Datenschutz und HIV
Eine praktische Anleitung für die Beratungspraxis

Ausarbeitung im Auftrag der Deutschen Aidshilfe

Jasper Prigge

2019

Inhaltsverzeichnis

1. Einführung

Du hast HIV? Diese Frage wurde seit dem Auftreten des HI-Virus in den 1980er Jahren unzählige Male gestellt. In den vergangenen Jahrzehnten hat der Schutz personenbezogener Daten von Menschen mit HIV dazu beigetragen, dass sie autonomer in ihrer Entscheidung sind, wem sie ihre Erkrankung offenbaren. Datenschutz ist ein wichtiger Baustein, um Diskriminierung zu verhindern und ermöglicht Menschen mit HIV einen selbstbestimmten Umgang mit ihrer Infektion.

Auch wenn in den vergangenen Jahren das Bewusstsein für den Schutz personenbezogener Daten zugenommen hat, sind Datenschutzverletzungen für Menschen mit HIV dennoch alltäglich. Outings in sozialen Netzwerken, die Markierung von Akten im Krankenhaus oder Mitteilungen von Behörden an Angehörige kommen immer wieder vor.

In der Praxis stellt die Komplexität des Datenschutzrechts in derartigen Situationen eine Herausforderung für Berater_innen dar. Sie stehen vor der Aufgabe, sich im Dickicht der Vorschriften zurechtzufinden, den konkreten Fall zutreffend einzuschätzen und mit den Klient_innen den richtigen Weg einzuschlagen, um ihre Rechte effektiv zu wahren. Dabei wirft die zunehmende Digitalisierung von Krankenkassen, Arztpraxen und freien Trägern zusätzlich neue Fragen auf, deren Beantwortung vielfach noch unsicher ist. Das Inkrafttreten der Datenschutzgrundverordnung (DS-GVO)[1] hat in diesem Zusammenhang zu einer weiteren Verunsicherung geführt, weil vielfach nicht ganz klar ist, welche Sachverhalte europäisch geregelt sind, wann die allgemeinen Vorschriften des Bundesdatenschutzgesetzes (BDSG[2]) anzuwenden sind und in welchen Fällen spezifische Sonderregelungen bestehen, beispielsweise wenn es um Sozialdaten geht.

Die vorliegende Ausarbeitung ist ein Hilfsmittel für Berater_innen und Menschen mit HIV, die mit Datenschutzverletzungen konfrontiert sind oder sein können. Das Ziel ist ein Überblick über die wichtigsten gesetzlichen Regelungen und Grundsätze des Datenschutzrechts im Kontext von HIV. Darüber hinaus sollen Handlungsmöglichkeiten aufgezeigt werden, wie bei Datenschutzverletzungen vorgegangen werden kann. Berücksichtigt werden die Diskussionen und praktischen Erfahrungen aus dem Arbeitskreis Antidiskriminierungsarbeit der Deutschen Aidshilfe.

Wie bereits angedeutet soll die Ausarbeitung keine umfassende Darstellung des Datenschutzrechts leisten. Auf eine Darstellung juristischer Streitstände wird, auch um die Verständlichkeit für Nichtjurist_innen zu erhöhen, weitgehend verzichtet. Ziel ist, einen grundlegenden Überblick über die wesentlichen Normen und Zusammenhänge zu vermitteln.

Für eine vertiefende Auseinandersetzung mit dem Datenschutzrecht, sei ein Blick in die einschlägigen Handkommentare zur Datenschutzgrundverordnung (DS-GVO), zum Bundesdatenschutzgesetz (BDSG) und dem zweiten Kapitel des zehnten Sozialgesetzbuchs (SGB X) empfohlen.

[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)

[2] Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl. I S. 2097.

2. Schutz personenbezogener Daten von Menschen mit HIV

Die Fragestellungen im Zusammenhang mit Datenschutz und HIV sind vielgestaltig. Schon die möglicherweise beteiligten Personen und Institutionen sind sehr unterschiedlich. In Betracht kommen Familie, Freunde, Personal in Arztpraxen und Krankenhäusern, Arbeitgeber_innen, Kolleg_innen, Mitarbeiter_innen von Krankenkassen und viele weitere mehr. In Abhängigkeit von der Lebenssituation der jeweiligen Klient_innen können auch andere Behörden, beispielsweise freie Träger, das Jobcenter oder die Schule, mit der HIV-Infektion befasst sein.

