Originalbeiträge

Thomas K. Heinz

Das neue Datenschutzrecht und seine Auswirkungen auf Sachverständige und Verfahrensbeistände

Zusammenfassung

Wer als Gutachter, Sachverständiger oder Verfahrensbeistand tätig ist, den treffen auch die Änderungen des Bundesdatenschutzgesetzes durch die Datenschutzgrundverordnung (DSGVO)[1]. In dem Moment, in dem eine Telefonnummer notiert wird, eine Adresse für eine Rechnung gespeichert oder eine E-Mail über ein Kontaktformular empfangen wird, ist man im Besitz personenbezogener Daten und hat entsprechend der DSGVO zu handeln. So ist beispielsweise schon beim Betreiben einer Website kenntlich zu machen, dass die Daten entsprechend den neuen Bestimmungen behandelt werden. Für Juristen wie Nichtjuristen besteht das Problem darin, dass die Bestimmungen der DSVGO vielfach mit sogenannten auslegungsbedürftigen Rechtsbegriffen (zum Beispiel "berechtigten Interessen") arbeiten, die wenig Rechtssicherheit bieten, zumal es praktisch bis heute bei zu vielen Definitionen keine klärenden Gerichtsentscheidungen gibt. Welche Auswirkungen haben die neuen Bestimmungen auf Sachverständige und Verfahrensberater, auf die Berichte und den Tagesablauf des Amtes bei der Erhebung, Verarbeitung und Verwaltung personenbezogener Daten?
Schlüsselworte: Datenschutzgrundverordnung, Sachverständiger, Gutachter, Verfahrensbeistand, personenbezogene Daten, auslegungsbedürftiger Rechtsbegriff

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) – https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=BG (Zugriff am 23.1.2019).

DOI: 10.5771/2365-1083-2019-1-6

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

The new data protection law and its effects to experts, appraisers and procedural assistance

Abstract

Anyone who works as an expert, appraiser or procedural advisor will also be subject to the amendments of the Federal Data Protection Act through the *General Data Protection Regulation* (DSGVO). At the moment a phone number is recorded, an address is saved for an invoice or an e-mail is received via a contact form, you are in possession of personal data and must act in accordance with the the requirements of DSGVO. For example, when running a website, it should be noted that the data will be treated according to the new regulations. For legal persons and non-legal persons, the problem here is that the DSVGO provisions in many places work with so called legal terms requiring interpretation (for example "legitimate interest"), which offer little legal certainty, especially since there are virtually no clarifying court decisions to date. What impact do the new provisions have on experts and procedural advisers, on the reports and daily routine of the office when collecting, processing and managing personal data?
Keywords: general basic data protection regulation, expert, appraiser, procedural assistance, personal data, legal term requiring interpretation

1 Einführung

Seit dem 25.5.2018 gilt die EU-DSGVO ohne weitere Übergangsregelung für alle EU-Mitgliedsstaaten und damit auch für die Bundesrepublik Deutschland. Das Bundesdatenschutzgesetz (BDSG) hat ausgedient und greift in Zukunft nur dort, wo die DSGVO Raum für nationale Regelungen bietet.[2] Die Ziele der Bestimmungen der DSGVO entsprechen im Wesentlichen denen des alten Bundesdatenschutzrechts. Neu sind die Haftungsregelungen bei Auftragsverarbeitern, die nun bei der entsprechenden Vertragspartei liegt, die Datenschutzfolgeabschätzung, die deutlich tiefer greift als die alte Vorabkontrolle, die erweiterten Anforderungen an die technischen und organisatorischen Maßnahmen, eine klare Stärkung der Transparenz und der Rechte der Betroffenen sowie die Verpflichtung, bei der Planung und Umsetzung den Datenschutz mit zu beachten und datenschutzfreundliche Einstellungen zu treffen.

Für Juristen wie Nichtjuristen ist hierbei problematisch, dass die Bestimmungen der DSVGO an vielen Stellen mit sogenannten auslegungsbedürftigen Rechtsbegriffen (z.B. „berechtigtes Interesse“) arbeiten, die wenig Rechtssicherheit bieten, zumal bis heute so gut wie keine klärenden Gerichtsentscheidungen vorliegen.

Durch die europäische Neuregelung deutlich verschärft wurde der Sanktionsrahmen. Bislang ist lediglich ein Fall bekanntgeworden. So hat die portugiesische Daten-

2 So auch aktuell bestätigt durch OLG Köln, Urteil vom 18.6.2018, Az. 15 W 27/18.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

schutzbehörde CNPD (Comissão Nacional de Protecção de Dados) ein Krankenhaus in Barreiro zu einer Geldstrafe von Euro 400.000 verurteilt[3].

Maßgeblicher Grund hierfür waren Patientendaten, welche nicht genügend vor Einsichten von außen geschützt wurden. So hätten u.a. Techniker auf sensible, personenbezogene Daten zugreifen können, welche im Regelfall eigentlich nur von behandelnden Ärzten eingesehen werden dürfen.

Das Regelwerk dient dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz sowie dem freien personenbezogenen Datenverkehr. Diese Ziele sollen insbesondere durch die Einhaltung der in Art. 5 DSGVO festgeschriebenen Grundsätze der Verarbeitung der Daten erreicht werden, als da sind: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht. Diese Grundsätze hat jeder einzuhalten, der ganz oder teilweise personenbezogene Daten automatisiert verarbeitet, wobei unter Verarbeitung auch Smartphones, Tablets, Druck- und Kopiersysteme zu rechnen sind, oder bei nicht automatisierter Verarbeitung solche Daten in einem Dateisystem speichert oder zu speichern beabsichtigt. Damit sind beispielsweise handschriftliche Aufzeichnungen personenbezogener Daten ebenfalls betroffen wie elektronische Aufzeichnungen.

2 *Sachverständige und Verfahrensbeistände als Verantwortliche*

Die Verordnung regelt die *Verantwortlichkeit* für die Einhaltung des Datenschutzes zweifach.

Nach Art. 4 Nr. 7; 24 DSGVO ist jede „natürliche oder juristische Person, Behörde, Einrichtung oder anderer Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet" grundsätzlich verantwortlich. Damit sind alle Personen, die bei Untersuchung und Vertretung beteiligt sind, als verantwortlich anzusehen, mithin auch Sachverständige und Verfahrensbeistände bei Erfüllung ihrer Aufgaben. Beide haben unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen sowie den Nachweis dafür erbringen zu können, dass die Datenverarbeitung gemäß dieser Verordnung erfolgt (Art. 24 Abs. 1 DSGVO).

Verantwortlicher ist auch der sog. *Auftragsverarbeiter* (Art. 4 Nr. 8 DSGVO), also „diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".

