung rechtlich erheblich. **449**

12. Prinzipien außerhalb des Art. 5 DS-GVO

a) Allgemein. Von den Grundsätzen des Art. 5 DS-GVO einerseits, aber auch von den Konzeptionsprinzipien, denen die DS-GVO folgt, andererseits sind die **übergreifenden datenschutzrechtlichen Prinzipien**, denen das Da- **450**

[612] *Herbst* in Kühling/Buchner DS-GVO Art. 5 Rn. 80; s. etwa für den Krankenhausbereich *Hauser* in KH 2016, 690 ff.

tenschutzrecht auch außerhalb der Grundverordnung folgt, zu trennen. Diese weiteren Prinzipien sind in ihrer Wirkung nicht mit denen des Art. 5 DS-GVO zu vergleichen, weil sie nur direktive Wirkung entfalten. Sie sind auch mit den Konzeptionsprinzipien nicht vergleichbar, weil sie keine kodifikationsinternen Prinzipien bilden. Die Prinzipien werden aus der **Analyse** des **Datenschutzrechtes** gewonnen und treffen Aussagen über die Besonderheiten dieses Gebietes. Die Prinzipien, die nun hier angesprochen sind, nehmen zunächst eine **wissenschaftliche Funktion** ein, indem sie die Rechtsordnung systematisieren und erklären können und auch eine Erleichterung bei dem Verständnis des Rechtsgebietes bieten können. Weiter besitzen sie auch eine sekundäre normative Bedeutung insofern, als sie Einfluss auf die Auslegung einzelner Rechtssätze gewinnen können, insbes. im Rahmen der systematischen Auslegung.

451 **b) Prinzip der Schutzräume.** Ein allgemeines Prinzip des Datenschutzrechtes ist dessen Raumabhängigkeit. Die **Raumabhängigkeit** meint, dass die Reichweite des Datenschutzrechtes von einem definierten Schutzraum abhängt. Der Begriff des Raumes ist dabei räumlich, gegenständlich und funktional zu verstehen. Der Anknüpfungspunkt des Datenschutzrechtes sind Daten. Daten sind omnipräsent wie auch die Luft oder das Licht. Dennoch ist das Datenschutzrecht selbst nicht omnipräsent. Vielmehr existieren Datenschutzbereiche. Ein Teil dieser Datenschutzräume ergibt sich aus der Natur der Sache und wird vom Gesetzgeber nur deklaratorisch nachgezeichnet, ein Teil dagegen wiederum konstitutiv bestimmt.

452 Ein Raum, der ursprünglich schon datenschutzfrei ist, ist das menschliche **Gehirn**. Daten, die im menschlichen Gehirn gespeichert werden, werden vom Datenschutzrecht nicht erfasst. Wenn ein Mensch in seinem natürlichen Speichermedium personenbezogene Daten abspeichert, bedarf er dafür keiner gesetzlichen Grundlage. Er unterliegt auch keiner Auskunftspflicht der betroffenen Person hinsichtlich der Daten, die er selbst im Kopf gespeichert hat. Zwar gibt es Auskunfts- und Zeugnispflichten gegenüber Gerichten und Behörden, diese sind aber durch deren Verwaltungsaufgabe und nicht durch den Datenschutz motiviert.

453 Vom Gesetzgeber definiert ist dagegen die Begrenzung des Datenschutzraumes auf **natürliche Personen** (§ 3 Abs. 1 BDSG/Art. 2 Abs. 1 DS-GVO). Juristische Personen genießen einen deutlich geringeren Datenschutz.

454 Weiter werden durch die Normsetzungskompetenzen im Wesentlichen drei Räume definiert, der Datenschutzraum im Anwendungsbereich der DS-GVO, der im Anwendungsbereich der Richtlinie für die Sicherheit (RL (EU) 2016/680) und der im Bereich der Autonomie der Mitgliedsstaaten. Künftig könnte als vierter Bereich Art. 39 EUV hinzukommen.

455 Eine **funktionale Raumdefinition** knüpft an die Formen des Datenumgangs an, der rechtlich definiert wird. Rechtliche Anknüpfungspunkte sind etwa: die Art der Datenverarbeitung (nur elektronische Datenverarbeitung nicht-öffentlicher Stellen), die Zugehörigkeit zu einer Datei oder die Verarbeitungsformen. So waren bekanntlich etwa die älteren Datenschutzgesetze noch weitgehend an das Vorhandensein einer Datei gebunden und im Bereich der Datenverarbeitung unter Privaten war der Vorgang der Datenerhebung zunächst noch nicht erfasst. Eine alte Unterscheidung, der aber neuerdings unge-

ahnte Wirkung zukommt, ist die zwischen verdeckter und offener Erhebung. Nach der verfassungsgerichtlichen Rechtsprechung gelten für die geheime Datenerhebung so massiv strengere Anforderungen, dass es gerechtfertigt ist, von einer kategorial anderen Art von Rechtfertigungsbedürftigkeit zu sprechen.