Um dies zu verdeutlichen, aber auch zur Veranschaulichung der weiteren Ausführungen, folgende Fälle aus dem Arbeitskreis Antidiskriminierung der Deutschen Aidshilfe:

> **Fall 1 (gelber Punkt):**
> Ein Mann wird akut ins Krankenhaus eingeliefert. Auf dem Aktendeckel wird der HIV-Status durch einen gelben Punkt kenntlich gemacht, um das Personal auf den ersten Blick zu informieren.
>
> **Fall 2 (Aktennotiz):**
> Eine Ärztin teilt ihrer Sprechstundenhilfe per Notiz in der elektronischen Akte mit, dass die Patientin HIV-positiv ist.
>
> **Fall 3 (WhatsApp-Nachricht):**
> Die Ex-Ehefrau eines HIV-positiven Kochs informiert den Arbeitgeber per WhatsApp über den HIV-Status. Daraufhin kündigt der Arbeitgeber fristlos aus wichtigem Grund. Wenn herauskomme, dass der Koch HIV habe, könne der Laden auch gleich dicht gemacht werden.
>
> **Fall 4 (Klassenfahrt):**
> Eine Jugendamtsmitarbeiterin ist mit der Vormundschaft eines HIV-positiven Jugendlichen betraut. Es steht eine Klassenfahrt an und an die Schüler_innen wird ein Bogen ausgegeben, in dem Medikamentenangaben gemacht und/oder chronische Krankheiten vermerkt werden sollen. Darf die Mitarbeiterin den HIV-Status offenbaren und darf die Schule die Daten speichern?

Wie mit derartigen Fallgestaltungen umzugehen ist, soll im weiteren Verlauf der Ausarbeitung dargestellt werden.

3. Überblick über das Datenschutzrecht

In diesem Abschnitt werden die rechtlichen Grundlagen des Datenschutzrechts dargestellt. Nach einem Überblick über die gesetzlichen Grundlagen werden die zentralen Begriffe des Datenschutzrechts und die Grundsätze der Datenverarbeitung erläutert. Danach wird die rechtliche Prüfung eines datenschutzrechtlichen Vorgangs vorgestellt.

3.1. Grundlagen

Das Datenschutzrecht ist eine Querschnittsmaterie. Aus diesem Grund gibt es eine Vielzahl gesetzlicher Grundlagen, die sich mit dem Schutz personenbezogener Daten befassen. Dies wird schon dadurch deutlich, dass im Zuge der Anpassung des deutschen Datenschutzrechts an die Datenschutzgrundverordnung Änderungen in über 150 Bundesgesetzen vorgenommen werden mussten[3].

Im Kontext mit HIV sind neben der DS-GVO vor allem das Bundesdatenschutzgesetz und die Vorschriften über den Sozialdatenschutz, geregelt im SGB X, sowie die Verschwiegenheitspflichten von Berufsgeheimnisträgern nach § 203 StGB von Bedeutung.

Recht auf informationelle Selbstbestimmung

In seinem Volkszählungsurteil[4] hat das Bundesverfassungsgericht im Jahr 1983 anerkannt, dass unter den Bedingungen der automatisierten Datenverarbeitung eine Gefährdungslage besteht, wenn es dem Staat erlaubt wäre, unkontrolliert Daten zu sammeln und auszuwerten. Abhängig von den technischen Möglichkeiten ist es möglich, auch aus scheinbar harmlosen Daten weitreichende Erkenntnisse abzuleiten.

> „[Nutzbarkeit und Verwendungsmöglichkeit von Daten hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr."[5]

Dem hat das Gericht ein Grundrecht auf informationelle Selbstbestimmung entgegengesetzt, das es später auch als „Grundrecht auf Datenschutz"[6] bezeichnet hat. Es folgt aus dem allgemeinen Persönlichkeitsrecht der Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG und gewährleistet die Befugnis, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Wann und in welchen Grenzen eine Person persönliche Lebenssachverhalte offenbart werden, soll sie grundsätzlich selbst bestimmen können.

Diese grundlegenden Erwägungen des Bundesverfassungsgerichts gelten zunächst in Bezug auf den Staat, der an Grundrechte gebunden ist. Zudem ist das Recht auf informationelle Selbstbestimmung nicht schrankenlos, sondern kann durch Gesetze im überwiegenden Interesse der Allgemeinheit beschränkt werden. Wenn beispielsweise Leistungsträger miteinander Informationen über eine

[3] BT-Drs. 19/5647.
[4] BVerfGE 65, 1.
[5] BVerfGE65, 1 (45).
[6] BVerfGE 84, 239 (280).

bestimmte Person austauschen, braucht es daher eine solche gesetzliche Grundlage, die eine Weitergabe dieser Daten ermöglicht.