3 Erste DSGVO-Sanktion: Krankenhaus in Portugal soll Strafe zahlen auf datenschutz.org unter https://www.datenschutz.org/erste-dsgvo-sanktion-krankenhaus-in-portugal-soll-strafe-zahlen/ (Zugriff am 23.1.2019).

https://doi.org/10.5771/2365-1083-2019-1-8 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

Da die *Beweislast* stets beim Verantwortlichen liegt, empfiehlt sich ein möglichst vollständiges und gut geplantes Datenschutzkonzept sowie eine akribisch geführte Dokumentation. Letztere ist ohnehin mit Einführung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO, nach der der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen können muss, kodifiziert.

3 Allgemeine Grundsätze der Behandlung personenbezogener Daten

3.1 Grundsätze für die Verarbeitung der Daten

Unter „personenbezogenen Daten" sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Abs. 1 DSGVO).

Die bisherigen Grundprinzipien des Datenschutzes bleiben erhalten und werden im Gesetz besonders betont. Man muss sich diese Prinzipien als die tragenden Grundlagen des Gesetzes vorstellen, die bei der Auslegung unklarer Fälle herangezogen werden. Dazu gehören entsprechend Art. 5 DSGVO vor allem die sechs Grundsäulen der/des

- **Rechtmäßigkeit** – Daten dürfen nur entsprechend dem Gesetz verarbeitet werden, was an sich selbstverständlich ist.
- **Transparenz** – Die Verarbeitung personenbezogener Daten muss für Betroffene nachvollziehbar sein, was zum Beispiel eine verständliche und vollständige Datenschutzerklärung erfordert. Die Informationspflichten wurden mit Art. 13 und 14 DSGVO erweitert und erfordern beispielsweise einen Hinweis auf die Rechtsgrundlage der Verarbeitung.
- **Verbots mit Erlaubnisvorbehalt** – Das bedeutet, dass jede Verarbeitung personenbezogener Daten verboten ist, außer wenn sie per Gesetz erlaubt ist.
- **Zweckbindung** – Das Gebot der Zweckbindung soll sicherstellen, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben worden sind. Das heißt, man muss sich bereits zu Beginn von Verarbeitungsprozessen Gedanken machen, wofür die Daten benötigt werden und dies dokumentieren. Eine nachträgliche Zweckänderung ist nur zulässig, wenn sie „mit dem ursprünglichen Zweck vereinbar ist" (Art 6 Abs. 4 DSGVO).
- **Datenminimierung** – Der Verantwortliche muss die Verarbeitung von personenbezogenen Daten auf das für den Verarbeitungszweck notwendige Maß beschränken; d.h. eine „Datenerhebung auf Vorrat" ist verboten (Art. 5 Abs. 1 lit. c DSGVO).

https://doi.org/10.5771/2365-1083-2019-1-8 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

- **Integrität und Vertraulichkeit** – Daten müssen durch technische und organisatorische Maßnahmen vor unbefugter Verarbeitung, Zerstörung, Veränderung oder Verlust geschützt werden.

Der Verantwortliche ist gemäß Art. 5 Abs. 2 DSGVO für die Einhaltung der obigen Vorgaben verantwortlich und muss deren Einhaltung nachweisen können („**Rechenschaftspflicht**").

3.2 Grundsätze zur Rechtmäßigkeit der Verarbeitung

Die Datenverarbeitung selbst ist nach Art. 6 DSVGO nur dann rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre *Einwilligung* zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben. Dies dürfte der häufigste Fall sein. Eine Einwilligung muss von einer einwilligungsfähigen Person, freiwillig für den konkreten Fall und in informierter Weise unmissverständlich in Form einer Erklärung oder einer sonstigen eindeutigen Handlung abgegeben sein. Ist die Person einwilligungsfähig, dann muss sie eine echte Wahl haben, was das „Ob" und das „Wie" der Einwilligung angeht. Nur dann ist die Einwilligung freiwillig. Das heißt, die Person darf sich nicht gezwungen fühlen, eine Einwilligung abgeben zu müssen. Der Betroffene muss immer verständlich darüber informiert werden, zu welchem Zweck seine Daten verarbeitet werden, auf welche Art, in welchem Umfang, ob die Daten an Dritte weitergegeben und wann sie gelöscht werden. Im Regelfall ist es ausreichend, wenn diese Hinweise in der Datenschutzerklärung platziert werden.
  Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates sollte eine vom Sachverständigen bzw. vom Verfahrensbeistand vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Die Einwilligung ist allerdings kein Allheilmittel. Zum einen sind die Anforderungen an deren Wirksamkeit sehr hoch. Zum anderen kann eine Einwilligung jederzeit widerrufen werden. Aus diesem Grund sollte zuerst immer geprüft werden, ob nicht die übrigen nachfolgend aufgeführten Rechtmäßigkeitsalternativen greifen:

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

- die Verarbeitung ist für die *Erfüllung eines Vertrags*, dessen Vertragspartei die betroffene Person ist, oder zur *Durchführung vorvertraglicher Maßnahmen erforderlich*, die auf Anfrage der betroffenen Person erfolgen. Hierbei greift insbesondere die Vertretung durch einen Verfahrensbeistand oder die Anfertigung eine Privatgutachtens.
- die Verarbeitung ist zur Erfüllung einer *rechtlichen Verpflichtung erforderlich*, der der Verantwortliche unterliegt.
- die Verarbeitung ist erforderlich, um *lebenswichtige Interessen* der betroffenen Person oder einer anderen natürlichen Person *zu schützen*. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Einige Arten der Verarbeitung können sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen; so kann beispielsweise die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich sein.
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die *im öffentlichen Interesse* liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Unter diese Alternative fällt die gerichtliche Bestellung eines Sachverständigen durch das Gericht oder eine andere öffentliche Stelle.
- die Verarbeitung ist zur Wahrung der *berechtigten Interessen* des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

3.3 Untersagungsgrundsatz bei der Verarbeitung von Daten „besonderer Kategorie"

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist nach Art. 9 Abs. 1 DSGVO untersagt. Die Verordnung spricht hier von der Verarbeitung „besonderer Kategorien". Ausgenommen von diesem Verbot ist der Ausnahmekatalog in Abs. 2 a) bis j). So ist beispielsweise die Verarbeitung personenbezogener Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erlaubt (Art. 9 Abs. 2 f) DSGVO), bei Einwilligung des Betroffenen ohnehin (Art. 9 Abs. 2 a) DSGVO).

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

3.4 Informationspflichten bei Erhebung der Daten

Die Rechte des Betroffenen sind eingehend in den Art. 12-23 DSGVO geregelt. Die wichtigsten Normen sollen nachfolgend kurz skizziert werden. Nach Art. 12 DSGVO hat jeder Betroffene das Recht auf transparente Information und Kommunikation. Zudem sind in der Norm Modalitäten für die Ausübung der Rechte der betroffenen Personen geregelt. Hierzu gehört beispielsweise, dass der Verantwortliche dem Betroffenen Informationen über ergriffene Maßnahmen zur Verfügung stellt, wenn dieser einen Antrag hierauf stellt (Art. 12 Abs. 3 DSGVO). Dies soll unverzüglich geschehen, jedenfalls aber innerhalb eines Monats nach Antragstellung.