c) Grundsatz der Direkterhebung. Nach dem Grundsatz der **Direkterhebung** sind personenbezogene Daten grds beim Betroffenen zu erheben. Eine Erhebung in anderer Weise bedarf einer sachlichen Rechtfertigung. Im deutschen Recht ist der Grundsatz in § 4 Abs. 2 BDSG aF normiert. Der Grundsatz ergibt sich der Sache nach schon aus dem Recht auf informationelle Selbstbestimmung, wobei die Bestimmung, wann Ausnahmen zulässig sind, sich nicht abschließend oder eindeutig aus der Verfassung selbst ergibt. Der Zweck des Grundsatzes der Direkterhebung liegt auf der Hand. Er dient dazu, die Subjektqualität der betroffenen Person bei Informationsvorgängen zu seiner Person zu stärken. Der Grundsatz der Direkterhebung geht dabei unausgesprochen von einer offenen Datenerhebung aus, dh von einer Informationsbeschaffung, die für den Betroffenen erkennbar ist, weil nur so sein Ziel erreicht werden kann. In der DS-GVO ist er nicht ausdrücklich normiert.[613] Er lässt sich gegebenenfalls mittelbar aus den Grundsätzen der Transparenz und des Treu und Glaubens herleiten. Inwieweit sich dies durchsetzen wird, bleibt aber abzuwarten. **456**

d) Erkennbarkeit der Datenvalidität. Gemäß Art. 7 Abs. 1 JI-RL ist bei den zu verarbeitenden Datenkategorien so weit wie möglich zu unterscheiden zwischen Daten, die auf Fakten beruhen, und Daten, die auf persönlicher Einschätzung beruhen. Die Norm setzt ihrem Sinn nach voraus, dass so weit wie möglich erkennbar ist, ob personenbezogene Daten auf **Fakten** oder auf persönlichen **Einschätzungen** beruhen. Sofern dies an dem Datum selbst erkennbar ist, wird man eine ausdrückliche Kennzeichnung nicht verlangen müssen. Häufig werden aber Tatsachen im Sicherheitsbereich auf Mutmaßungen gestützt, ohne dass erkennbar ist, dass die Tatsache nicht selbst ermittelt, sondern geschlossen wurde. Art. 7 Abs. 2 JI-RL verlangt in diesen Fällen einen Hinweis, dass die Tatsache auf einer Schlussfolgerung beruht. Erforderlich wird es daher sein, in den datenschutzrechtlichen Grundlagen des nationalen Rechts zumindest eine Sollvorschrift aufzunehmen, die die Offenlegung bei Tatsachen, die auf Schlussfolgerungen beruhen, verlangt. **457**

Weiter ist gem. Art. 7 Abs. 2 JI-RL die Datenqualität im Auge zu behalten und gem S. 1 mögliche **invaliden** Daten nicht zu übermitteln und falls sie übermittelt werden nach S. 3 die Umstände mitzuteilen, die eine Beurteilung der Validität erlauben. Vom Text her verlangt die Norm nicht eine unterschiedliche Datenverarbeitung, sondern die Erkennbarkeit des Grades der Richtigkeit und der Zuverlässigkeit bzw der Unterscheidung zwischen Fakten und Werturteil. Die Norm richtet sich primär an die Datenverarbeitung, ist aber ohne entsprechende Verankerung im Datenschutzrecht selbst nicht zu erfüllen. Abs. 2 ist wiederum als ein weiches Optimierungsgebot formuliert, dennoch sind seine Vorgaben ganz erheblich und für die deutsche Rechtsordnung neu. **458**

[613] *Buchner* DuD 2016, 155 (156); *Raab* Harmonisierung, 2015, 58; *Gola* in Gola DS-GVO Einl. Rn. 41.

Art. 7 Abs. 2 JI-RL verlangt die Angabe der Wahrscheinlichkeit der Richtigkeit von Daten. Im deutschen Recht spielen die Verlässlichkeit und die Richtigkeit von Tatsachen insofern eine Rolle, als je nach Eingriffsgrundlage der zugrunde liegende Sachverhalt eine unterschiedliche Richtigkeitsgewährleistung besitzen muss.

459 Das erforderliche Ausmaß der Verlässlichkeit der Datengrundlage wird der Sache nach bei der erforderlichen polizeilichen Gefahrenprognose oder dem strafverfahrensrechtlichen Verdachtsmoment mitgeprüft. Eine formale Kennzeichnung sieht das deutsche Recht nicht vor. Für den Bundesbereich wird Art. 7 JI-RL durch § 73 BDSG nF umgesetzt, nach dem der Verantwortliche bei der Verarbeitung so weit wie möglich danach zu unterscheiden hat, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen. Die Vorschrift ist ausgesprochen weich formuliert und als unverbindliche Optimierung ausgestattet. Angesichts der Innovation dieser Vorgabe erscheint eine vorsichtige Formulierung nicht unsinnig. Die Gesetzesbegründung verweist darauf, die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, wie etwa unterschiedliche Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit bleiben dem Fachrecht überlassen.[614]

460 Der **Gedanke der Bewertung der Daten** nach ihrer Qualität setzt sich bei der **Übermittlung** fort. Im Rahmen der Übermittlung muss der Empfänger so weit wie möglich Informationen haben, um die Qualität der Daten beurteilen zu können. Dies regelt ausdrücklich § 74 BDSG nF, der verlangt, dass die übermittelnde Stelle erstens die Daten auf ihre Qualität vor der Übermittlung überprüft und zweitens notwendige Informationen für die Prüfung des Empfängers beifügt (§ 74 BDSG-RJ). In der Gesetzesbegründung wird darauf hingewiesen, dass im Hinblick auf die Vervollständigung unvollständiger Daten als möglichen Sinn und Zweck einer Datenübermittlung die in der JI-RL enthaltene Vermeidung der Übermittlung „unvollständiger" Daten nicht übernommen worden sei. Ferner sei bei der Anwendung und Auslegung der Anforderungen des § 74 BDSG nF zu beachten, dass die Frage nach der „Aktualität" von Daten und der damit verbundenen Vorgabe, keine „nicht mehr aktuellen" Daten zu übermitteln bzw. bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks sich beantworten lasse. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktueller Daten wie alte Meldeadressen, alte (Geburts-)namen etc. bedeutsam und für die Aufgabenerfüllung erforderlich sein.[615]

[614] BT-Drs. 18/11325, S. 118.
[615] BT-Drs. 18/11325, S. 118.