Private sind nicht unmittelbar an das Recht auf informationelle Selbstbestimmung gebunden. Die Gefahren für die Betroffenen von Datensammlungen, die das Bundesverfassungsgericht vor Augen hatte, als es über die Volkszählung urteilte, bestehen durch die digitale Datenverarbeitung heute bei Unternehmen in vergleichbarer Weise. Im Datenschutzrecht findet das Recht auf informationelle Selbstbestimmung deshalb seinen Ausdruck in dem Grundsatz, dass eine Verarbeitung von Daten nur dann zulässig ist, wenn dies gesetzlich erlaubt ist (→Verbot mit Erlaubnisvorbehalt, Siehe in 3.3 Rechtmäßigkeit, Treu und Glauben, Transparenz).

Auf europäischer Ebene ist das Recht auf den Schutz personenbezogener Daten in Art. 8 der Grundrechte-Charta verankert.

Im Falle von Verletzungen des allgemeinen Persönlichkeitsrechts sind die Betroffenen nicht schutzlos. Sowohl Behörden als auch Private können rechtlich dazu verpflichtet werden, rechtswidrige Eingriffe zu unterlassen und ggf. eingetretene Nachteile rückgängig zu machen. Welche Anspruchsgrundlage heranzuziehen ist, richtet sich nach dem Einzelfall.

Datenschutzgrundverordnung

Die Datenschutzgrundverordnung hat die frühere Datenschutzrichtlinie[7] der Europäischen Union abgelöst und gilt seit dem 25.05.2018 unmittelbar in allen Mitgliedstaaten. Das bedeutet, dass die DS-GVO, soweit sie anwendbar ist, alleinige Rechtsgrundlage ist, wenn sie nicht eine Abweichung durch ein nationales Gesetz erlaubt.

Der Anwendungsbereich ist für die Bestimmung der **Rechtsgrundlage** einer Datenverarbeitung von Bedeutung. Wenn die DS-GVO nicht anzuwenden ist, bedeutet dies allerdings nicht, dass ein Verhalten rechtmäßig ist. Im oben genannten Beispiel könnte die Person, deren HIV-Status durch ein Posting gegen ihren Willen offenbart wird, möglicherweise wegen einer Verletzung ihres allgemeinen Persönlichkeitsrechts vorgehen. Ihr steht ein Anspruch auf Unterlassung der rechtswidrigen Veröffentlichung zu, der gegebenenfalls durch eine einstweilige Verfügung gerichtlich gesichert werden kann, aber auch ein „Schmerzensgeld“ kommt in Betracht. In derartigen Fällen, in denen weitere Verletzungen des Persönlichkeitsrechts drohen, sollte zeitnah anwaltlicher Rat eingeholt werden, von einem eigenen Vorgehen ist eher abzuraten.

Die DS-GVO unterscheidet nicht grundlegend zwischen öffentlichen und nicht-öffentlichen Stellen. Im Ausgangspunkt macht es insoweit keinen Unterschied, ob eine Behörde personenbezogene Daten verarbeiten will oder ein privates Unternehmen. Allerdings finden sich in der DSGVO mehrere Sondervorschriften für öffentliche Stellen.

Der sachliche Anwendungsbereich der Verordnung umfasst nach Art. 2 Abs. 1 DS-GVO die ganz oder teilweise **automatisierte Verarbeitung** personenbezogener Daten. Anwendbar ist die DS-GVO zudem, wenn Daten in einem Dateisystem gespeichert werden.

[7] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr von 1995.

Beispiel:
Die DS-GVO ist anwendbar, wenn der Arbeitgeber einen Mitarbeiter per E-Mail über die HIV-Infektion eines Bewerbers für eine Stelle informiert. Anders wäre es, wenn der Arbeitgeber den Mitarbeiter mündlich von der HIV-Infektion in Kenntnis gesetzt hätte. In diesem Falle kann auf das allgemeine Persönlichkeitsrecht des Arbeitnehmers aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zurückgegriffen werden.

Merke:
Dass die Datenschutzgrundverordnung in ihrem Anwendungsbereich begrenzt ist, wird nicht selten übersehen. Sie ist nicht auf alle Fallgestaltungen anzuwenden, die mit der Verarbeitung personenbezogener Daten zusammenhängen.

Nicht vom Anwendungsbereich erfasst sind nach Art. 2 Abs. 2 Buchst. c) DS-GVO Datenverarbeitungen, wenn eine natürliche Person ausschließlich im **persönlichen oder familiären Bereich** tätig wird. Die Verarbeitung von Daten muss sich auf den Privatbereich beschränken[8]. Wenn nicht nur Familienmitglieder oder enge Freunde einen Zugriff auf personenbezogene Daten erhalten, sondern z.B. der Arbeitgeber oder die Öffentlichkeit[9], kann die Datenschutzgrundverordnung angewendet werden.