Sofern ein Sachverständiger oder Verfahrensbeteiligter Daten bei der betreffenden Person erhebt, hat er der betroffenen Person zum Zeitpunkt der Erhebung der Daten gemäß Art. 13 DSGVO folgende Informationen mitzuteilen:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- sofern vorhanden, die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogene Daten verarbeitet werden sollen, sowie Rechtsgrundlage für die Verarbeitung;
- sofern die Bearbeitung auf Art. 6 Abs. 1 f DSGVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- gegebenenfalls den oder die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln.

Zusätzlich zu den vorstehenden Informationen sind der betroffenen Person zum Zeitpunkt der Datenerhebung weitere Informationen zur Verfügung zu stellen, die erforderlich sind, um eine faire und transparente Datenverarbeitung zu gewährleisten:

- die *Dauer*, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines *Auskunftsrechts* seitens des Betroffenen über die erhobenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines *Widerspruchsrechts* gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- sofern die Verarbeitung auf Art. 6 Abs. 1 a DSGVO oder Art. 9 Abs. 2 a DSGVO beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines *Beschwerderechts* bei einer Aufsichtsbehörde;
- ob die Bereitstellung personenbezogener Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogene Daten freizustellen, welche möglichen Folgen die Nichtbereitstellung hätte und

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profil gemäß Art. 22 Abs. 1 und Abs. 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Ist beabsichtigt, die Daten zu einem anderen Zweck weiter zu verarbeiten als den, für den die Daten erhoben wurden, so sind der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und aller anderen maßgeblichen Informationen zur Verfügung zu stellen.

3.5 Exkurs: Melde- und Informationspflichten bei Datenpannen

Für die früher in § 42a BDSG vorgeschriebene Melde- und Informationspflicht bei Datenpannen gelten zukünftig die Vorgaben des Art. 33 DSGVO. Danach müssen grundsätzlich alle Verletzungen des Schutzes personenbezogener Daten gemeldet werden, es sei denn, das Risiko einer Verletzung persönlicher Rechte und Freiheiten ist unwahrscheinlich. Die Meldung hat binnen 72 Stunden nach Bekanntwerden der Verletzung zu erfolgen. In Deutschland ist der Bundesbeauftragte für Datenschutz die zuständige Aufsichtsbehörde (§ 65 DSAnpUG-EU[4]). Zudem müssen die von einer Verletzung Betroffenen benachrichtigt werden (Art. 34 DSGVO und § 66 DSAnpUG-EU). Diese Benachrichtigungspflicht entfällt nur dann, wenn seitens der Verantwortlichen Vorkehrungen getroffen wurden, die Daten – etwa durch Verschlüsselung – Unbefugten unzugänglich zu machen, der Verantwortliche nachträglich Maßnahmen ergriffen hat, durch die das hohe Risiko für die Rechte und Freiheiten des Patienten aller Wahrscheinlichkeit nach nicht mehr besteht, oder die Vorkehrungen einen unverhältnismäßig hohen Aufwand erfordern würden. Dann allerdings hat eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen.

4 Auswirkungen der Grundsätze für Sachverständige und Verfahrensbeistände

Welche Auswirkungen haben nun die beschriebenen gesetzlichen Vorgaben für Gerichts- bzw. Privatsachverständige und Verfahrensbeistände?

Zunächst ist zwischen gerichtlich bestellten und aufgrund privater Vereinbarung tätigen Sachverständigen zu unterscheiden, wobei neben natürlichen Personen auch Behörden Sachverständige sein können, die bestellt bzw. beauftragt werden. Als Beispiel seien Kammern (z.B. Landesärztekammer), Ämter (z.B. Gesundheitsamt) oder Institute (z.B. Institut für Rechtsmedizin) genannt. Der Gerichtsgutachter wird für den Einzelfall durch Gerichte ernannt, wobei es auf das jeweilige Verfahrensrecht, wie z.B.

4 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30.6.2017 (DSAnpUG-EU), BGBl. 2017 Teil I Nr. 44.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

§§ 404 ZPO, 280 FamFG, ankommt. Der Privatgutachter ist für private Auftraggeber aufgrund eines privatrechtlichen Vertrages tätig.

Beide haben die Aufgabe, unparteiisch, unabhängig und objektiv den vom jeweiligen Auftraggeber vorgegebenen Sachverhalt fachlich zu beurteilen oder zu bewerten. Sachverständige müssen also in ihrer Aussage glaubhaft und in ihrer Person vertrauenswürdig sein, so dass ihre Feststellungen verkehrsfähig sind, wie eine Urkunde. Der Privatgutachter ist insoweit allerdings „Partei". Für ihn gelten die „Neutralitätsanforderungen", wie z.B. die Unparteilichkeit, nur eingeschränkt; die allgemeinen Vorgaben, wie Nachvollziehbarkeit oder das Begründungserfordernis des Ergebnisses, hingegen uneingeschränkt.

4.1 Auswirkungen auf den Privatsachverständigen

Bereits im Rahmen eines ersten Anbahnungsgespräches, bei dem noch keine Geschäftsbeziehung besteht, werden von dem Auftraggeber E-Mail-Anschrift, Name, Adresse und Telefonnummer angegeben. Bereits hier besteht die Transparenzpflicht, das heißt, dass der Sachverständige bei Übernahme dieser Daten in sein System die Pflichtangaben nach Art. 13 DSGVO zurückzusenden hat, bevor die Beauftragung durchgeführt wird. Sofern kein Vertrag zustande kommt, ist mit den mitgeteilten Daten entsprechend umzugehen. Zu beachten ist, dass auch ein Notizbuch eine geordnete Datenverarbeitung darstellt und hierfür die gleichen Regeln wie für die EDV gelten; nur Aufzeichnungen, die „ungeordnet" sind, also der klassische Schmierzettel, fallen nicht darunter, sofern sie nicht abgeheftet und damit archiviert werden sollen.

Bei Verwendung von Cloud-Anwendungen (Apple iCloud, Dropbox, Google Drive, Windows OneDrive, etc.) zur Speicherung der Kontaktdaten empfiehlt es sich, die Daten verschlüsselt zu übertragen oder geeignete Garantien (beispielsweise EU-Standardvertragsklauseln / Privacy Shield) für die Sicherheit beizubringen und Auftragsbearbeitungsverträge abzuschließen.

Für die Speicherung personenbezogener Daten auf dem Mobiltelefon ist als Mindestschutz ein Pin-Code Pflicht, besser noch ein verschlüsselter Speicher in Verbindung mit einem Virenschutz. Auch sollte hier auf die Übermittlung an einen Cloud-Dienstleister verzichtet werden, es sei denn es sind mit diesem entsprechende vertragliche Regelungen getroffen.

Kontaktformulare auf der eigenen Homepage werden immer beliebter. Hierbei sollten nur objektiv erforderliche und relevante Daten als Eintragefelder abgefragt werden. Das Kontaktformular sollte einen Hinweis auf die Datenschutzerklärung enthalten, die leicht mittels Mausklick aufgerufen werden kann. Besser noch wäre die Möglichkeit, einen Haken auf die Datenschutzerklärung mit Anzeigemöglichkeit zu setzen, da dann die Kenntnisnahme bestätigt ist.

Ansonsten bedarf es keiner weiteren Maßnahmen seitens des Sachverständigen mit Ausnahme der sicheren Übermittlung des Gutachtens an den Betroffenen. Als sicher gilt die Übermittlung postalisch im Umschlag, wobei es keines Einschreibens bedarf.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

Sofern das Gutachten per E-Mail versandt wird, ist die Mindestanforderung Server2-Server TLS Verschlüsselung, gegebenenfalls sogar mit PFS oder ganz sicher mit Ende2 Ende mittels pgp, S/MIME.

In der Regel werden Gutachten für einen bestimmten Zweck erstellt, so dass auch Dritte Einblick in das Gutachten nehmen können oder sollen. Hier fragt sich, was als Sachverständiger zu beachten ist. Rein formal wird das Privatgutachten für einen Berechtigten, den Besteller, erstellt. Wenn dieser die Informationen weitergibt, obliegt dies nicht mehr dem Sachverständigen.

Beispielsweise im Rahmen eines *Gutachterauftrags für die öffentliche Hand*, die nicht durch hoheitliche Bestellung erfolgt, dürfte der Sachverständige Auftragsverarbeiter sein. Die Rechtsgrundlage seiner Beauftragung liegt in Art. 28 Abs. 3 Satz 1 DSGVO in Form eines wirksamen Auftragsverarbeitungsvertrages. Dessen Voraussetzungen sind:

Vertragliche Verpflichtung + Sicherheitskonzept + Liste der Bearbeiter = Auftragsverarbeitungsvertrag.

In einem Auftragsverarbeitungsvertrag muss sich der Auftragnehmer dazu verpflichten, die Daten nur entsprechend dem Auftrag und nach Weisung zu verarbeiten. Dazu gehört noch eine Anzahl weiterer Pflichten, zu denen unter anderem die Verpflichtung der Mitarbeiter auf Vertraulichkeit, Mitwirkung, Kontrollrechte und technisch-organisatorische Maßnahmen zum Schutz der Daten gehören.

Es würde den Rahmen sprengen, alle Punkte eines Auftragsverarbeitungsvertrages zu erläutern, die nachstehende vereinfachte Checkliste sollte aber Transparenz bieten.

Checkliste: Notwendige Inhalte eines Auftragsverarbeitungsvertrages

- Angaben zum Auftraggeber und Auftragnehmer,
- Kategorien der verarbeiteten Daten (z.B. E-Mailadressen, Namen, Anschriften),
- Zweck der Verarbeitung,
- Vertragliche Verpflichtungen auf Befolgung von Weisungen, Genehmigung von Kontrollen, Beauftragung von Mitarbeitern nur mit Zustimmung, Mitwirkung- und Information,
- Technisch-organisatorische Schutzmaßnahmen und sonstige Garantien und
- Liste der fachlichen Mitarbeiter.

4.2 Auswirkungen auf den Gerichtssachverständigen

Der Gerichtssachverständige wird für den Einzelfall durch das Gericht ernannt und steht nur zu diesem in einem Rechtsverhältnis. Da das Gericht über die Zwecke und Mittel der Verarbeitung von Personendaten entscheidet, dürfte in dem gerichtlich be-

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

stellten Sachverständigen im Verhältnis zur Justizbehörde ein Auftragsverarbeiter zu sehen sein, der im Auftrag des verantwortlichen Gerichts die Daten verarbeitet.[5]

Für den Gerichtssachverständigen gelten dieselben Anforderungen, wie für den Privatsachverständigen, was die Erhebung und Bearbeitung sowie die Verwaltung der Daten betrifft. Ebenso wie dieser überlässt er mit Fertigstellung seines Gutachtens die persönlichen Daten der Betroffenen seinem „Auftraggeber", mithin dem Gericht. Mit Übergabe des Gutachtens ist es Sache des Gerichts, die Daten DSGVO-konform zu behandeln und zu verwalten.

Wie sieht es aber nun mit der Weitergabe der vom Gerichtssachverständigen erhobenen und verwalteten Daten an das Gericht aus? Hier sieht die Verordnung einen Auftragsverarbeitungsvertrag als Erlaubnisgrund für eine Datenweitergabe vor, getreulich dem Satz „Wer für den Schutz der Daten vertraglich sorgt, der darf sie weitergeben". Für solche Fälle der „Auftragsverarbeitung" sieht das Gesetz den Abschluss und die Erfüllung eines speziellen Vertrags als hinreichende Risikominderung für die Betroffenen und damit als Erlaubnisgrundlage vor (Art. 28 Abs. 3 Satz 1DSGVO). Das bedeutet, die berechtigten Interessen an der Weitergabe von Daten überwiegen dann die Datenschutzinteressen betroffener Personen und die Weitergabe ist erlaubt.

Da der Gerichtssachverständige für das Gericht nicht „per Vertrag" tätig wird, sondern kraft hoheitlicher Bestellung, ersetzt diese die vertragliche Grundlage des Art. 28 Abs. 3 Satz 1 DSGVO.

Da die meisten Gerichtsverfahren öffentlich sind, und neben den materiellen Sachverhalten sicherlich hin und wieder auch persönliche Daten in einer mündlichen Verhandlung zur Sprache kommen, ist es allein Sache des Gerichts dafür Sorge zu tragen, wie die im Gutachten niedergelegten persönlichen Daten im Rahmen einer mündlichen Verhandlung behandelt werden.

4.3 Auswirkungen auf das Gutachten

Die wesentliche Tätigkeit eines jeden Sachverständigen liegt in der Sammlung von Informationen zu einem Sachverhalt, der Bewertung der gesammelten Informationen und der Erstellung eines Gutachtens. An das Ergebnis der sachverständigen Arbeit sind bestimmte Ansprüche zu stellen.[6] Die Arbeit muss klar definiert sein und das Gutachten muss inhaltlich und formal bestimmte Eigenschaften aufweisen. Zwar gibt es derzeit keine gesetzliche Regelung für die Erstellung von Gutachten, dennoch haben sich in der Rechtsprechung Grundsätze dazu entwickelt. Gutachten müssen auf jeden

5 Gerichte sind nicht „Empfänger" im Sinne der Verordnung. „Empfänger" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten gemäß Art. 4 Abs. 9 DSGVO nicht als Empfänger.