Beispiel:
Das Outing eines HIV-Positiven auf einem privaten Facebook-Profil ist eher nicht an der DS-GVO zu messen, wohl aber, wenn der Post öffentlich einsehbar ist. In ersterem Fall kann gleichwohl unter Berufung auf das allgemeine Persönlichkeitsrecht gegen das Outing vorgegangen werden. Der Verletzer kann zur Unterlassung verpflichtet werden, zusätzlich könnte ein „Schmerzensgeld" zu zahlen sein.

Die Tätigkeit der Polizei, Staatsanwaltschaften und Gerichte unterliegt ebenfalls nicht der DS-GVO. Nach Art. 2 Abs. 2 Buchst. d) DS-GVO gilt sie nicht für Tätigkeiten von Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Maßnahmen dieser Behörden sind daher weiterhin an den nationalen Regelungen zu messen.

Beispiel[10]:
Datenspeicherungen der NRW-Polizei im Kontext mit einem Ermittlungsverfahren wegen einer (möglichen) Übertragung von HIV richten sich nach dem Polizeigesetz NRW. Die Polizeigesetze regeln, welche Daten gespeichert werden dürfen und verpflichten die Polizeibehörden zur Löschung von Daten, deren Speicherung unzulässig ist.

Der **räumliche Anwendungsbereich** der DS-GVO ist ebenfalls sehr weitgehend. Er ist nach Art. 3 Abs. 2 DS-GVO bereits dann eröffnet, wenn Daten einer Person verarbeitet werden, die sich in der Europäischen Union befindet.

[8] *Bäcker*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 2 Rn. 15;
[9] Das gilt vor allem im Internet:„Jegliche öffentlich online zugängliche Daten sind nicht privilegiert", *Ernst*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 2 Rn. 21.
[10] Siehe https://magazin.hiv/2017/06/13/hiv-kriminalisierung-in-duesseldorf/.

Bundesdatenschutzgesetz

Das BDSG wurde durch die DS-GVO abgelöst, es hat nur noch eine ergänzende Funktion. Es ist nur noch für die Bereiche relevant, in denen die DS-GVO eine Abweichung ermöglicht, was unter anderem beim Schutz von Beschäftigtendaten der Fall ist[11]. So dürfen nach § 26 Abs. 1 BDSG Daten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung von Verpflichtungen, die sich aus einem Gesetz, einem Tarifvertrag oder einer Betriebs-/Dienstvereinbarung ergebenden Rechte und Pflichten der betrieblichen Interessenvertretung erforderlich ist.

Die Länder haben im Rahmen ihrer Zuständigkeiten eigene Datenschutzgesetze erlassen[12], auch für Landesbehörden gilt die DS-GVO allerdings vorrangig, soweit sie anwendbar ist.

SGB I und X (Sozialdatenschutz)

Der Schutz von Sozialdaten ist, ebenfalls lediglich ergänzend zur DS-GVO[13], im zweiten Kapitel des SGB X geregelt. Den Begriff der Sozialdaten nennt § 67 Abs. 2 Satz 1 SGB X. Hierbei handelt es sich um personenbezogene Daten, die von einem Leistungsträger verarbeitet werden. Leistungsträger sind nach § 12 Satz 1 SGB I die in den §§ 18 bis 29 SGB I genannten Körperschaften, Anstalten und Behörden.

Nach § 35 Abs. 1 Satz 1 SGB I hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis). Daher muss sich die Zulässigkeit einer Verarbeitung aus einer Vorschrift in den Sozialgesetzbüchern oder aus sonstigem Recht ergeben.

StGB

Das Strafgesetzbuch kennt verschiedene Straftatbestände, die personenbezogene Daten schützen.

Im Gesundheitsbereich ist insbesondere **§ 203 StGB** von Bedeutung. Wer hiernach unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm/ihr in der Eigenschaft einer der dort genannten Berufsgruppen, z.B. Ärzt_in, Rechtsanwält_in oder Sozialarbeiter_in anvertraut worden oder sonst bekanntgeworden ist, macht sich strafbar. Dies gilt beispielsweise für einen Betriebsarzt, der den HIV-Status eines Beschäftigten an den Arbeitgeber übermittelt, ohne z.B. durch eine Schweigepflichtentbindung oder eine anderweitige Einwilligung dazu berechtigt zu sein. Eine solche Verletzung von Privatgeheimnissen kann mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft werden. Zusätzlich drohen berufsrechtliche Konsequenzen.

[11] Siehe § 26 BDSG.
[12] Für einen Überblick siehe *Taeger/Schmidt*, in: Taeger/Gabel, DSGVO/BDSG, Einführung Rn. 65.
[13] So ausdrücklich § 67 Abs. 1 SGB X.