6 Hierzu im Einzelnen: Heinz, Die Haftung des medizinischen Sachverständigen, GesR 2015, 398.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

Fall nachvollziehbar sein. Sie müssen die Begründung für die Schlussfolgerungen des Sachverständigen enthalten. Häufig fehlen diese Inhalte in Gutachten und dadurch sind diese unbrauchbar. So ist ein Gutachten beispielsweise mangelhaft, wenn es in nicht nachvollziehbarer Weise nur das Ergebnis mitteilt.[7]

Im Rahmen der Gutachtenerstellung ist zu berücksichtigen, wie personenbezogene Daten anderer Personen als der Verfahrensbeteiligten nach den Bestimmungen der DSGVO zu behandeln sind. Zu denken ist beispielsweise an die Nennung von Personen, die dem Gutachter (telefonisch) eine Auskunft erteilt haben (beispielsweise Sozialamt, Wohnungsamt, Schulbehörde). Auch deren persönliche Daten unterfallen dem Schutz der Verordnung, denn die DSGVO unterscheidet nicht hinsichtlich der Verwendung der Daten.

Aus diesem Grund empfiehlt sich auf die namentliche Benennung von Personen, bei denen Einkünfte eingeholt wurden, zu verzichten. Andernfalls müsste bei diesen eine Einwilligung eingeholt oder eine Interessenabwägung durchgeführt und diese Personen dann auch nach Art. 13 DSGVO informiert werden. Praktikabel ist es nur, auf die Behörde oder die entsprechende Abteilung zu verweisen und dies im Gutachten so formuliert aufzunehmen.

Allerdings steht noch die Frage im Raum, wie in Gutachten, die den Gerichten vorgelegt werden, die aufgenommenen persönlichen Daten zu behandeln sind. Hierzu wird die Auffassung vertreten, dass dieser Punkt vernachlässigbar sei, da nur die Parteien des Rechtsstreits die Daten sehen würden und diese nicht veröffentlicht würden.[8] Dem ist aber nicht so, soweit die Verhandlungen öffentlich sind. Aufgrund von Zitaten aus dem Gutachten könnten etwaige persönliche Daten die Öffentlichkeit in Form der Zuhörerschaft im Gerichtssaal erreichen. Eine ähnliche Problematik besteht im Rahmen der ärztlichen Schweigepflicht. Diesbezüglich ist allgemein anerkannt, dass die Schweigepflicht durchbrochen werden kann in Rechtsstreitigkeiten für und gegen einen Arzt oder eine Klinik, sei es zur Verfolgung oder Abwehr von Rechtsansprüchen. Letztendlich dürfte diese Frage aber in der Verantwortung der Gerichte liegen.

4.4 Auswirkungen auf den Verfahrensbeistand

Im Rechtsverhältnis des Betroffenen zum Verfahrensbeistand gelten im Wesentlichen dieselben Anforderungen wie für Sachverständige. Deren Gutachten sind ihre Handakten, die es ebenso sicher zu behandeln gilt.

7 OLG Düsseldorf, Beschluss vom 21.8.1995, Az. 10 W 66/95.

8 Drissler, EU-Datenschutzgrundverordnung – Was gilt es für Sachverständige in der Immobilienbewertung zu beachten? Unter https://www.edcud.de/dyngfx/news_325_1521643182.pdf (Zugang am 23.1.2019).

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

5 Auswirkungen auf den alltäglichen Büroablauf

Die nachfolgenden Ausführungen gelten für Sachverständige ebenso wie für Beistände, insbesondere aber auch für deren Mitarbeiter. Für die Datenerhebung, Bearbeitung, Sicherung und Verwahrung gibt Art. 32 DSGVO Vorgaben, was die Sicherheit anbetrifft.

5.1 Erhebung, Bearbeitung und Verwaltung der Daten

Der verantwortliche Sachverständige bzw. Verfahrensbeistand, aber auch dessen Mitarbeiter sind nach Art. 32 DSGVO gehalten, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen – und dies gilt insbesondere im Rahmen der Bearbeitung per EDV – schließen unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein. Die Beteiligten sind so auszuwählen, dass die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit für die Verarbeitung auf Dauer sichergestellt sind. Zudem müssen die Daten bei einem technischen Störfall rasch wiederhergestellt werden können. Unbefugten Zugang zu den Daten oder Datenverlust ist mit geeigneten Mittel vorab zu begegnen, was hausintern ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung bedingt. Schließlich haben die Verantwortlichen geeignete Schritte zu unternehmen, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

So dürfen die Daten auf dem Bürorechner und sämtlichen anderen Datenträgern sowie Ausdrucken keinen unbefugten Dritten zugänglich sein. Das bedeutet, dass Praxismitarbeiter im Empfangsbereich und im Behandlungs- bzw. Besprechungszimmer dafür Sorge tragen, dass kein unbefugter Dritter auf Daten von Betroffenen zugreifen kann oder Dritte Kenntnis von deren Daten erhalten, indem sie beispielsweise Einblick auf den Monitor am Empfang oder am Schreibtisch oder in Karteikarten haben. Behandlungs- oder Handakten sind daher immer vor dem Zugriff oder Blicken Dritter zu schützen. Jeder Computer ist mit einem Passwort zu versehen, das nur dem jeweiligen Benutzer bekannt sein darf. Sobald der Arbeitsplatz verlassen wird, ist der Computer zu sperren – d. h. den Kennwortschutz zu aktivieren. Dies gilt auch für kurze Abwesenheitszeiten. Datenträger oder Ausdrucke mit personenbezogenen Daten dürfen nicht offen am Arbeitsplatz oder im Drucker liegen, wenn Unbefugte darin Einsicht nehmen können.

Externe Datenträger wie CDs, DVDs oder USB-Sticks dürfen nicht an einen der Bürorechner angeschlossen werden. Eine Ausnahme gilt dann, wenn dies ausdrücklich angeordnet ist und dienstlichen Zwecken dient.

Der Internetanschluss des Büros sowie das E-Mail-System sind ausschließlich für den dienstlichen Gebrauch zu nutzen; eine private Nutzung ist nicht zulässig. Zugangsdaten dürfen nicht an Dritte weitergegeben werden. Installation von Software oder das

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

Herunterladen von Daten aus dem Internet ist untersagt. Fremde Programme dürfen nicht installiert oder auf die Festplatte kopiert werden.
Zum Virenschutz und dem Schutz vor Angriffen von außen müssen Firewall und Virenschutzprogramme aktiviert sein und genutzt werden. Besteht der Verdacht auf einen unbefugten Zugriff von außen oder den Befall mit Viren, so haben Mitarbeiter unverzüglich den zuständigen Vorgesetzten zu informieren. Raubkopien dürfen keinesfalls verwendet werden. Vorhandene Software und die dazugehörigen Handbücher dürfen nicht kopiert und auf anderen Rechnern eingesetzt werden.
Daten dürfen nicht an andere Stellen gefaxt oder gemailt werden, wenn der Betroffenen dazu nicht seine Einwilligung gegeben hat oder gesichert ist, dass die Daten wirklich nur von dem Adressaten gelesen werden können.

5.2 Auswirkungen auf die elektronische Dokumentation mittels EDV

Im Rahmen der elektronischen Dokumentation mittels EDV ist zwischen der Datenverwaltung zu eigenen Dokumentationszwecken und externen Dokumenten zu unterscheiden.