Auch **Mitarbeiter von Behörden** sind nach § 203 Abs. 2 StGB verpflichtet, ihnen anvertraute oder bekanntgewordene Geheimnisse zu wahren. Auf den Informationsaustausch *innerhalb* einer Behörde ist die Vorschrift nicht anzuwenden[14]. Eine Mitteilung von Tatsachen an *externe* Behörden oder Dritte ist hingegen nur zulässig, wenn eine rechtliche Vorschrift dies erlaubt[15]. Angesichts der Vielzahl an Gesetzen, die einen Datenaustausch ermöglichen, bspw. zwischen verschiedenen Behörden, ist sorgfältig zu ermitteln, auf welche Rechtsgrundlage eine Übermittlung gestützt werden kann. **Dabei kann es zweckmäßig sein, die Behörde um eine Stellungnahme zu bitten, auf welche Rechtsgrundlage sie eine Datenübermittlung stützt.** Erfolgt hierauf keine Reaktion, kann die/der zuständige behördliche Datenschutzbeauftragte oder die Aufsichtsbehörde hinzugezogen werden.

Unter **Geheimnis** sind Tatsachen zu verstehen, die sich auf den die jeweilige Person beziehen und nur einem begrenzten Personenkreis bekannt, also nicht bereits öffentlich sind[16]. Der Umstand, dass eine Person mit HIV infiziert ist oder nähere Einzelheiten zum Gesundheitszustand, sind damit in aller Regel erfasst.

Das Geheimnis wird **offenbart**, wenn es einem Dritten mitgeteilt wird[17]. Anonyme Mitteilungen erfüllen den Tatbestand nicht, wobei darauf zu achten ist, dass nicht durch äußere Umstände ein Rückschluss auf die Person möglich ist. Keine hinreichende Anonymisierung wäre es, wenn ein Dritter durch Ausschlussverfahren in der Lage wäre, die Person zu identifizieren, selbst wenn dies einen gewissen Aufwand erfordern würde. Eine Anonymisierung liegt daher nicht vor, wenn beispielsweise von „einem Mitarbeiter" einer bestimmten Kindertageseinrichtung gesprochen wird, der mit HIV infiziert ist, wenn dort nur ein oder zwei Männer arbeiten. Auch wenn der Name nicht genannt wird, ist es zumeist ohne größeren Aufwand möglich, die konkrete Person zu identifizieren. Wenn aber von einem städtischen Mitarbeiter gesprochen wird, ohne zu erwähnen, in welcher Einrichtung er arbeitet, liegt kein Personenbezug mehr vor. Denn dann kommen eine Vielzahl von Personen in Betracht, die gemeint sein können.

Kein Offenbaren liegt nach § 203 Abs. 3 Satz 1 StGB vor, wenn die verpflichtete Person ein Geheimnis den bei ihr berufsmäßig tätigen **Gehilfen** oder den bei ihr zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Eine Ärztin ist daher befugt, der Sprechstundenhilfe eine Mitteilung über den Gesundheitszustand des Patienten zu machen. Auch weitere Personen, z.B. ein Dienstleister, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, dürfen einen Umgang mit Geheimnissen haben, allerdings nur soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist. Reinigungskräfte oder Transportpersonal in einem Krankenhaus dürfen daher nicht über eine vorliegende HIV-Infektion informiert werden, denn in aller Regel wird diese Information für die Erfüllung ihrer Aufgaben nicht erforderlich sein. Voraussetzung ist stets, dass das Personal oder der Dienstleister zur Geheimhaltung verpflichtet wurde.

Unbefugt ist das Offenbaren eines Geheimnisses, wenn kein Einverständnis der Person vorliegt. Ein solches kann ausdrücklich, aber auch durch schlüssiges Verhalten erklärt werden[18].

---

[14] OLG Frankfurt am Main, NStZ-RR 2003, 170.
[15] *Weidemann*, in: v. Heintschel-Heinegg, BeckOK StGB, §203 Rn. 55.
[16] *Weidemann*, in: v. Heintschel-Heinegg, BeckOK StGB, §203 Rn. 4.
[17] *von Cierniak/Niehaus*, in: Münchener Kommentar, StGB, § 203 Rn. 51.
[18] *Weidemann*, in: v. Heintschel-Heinegg, BeckOK StGB, §203 Rn. 39.

Wenn eine **gesetzliche Pflicht[19] oder eine Berechtigung** besteht, ein Geheimnis zu offenbaren, fehlt es an der Rechtswidrigkeit der Tat. Daher ist immer im Einzelfall zu ermitteln, auf welcher Grundlage die Mitteilung erfolgen kann.

Eine Möglichkeit eröffnet der rechtfertigende Notstand nach § 34 StGB[20]. Ein Arzt darf unter Berufung hierauf die HIV-Infektion seines Patienten ansteckungsgefährdeten Dritten in Ausnahmefällen mitteilen. Voraussetzung dafür ist, dass er keine andere Wahl mehr hatte, um die unmittelbare Gefährdung anderer auszuschließen[21]. Nur wenn daher konkrete Anhaltspunkte dafür bestehen, dass sein Versuch, den Patienten zu verantwortungsbewusstem Verhalten oder zur Information der gefährdeten Personen zu bewegen, nicht erfolgreich war, wird er ausnahmsweise seine Schweigepflicht brechen dürfen[22]. Dabei wird es sich um Ausnahmefälle handeln, in denen die Zulässigkeit der Datenweitergabe sorgsam zu prüfen ist. In keinem Fall kommt ein Bruch der Schweigepflicht in Betracht, wenn die Patientin/der Patient aufgrund einer erfolgreichen Behandlung nicht infektiös ist. Denn hier besteht realistischerweise gerade keine Gefährdung mehr, die so weit über das allgemeine Lebensrisiko hinausginge, dass den Interessen anderer Personen der Vorrang gegenüber dem Persönlichkeitsrecht der Patientin/des Patienten zukommt.

Eine gesetzliche Pflicht zur namentlichen Meldung einer HIV-Infektion besteht nicht[23]. Ob bei Strafgefangenen unter den heutigen medizinischen Bedingungen, insbesondere wenn die Person nicht mehr infektiös ist, noch immer eine Unterrichtung der Bediensteten zulässig ist, dürfte zweifelhaft sein[24].

Im **Fall 1** (gelber Punkt) ist der sachliche Anwendungsbereich der Datenschutzgrundverordnung eröffnet. Zwar stellt eine Papierakte keine automatisierte Verarbeitung dar. Allerdings handelt es sich bei Akten dann um ein Dateisystem, wenn sie nach bestimmten Kriterien geordnet sind. Indem ein gelber Punkt als Hinweis auf die HIV-Infektion auf die Akte geklebt wird, besteht Ordnung des Akteninhalts jedenfalls insoweit, als Patienten mit einer spezifischen Erkrankung (HIV) auf dem Deckblatt gekennzeichnet werden.

Die Aktennotiz der Ärztin in **Fall 2** (Aktennotiz) ist ebenfalls an der DS-GVO zu messen, ohne dass es darauf ankäme, wie die Akte geordnet ist. Bei einer e-Akte handelt sich jedenfalls um eine automatisierte Verarbeitung personenbezogener Daten.

Die Information des Arbeitgebers über den HIV-Status in **Fall 3** (WhatsApp-Nachricht) fällt nicht mehr in den ausschließlichen persönlichen oder familiären Bereich, sondern greift darüber hinaus. Da es sich auch um eine automatisierte Datenverarbeitung handelt, ist die Datenschutzgrundverordnung anwendbar.

[19] *von Cierniak/Niehaus*, in: Münchener Kommentar, StGB, § 203 Rn. 91.
[20] *von Cierniak/Niehaus*, in: Münchener Kommentar, StGB, § 203 Rn. 87.
[21] LG Braunschweig, NJW 1990, 770 (771).
[22] *von Cierniak/Niehaus*, in: Münchener Kommentar, StGB, § 203 Rn. 90.
[23] Siehe § 7 Abs. 3 Nr. 2 IfSG.
[24] Eine Zulässigkeit wurde in den 1980er Jahren noch überwiegend angenommen, *Dargel*, Helmut, NStZ 1989, 207 (210); vgl. *Heger*, in: Lackner/Kühl, StGB, § 203 Rn. 20 m.w.N.

3.2. Grundbegriffe

Das Datenschutzrecht bezieht sich auf **personenbezogene Daten**. Nach Art. 4 Nr. 1 DS-GVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Begriff ist damit ziemlich weit: Solange ein Personenbezug besteht, unterliegt eine Information den Regelungen der Datenschutzgrundverordnung. Dies gilt solange, wie nicht der Bezug zu einer Person von der Sachinformation getrennt wird, sodass eine Zuordnung nicht mehr möglich ist.

Zu beachten ist, dass Daten ihren Personenbezug nicht verlieren, wenn eine direkte oder indirekte Identifizierbarkeit besteht. Dazu ist eine Kenntnis des Namens der betroffenen Person nicht erforderlich. Es reicht aus, dass eine Zuordnung erfolgen kann.

> **Beispiel:**
> Ein Fingerabdruck ist ein personenbezogenes Datum, auch wenn unklar ist, von welcher Person er stammt.