5.2.1 Daten für eigene Dokumentation

Die Datensicherheit fordert, dass Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien besonderer Sicherungs- und Schutzmaßnahmen bedürfen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Um eine beweissichere elektronische Dokumentation zu gewährleisten, muss das Dokument mit einer qualifizierten elektronischen Signatur des Verantwortlichen versehen werden, wenn dieser auf eine herkömmliche schriftliche Dokumentation verzichten will. Auf diese elektronischen Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden nach § 371a Abs. 1 ZPO in der Fassung des *Gesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz (*JustizkommunikationsG)[9] die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Die Beweiskraft für elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, ist mit schriftlichen Dokumenten vergleichbar, allerdings mit der Folge, dass ein solches Dokument nicht mehr inhaltlich verändert werden kann, ohne dessen Signatur zu zerstören. Aus diesem Grund müssen Ergänzungen sowie Berichtigungen stets in einem gesonderten Dokument festgehalten und dieses mit dem Ursprungsdokument untrennbar verbunden werden. Technisch ist das durch eine sogenannte „elektronische Klammer“ möglich.

9 JKomG – Bundesgesetzblatt 2005, Teil I Nr. 18, S. 837.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

5.2.2 Daten für externe Dokumentation

Externe Dokumente, wie z.B. Dokumente von Kollegen, lassen sich, sofern sie mit einer qualifizierten elektronischen Signatur versehen sind, in die eigene Dokumentation übertragen. Werden die Dokumente in Schriftform übermittelt, werden sie regelmäßig „eingescannt". Der Nachweis, dass das elektronische Dokument dem schriftlichen Original entspricht, kann in der Regel nur durch den Vergleich beider Dokumente erbracht werden. Eine solche Handhabung liefe aber dem Sinn und Zweck der elektronischen Dokumentation zuwider, da auch das Originaldokument aufbewahrt werden müsste. Die Lösung kann darin bestehen, dass das elektronische Dokument mit einem Vermerk versehen wird, wann und durch wen das Originaldokument in eine elektronische Form übertragen worden ist. Zudem muss dokumentiert werden, dass die Wiedergabe auf dem Bildschirm und damit auch in der elektronischen Datei mit dem Originaldokument inhaltlich und bildlich übereinstimmen. Um zu vermeiden, dass das schriftliche Original nicht vollständig erfasst wird, sollten beide Seiten eingescannt werden, auch wenn die Rückseite inhaltlich leer sein sollte. Alternativ ließe sich in dem Vermerk auch ein Hinweis aufnehmen, dass nach der Umwandlung des Dokuments eine Überprüfung auf Vollständigkeit erfolgt ist.

Aber auch durch diese Maßnahme kann der Beweiswert des schriftlichen Originaldokuments nicht ersetzt werden. Die Umwandlung in eine elektronische Form und die Vernichtung des Originaldokuments sind nur zu empfehlen, wenn das Dokument bei einer anderen Stelle, wie z. B. bei dem Verfasser des Arztbriefes, noch zu einem Vergleich zur Verfügung steht. Die Aufbewahrung des Originals ist darüber hinaus in besonders schadensträchtigen Fällen zu empfehlen; es sollte angesichts der Beweissituation stets sorgfältig abgewogen werden, ob das Originaldokument vernichtet werden kann.

Zu beachten ist, dass beim Einscannen von Dokumenten die Dokumente wirklich vollständig sind und das elektronische Dokument dem Original entspricht. Beim Einscannen werden folgende Angaben vermerkt: Wann das Dokument eingescannt wurde und wer das Dokument eingescannt hat. Des Weiteren die Bestätigung der bildlichen und inhaltlichen Übereinstimmung der Wiedergabe auf dem Bildschirm mit dem Originaldokument und der Vermerk über die Überprüfung auf Vollständigkeit.

5.3 Auswirkungen auf den eigenen Internetauftritt

Der Büro- bzw. Kanzlei-Homepage kommt werblich eine besondere Bedeutung zu. So wurden Bedenken laut, die DSGVO erlaube keine personenbezogenen Bilder mehr auf der hauseigenen Homepage. Mit diesen Bedenken hat sich jüngst das OLG Köln[10] auseinandergesetzt und festgestellt, das Art. 85 DSGVO den nationalen Gesetzgebern einen Gestaltungsspielraum lässt, denn für die Bundesrepublik besteht ein Spannungs-

10 OLG Köln, Urteil vom 18.6.2018, Az. 15 W 27/18.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

verhältnis zwischen der DSGVO und dem Kunsturhebergesetz (KUG)[11]. Danach ist eine Veröffentlichung von Aufnahmen von Personen ohne deren Einwilligung u.a. auf einer Internetseite grundsätzlich unzulässig (§§ 22, 23 KUG). Der Kölner Senat gelangt zu dem Ergebnis, dass das KUG auch nach Wirksamwerden der DSGVO die Handlungsrichtlinien vorgibt. Die Entscheidung betrifft allerdings nur den begrenzten Bereich der Veröffentlichung von Fotos zur journalistischen Berichterstattung. Nicht erfasst von dem Urteil ist zudem der dem Ins-Netz-Stellen vorangehende Schritt: Das Anfertigen von Fotos, das ebenfalls als Verarbeitung von Daten im Sinne der DSGVO anzusehen ist. Auch über das Onlinestellen zu nicht-journalistischen Zwecken durch Künstler, Unternehmen, Blogger oder Privatpersonen hat das Gericht keine Aussage getroffen. So schafft das Urteil nur ein bisschen Klarheit. Um Rechtssicherheit müssen fürderhin die Gerichte bemüht sein.

Ein weiterer Problemfall: Ist eine fehlende Datenschutzerklärung auf einer Homepage nun wettbewerbswidrig? Nach unterschiedlichen Urteilen zweier Landgerichte gibt es nun ein obergerichtliches Urteil zu dem Thema. Nach einer Entscheidung des LG Würzburg[12] sind Abmahnungen wegen fehlender Datenschutzerklärungen auf einer Homepage zulässig. Das LG Bochum[13] hat genau das Gegenteil entschieden. Die Gerichte haben mit diesen Entscheidungen juristisches Neuland nach Inkrafttreten der DSGVO betreten. Nun gibt es ein Urteil des OLG Hamburg[14], das allerdings nicht die gewünschte Klärung bringt. Das OLG nimmt eine vermittelnde Position ein: Die jeweilige Vorschrift der DSGVO muss daraufhin untersucht werden, ob sie auch ein wettbewerblich relevantes Marktverhalten betrifft. Ist dies der Fall, können Mitbewerber sich auf das Gesetz gegen den unlauteren Wettbewerb (UWG) stützen und Verstöße abmahnen. Der Senat hat im konkreten Fall die datenschutzrechtswidrige Nutzung von personenbezogenen Daten zu Webzwecken als abmahnfähigen Verstoß anerkannt. Diese Rechtsauffassung hat zur Folge, dass nun jede DSGVO-Norm auf ihre Marktrelevanz hin überprüft werden müsste, ggf. durch mehrere Gerichtsinstanzen. Es bleibt abzuwarten, ob andere Gerichte sich dieser Rechtsansicht anschließen oder ob es zu einer gesetzgeberischen Klarstellung kommt.

6 Auswirkungen auf die Datenweitergabe an Dritte

Die Weitergabe von Unterlagen an Dritte bedarf der Zustimmung des Betroffenen in „eindeutiger und unmissverständlicher Weise". Wie dürfen nun die Daten in der Alltagsarbeit – insbesondere „außer Haus" – ohne Verletzung der datenschutzrechtlichen Bestimmungen verwendet werden? Auf jeden Fall muss ein Einblick Dritter in die Unterlagen bei Datenübertragung durch den Verantwortlichen bzw. seine Mitarbeiter ver-

11 Gesetz vom 09.01.07 (RGBl. I 07,7) mit Wirkung vom 01.01.66 aufgehoben, soweit das Gesetz nicht den Schutz von Bildnissen betrifft zuletzt geändert durch Art. 3 § 31 des Gesetzes vom 16.02.01 (BGBl. I 01,266).
12 LG Würzburg, Beschluss vom 13.9.2018, Az. 11 O 1741/18 UWG.
13 LG Bochum, Beschluss vom 7.8.2018, Az. I-12 O 85/18.
14 OLG Hamburg, Urteil vom 25.10.2018, Az. 3 U 66/17.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

hindert werden. Jemand, der Daten nicht ausreichend gesichert über die öffentlichen Netze versendet, nimmt eine Kenntnisnahme Dritter billigend in Kauf. Eine Datenweitergabe per Fax sollte nur in Routinefällen oder in absoluten Notfällen vorgenommen werden, wenn die Gefahr besteht, dass unbeteiligte Dritte von dem Inhalt Kenntnis erhalten.

Wenn beispielsweise eigene Rechnungen in der Cloud eines Software-Anbieters bearbeitet werden – und sei es nur zur eigenen Datensicherung –, kommt es zur Weitergabe von Daten an Dritte. Oder die hauseigene IT wird durch externe Techniker ferngewartet. Doch wie hält man dabei die DSGVO ein? Bei all diesen Fällen der Weiterleitung, des Empfangs oder der bloßen Möglichkeit der Kenntnisnahme von personenbezogenen Daten durch Dritte (kurz „Weitergabe"), handelt es sich um erlaubnispflichtige Verarbeitungen.

Die *Einwilligung* zur Weitergabe von Daten sollte nur eine Lösung sein. Zum einen können die betroffenen Personen in die Weitergabe ihrer Daten einwilligen (Art. 6 Abs. 1 lit. a DSGVO). Doch an Einwilligungen werden hohe Anforderungen gestellt und zudem können sie schnell widerrufen werden. Wann immer möglich, sollte die Datenweitergabe (auch wenn nur zusätzlich) auch auf eine gesetzliche Erlaubnisnorm gestützt werden. So ist die zur Vertragserfüllung erforderliche Weitergabe von Daten zulässig. Die Weitergabe kann *zur Vertragserfüllung* erforderlich, den Interessen der Betroffenen entsprechend und damit gesetzlich erlaubt sein (Art. 6 Abs. 1 lit. b DSGVO). Das ist beispielsweise der Fall, wenn ein E-Shop-Betreiber Daten der Kunden an eine Bank und einen Paketzusteller zwecks Bezahlung und Zustellung weitergibt. Die Weitergabe von Daten, kann auch ohne Einwilligung und Vertrag zulässig sein, wenn *berechtigte Interessen* an der Weitergabe bestehen. Zu den berechtigten Interessen nach Art. 6 Abs. 1 lit. f DSGVO gehören z.B. Interessen an der Gewinnmaximierung, Kostensenkung, Optimierung der Dienste und Steigerung der Usability. Wenn die Interessen der Nutzer am Schutz ihrer Daten nicht überwiegen, ist in solchen Fällen die Weitergabe erlaubt. Bei dieser Interessensabwägung kommt es zum einen auf die Art der Daten, den Zweck der Datenweitergabe und mögliche Risiken für die Betroffenen an. So wird die Abwägung grundsätzlich negativ ausfallen, wenn beispielsweise ein E-Shop Kundendaten an Adresshändler verkauft. Hier wird im Regelfall eine Einwilligung der Nutzer notwendig sein. Dagegen sind die Rechte der Nutzer berufsrechtlich und strafrechtlich (§ 203 StGB) gesichert, wenn die Kundendaten an den Steuerberater des E-Shops weitergegeben werden. In den meisten Fällen liegt die Risikolage irgendwo zwischen diesen beiden Polen und kann mit speziellen Verträgen so gemindert werden, dass die Datenweitergabe erlaubt ist.

Das OLG München[15] hat in einem Teilurteil die Weitergabe von Kundendaten im Rahmen eines geltend gemachten Auskunftsanspruchs aus § 242 BGB für rechtmäßig erachtet. Hintergrund war ein bestehender Vertragshändlervertrag zwischen der Klägerin und der Beklagten, aus dem die Beklagte eine Vertragsverletzung im Rahmen einer Widerklage geltend machen wollte. Hierzu machte sie einen Anspruch auf Aus-

15 OLG München, Urteil vom 24.10.2018, Az. 3 U 1551/17.

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

kunft über abgewickelte Lieferungsverträge der Klägerin geltend, die möglicherweise die Vereinbarungen aus dem gemeinsamen Vertragshändlervertrag verletzten. Die Auskunft beinhaltete dementsprechend auch eine Weitergabe der Daten von Kunden der Klägerin. Ein solcher Auskunftsanspruch ist nach ständiger Rechtsprechung des BGH aus dem Grundsatz von Treu und Glauben (§ 242 BGB) gegeben, wenn sich der Anspruchsberechtigte im Unklaren über den Umfang seines Rechts befindet und der Verpflichtete unschwer dazu in der Lage ist, die Auskunft zu erteilen. Das OLG München sah den Auskunftsanspruch als gegeben an und verneinte hier ein Entgegenstehen der Vorschriften der DSGVO. Gestützt hat das Gericht den Anspruch auf Art. 6 Abs. 1 lit f) DSGVO. Die genannte Vorschrift verlangt bekanntlich ein sogenanntes „berechtigtes Interesse" des Verantwortlichen oder eines Dritten. Das OLG sah hier ein berechtigtes Interesse auf Seiten eines Dritten, nämlich der Beklagten bzw. Widerklägerin. Eine Datenverarbeitung kann immer dann auf die Rechtsgrundlage des Art. 6 Abs. 1 lit. f) DSGVO gestützt werden, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Bei der vorzunehmenden Abwägung zwischen den Interessen der Betroffenen und des Verantwortlichen bzw. des Dritten sieht das Gericht dann eine möglichst weite Auslegung des berechtigten Interesses als (unions-)grundrechtlich geboten an. Nicht nur rechtliche Interessen seien dabei zu berücksichtigen, sondern auch wirtschaftliche oder ideelle. Bei der Abwägung der Interessen trägt das Gericht der Tatsache Rechnung, dass auf Seiten der Betroffenen keine höchstpersönlichen Daten oder ein besonderes Know-how der betroffenen Branche weitergegeben wurden, sondern ausschließlich wirtschaftliche Daten über mehrere Kaufabwicklungen. Diese waren zudem im konkreten Fall noch nach außen überprüfbar. Da auf der anderen Seite das Interesse der Beklagten an einer Durchsetzung möglicher Schadensersatzansprüche stand, konnten nach Auffassung des Gerichts die Interessen der Betroffenen hier nicht überwiegen.