Die **Verarbeitung** personenbezogener Daten betrifft nach Art. 4 Nr. 2 DS-GVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Die Übermittlung von Daten per E-Mail ist daher genauso eine Verarbeitung wie die Vernichtung einer elektronischen Patientenakte oder das Offenlegen des Gesundheitszustands eines Patienten durch einen ungenügenden Sichtschutz an der Anmeldung einer Arztpraxis, durch die Besucher einen Blick auf den Computermonitor erhalten.

Verantwortlicher für die Datenverarbeitung ist nach Art. 4 Nr. 7 DS-GVO, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Es handelt sich um die natürlichen Personen, die tatsächlich über die Verarbeitung bestimmen, bspw. den Geschäftsführer einer GmbH oder den Behördenleiter. Dem Verantwortlichen obliegt es nach Art. 24 Abs. 1 Satz 1 DS-GVO insbesondere, geeignete technische und organisatorische Maßnahmen zu ergreifen, damit die Datenverarbeitung im Einklang mit den gesetzlichen Vorschriften erfolgt.

Der Verantwortliche muss geeignete **technische und organisatorische Maßnahmen** (TOM) ergreifen, um den Schutz personenbezogener Daten sicherzustellen. Art. 32 Abs. 1 DS-GVO fordert „ein dem Risiko angemessenes Schutzniveau“. Zu beachten ist, dass Schutzmaßnahmen immer dem Stand der Technik entsprechen müssen. Unzureichende Maßnahmen eine Haftung des Verantwortlichen oder des Auftragsverarbeiters für den dadurch eingetretenen Schaden nach sich ziehen kann.

3.3. Datenschutzgrundsätze

Art. 5 DS-GVO nennt sieben Grundsätze für die Verarbeitung personenbezogener Daten, die das gesamte Datenschutzrecht durchziehen. Sie sind verbindliche Regelungen[25] und daher bei jeder Datenverarbeitung zu beachten. Entspricht die Datenverarbeitung ihnen nicht, ist sie nicht rechtmäßig.

Rechtmäßigkeit, Treu und Glauben, Transparenz

Personenbezogene Daten müssen gemäß Art. 5 Abs. 1 lit. a) DS-GVO rechtmäßig verarbeitet werden. **Die DS-GVO geht von einem Verbot mit Erlaubnisvorbehalt[26] aus.** Eine Verarbeitung personenbezogener Daten ist grundsätzlich unzulässig, wenn nicht die Verordnung die Verarbeitung zulässt[27]. Der Grundsatz der Rechtmäßigkeit erfordert, dass sich eine Verarbeitung auf eine der in Art. 6 Abs. 1 DS-GVO genannten Rechtsgrundlagen (→Siehe in 3.4. Rechtsgrundlagen der Datenverarbeitung) stützen lässt.

Eine Verarbeitung nach Treu und Glauben erfordert, dass der Verantwortliche die Interessen der betroffenen Person berücksichtigt[28] bzw. „fair“[29] ablaufen soll. Die betroffene Person soll vor unklaren Datenverarbeitungen geschützt werden, z.B. einer heimlichen Datenerhebung, wenn diese auch offen durchgeführt werden könnte[30].

Transparenz soll der betroffenen Person eine Kenntnis darüber verschaffen, in welchem Umfang ihre personenbezogenen Daten verarbeitet werden. Dies setzt voraus, dass „alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind.“[31] Welche Informationen der Verantwortliche bereitstellen muss, wird durch die Art. 12 ff. DS-GVO (→ Siehe in 3.5 Informationspflichten) geregelt.

Kritisch anzumerken ist, dass viele Informationen in Arztpraxen und Krankenhäusern die Vorgaben der DS-GVO an die Transparenz kaum einhalten werden. Klein gedruckte Informationen über mehrere Seiten in komplizierter Sprache sind nicht selten. Den Patientinnen/Patienten muss zudem genügend Zeit zur Verfügung stehen, die Informationen zu lesen, bevor beispielsweise in eine Datenverarbeitung eingewilligt wird.

Zweckbindung

Daten unterliegen nach Art. 5 Abs. 1 lit. b) DS-GVO einer Zweckbindung. Sie dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Der Zweck sollte vor der Erhebung festgelegt, spätestens aber mit Beginn der Verarbeitung muss er fixiert werden[32]. Eine Datensammlung für unbestimmte Zwecke ist unzulässig. Eine Änderung des Zwecks ist möglich, allerdings nur unter den Voraussetzungen des Art. 6 Abs. 4 DS-GVO.