7 Die Rechte der Betroffenen

Nach Art. 15 DSGVO hat der Betroffene weitreichende Auskunftsrechte. Zunächst hat er das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob die ihn betreffenden personenbezogenen Daten verarbeitet werden. Ist dies der Fall, so hat er ein Recht auf Auskunft über diese Daten und auf nachfolgende Informationen:

- die Zwecke der Verarbeitung,
- die Kategorien der persönlichen Daten, die verarbeitet werden,
- den oder die Empfänger oder Kategorien von Empfängern, gegenüber denen die Daten offen gelegt wurden oder noch werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,
- sofern möglich, die geplante Dauer der Datenspeicherung, oder falls nicht möglich, die Kriterien für die Festlegung des Zeitraums,

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

- das Bestehen eines Rechts auf Berichtigung oder Löschung der personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchs gegen diese Verarbeitung,
- über die Existenz eines Beschwerderechts bei einer Aufsichtsbehörde, sowie
- alle verfügbaren Informationen über die Herkunft der Daten, wenn diese nicht bei der betroffenen Person erhoben werden.

Von besonderer Bedeutung sind die Rechte des Betroffenen in den Art. 16 (Berichtigung), Art. 17 (Löschung) und Art. 18 (Einschränkung der Verarbeitung) DSGVO. Auch diese Rechte sind sehr weitreichend. Die Berichtigung personenbezogener Daten kann durch den Berechtigten dann verlangt werden, wenn die Daten unrichtig sind. Das Recht auf Löschung besteht dann, wenn die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Ein Löschungsrecht besteht auch dann, wenn die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1a DSGVO oder Art. 9 Abs. 2a DSGVO stützt widerruft, und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt. Die Einschränkung der Verarbeitung kann dann verlangt werden, wenn die Richtigkeit der personenbezogenen Daten vom Patienten bestritten wird, und zwar für eine Dauer, die es den Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen. Dasselbe gilt, wenn die Verarbeitung unrechtmäßig ist und der Patient die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der Daten verlangt. Schließlich besteht noch ein Recht auf Einschränkung, wenn der Verantwortliche die Daten für die Zwecke der Verarbeitung nicht mehr, der Patient sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, und endlich der Betroffene Widerspruch gegen die Verarbeitung gemäß Art. 21 Abs. 1 DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen die des Betroffenen überwiegen.

Art. 21 DSGVO regelt sein Widerspruchsrecht. Danach kann er aus Gründen, die sich aus einer besonderen Situation ergeben, jederzeit gegen die Verarbeitung ihn betreffende personenbezogener Daten, die aufgrund von Art. 6 Abs. 1e oder f der DSGVO erhoben wurden, Widerspruch einlegen. Der Verantwortliche darf die personenbezogenen Daten dann nicht mehr verarbeiten, es sei denn er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen. Eine weitere Ausnahme ist dann gegeben, wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

8 Sanktionsmittel

Zur Durchsetzung der Einhaltung der geschilderten Bestimmungen sieht die Verordnung erhebliche Sanktionen vor, die ernst zu nehmen sind: So wurden die Bußgelder drastisch erhöht. Von den bisherigen Euro 50.000,00 auf künftig bis zu Euro 10 Millionen oder bis zu 2 % des Jahresumsatzes bzw. von den Euro 300.000,00 auf bis zu Euro

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.

20 Millionen oder bis zu 4 % des Jahresumsatzes. In welcher Höhe die Aufsichtsbehörden Bußgelder und Strafen bei Verstößen verhängen werden, bleibt allerdings abzuwarten. Eine mehr oder weniger unklare Vorgabe existiert jedoch bereits: Die Verhängung eines Sanktionsmittels muss gemäß Art. 83 DSGVO in jedem Einzelfall *wirksam*, *verhältnismäßig* und *abschreckend* sein. Diese drei Tatbestandsmerkmale, die ausschließlich mit auslegungsbedürftigen Rechtsbegriffen arbeiten, werden allerdings nicht viel Rechtssicherheit bringen, so dass es wohl geraume Zeit dauern wird, bis die Judikatur über Einzelfallentscheidungen hier Rechtssicherheit geschaffen hat. Bislang ist lediglich ein Fall bekanntgeworden.

Zudem haften zukünftig Verantwortliche – Geschäftsführer, Mitarbeiter und Datenschutzbeauftragte oder Auftragsverarbeiter – bei Datenschutzverstößen unter Umständen auch mit ihrem Privatvermögen. Auch Schadensersatzansprüche kann jede Person, der ein materieller oder immaterieller Schaden entstanden ist, nach Art. 82 Abs. 1 DSGVO direkt gegenüber dem Verantwortlichen geltend machen.

Literatur

Drissler, E (2018). EU-Datenschutzgrundverordnung – Was gilt es für Sachverständige in der Immobilienbewertung zu beachten? Immobilien & bewerten. Unter https://www.edcud.de/dyngfx/news_325_1521643182.pdf (Zugriff am 23.1.2019).

Drissler, E. (2018. Die neue Datenschutzgrundverordnung DSGVO. Präsentation auf dem Hessischen Immobilientag 16.5.2018 – IVD Mitte e.V. https://mitte.ivd.net/wp-content/uploads/sites/3/2018/05/Drissler-DSGVO.pdf (Zugriff am 23.1.2019).

Heinz, T. (2015). Die Haftung des medizinischen Sachverständigen. Zeitschrift für GesundheitsRecht 14(7), 398-402.

Kontakt:

Dr. Thomas K. Heinz
Rechtsanwalt, Fachanwalt für MedR
Rechtsanwälte MEKAT MITTELACHER WOLICKI
Zeilweg 42
D-60439 Frankfurt
web www.mmw-law.de
email dr.tkheinz@freenet.de

https://doi.org/10.5771/2365-1083-2019-1-6 - Generiert durch IP 216.73.217.60, am 03.05.2026, 04:37:46. © Urheberrechtlich geschützter Inhalt. Ohne gesonderte Erlaubnis ist jede urheberrechtliche Nutzung untersagt, insbesondere die Nutzung des Inhalts im Zusammenhang mit, für oder in KI-Systemen, KI-Modellen oder Generativen Sprachmodellen.