---

[25] *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 5 Rn. 1.
[26] *Schantz*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 5 Rn. 5.
[27] Erw.-Gr. 40.
[28] *Schantz*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 5 Rn. 7.
[29] Unter Hinweis auf die englische Fassung der Verordung *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 5 Rn. 14; ferner *Albrecht*, CR 2016, 88.
[30] *Schantz*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 5 Rn. 9.
[31] Erw.-Gr. 39.
[32] *Schantz*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 5 Rn. 14.

Datenminimierung

Der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c) DS-GVO bestimmt, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Damit sollen unnötige Datenverarbeitungen vermieden werden. Wenn es möglich ist, das Ziel der Datenverarbeitung durch einen geringeren Eingriff in die Rechte der Person zu erreichen, fehlt es an der Erforderlichkeit[33].

Richtigkeit

Daten müssen sachlich richtig sein. Art. 5 Abs. 1 lit. d) DS-GVO fordert, dass sie erforderlichenfalls auf dem neuesten Stand zu bringen sind. Die betroffene Person hat nach Art. 16 DS-GVO einen Anspruch auf Berichtigung. Zudem sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Speicherbegrenzung

Nach dem Grundsatz der Speicherbegrenzung des Art. 5 Abs. 1 lit. e) DS-GVO müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Die Dauer der Speicherung ist auf das Mindestmaß zu beschränken[34].

Integrität und Vertraulichkeit

Personenbezogene Daten müssen nach Art. 5 Abs. 1 lit. f) DS-GVO in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Der Verantwortliche muss die Datensicherheit durch geeignete technische und organisatorische Maßnahmen sicherstellen.

Rechenschaftspflicht

Schließlich ist der Verantwortliche gemäß Art. 5 Abs. 2 DS-GVO für die Einhaltung der beschriebenen Datenschutzgrundsätze verantwortlich und muss dies nachweisen können. Um der Nachweispflicht genügen zu können, muss der Verantwortliche die Verarbeitung dokumentieren.

Das Kleben eines gelben Punktes auf die Patientenakte in **Fall 1** informiert nicht nur das mit der Behandlung betraute Krankenhauspersonal über die HIV-Infektion der betroffenen Person. Auch Dritte können diese zur Kenntnis nehmen, wenn sie mit der Bedeutung des Punktes vertraut sind. Der Grundsatz der Vertraulichkeit wird hier nicht gewahrt. Die Diagnose in der Akte zu nennen, würde dem Informationsbedürfnis der behandelnden Beschäftigten gerecht und dabei die Daten der betroffenen Person schützen.

[33] *Schantz*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 5 Rn. 25.
[34] Erw.-Gr. 39.

3.4. Rechtsgrundlagen der Datenverarbeitung

Die Rechtmäßigkeit einer Verarbeitung richtet sich, wenn es sich nicht um besondere Kategorien personenbezogener Daten wie z.B. Gesundheitsdaten handelt (→ Siehe in Besondere Kategorien personenbezogener Daten), nach Art. 6 Abs. 1 DS-GVO. Zumeist wird es im Zusammenhang mit HIV um solche besondere Kategorien personenbezogener Daten gehen. Wo dies nicht der Fall ist, muss die allgemeine Rechtsgrundlage des Art. 6 DS-GVO herangezogen werden.

Allgemeine Rechtsgrundlage (Art. 6 DS-GVO)

Die Verarbeitung personenbezogener Daten erfordert eine Rechtsgrundlage, die sich aus Art. 6 Abs. 1 DS-GVO geben kann. Für die ab Verarbeitung besonderer Kategorien personenbezogener Daten gilt allerdings, dass diese grundsätzlich unzulässig ist, es sei denn es liegt eine Ausnahme von dem grundsätzlichen Verbot der Verarbeitung nach Art. 9 Abs. 2 DS-GVO vor. Die allgemeine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO findet in diesem Fall keine Anwendung, da Art. 9 Abs. 2 DS-GVO diese Ausnahmen abschließend regelt.

Im Regelfall bedarf es daher der Prüfung, ob einer der Rechtsgrundlagen nach Art. 6 Abs. 1 DS-GVO vorliegt. Alternativ können weitere Gesetze eine Verarbeitung zulassen.

Neben den einzelnen Erlaubnistatbeständen des Art. 6 Abs. 1 DS-GVO sind stets die Datenschutzgrundsätze aus Art. 5 DS-GVO und die weiteren Anforderungen, insbesondere die Informationspflichten gegenüber der betroffenen Person, zu berücksichtigen.

Einwilligung

Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 lit. a) DS-GVO zulässig, wenn die betroffene Person ihre Einwilligung erteilt. Die Möglichkeit, in eine Datenverarbeitung einzuwilligen, folgt aus dem Recht der betroffenen Personen auf informationelle Selbstbestimmung. Sie selbst können entscheiden, in welchen Fällen sie ihre Daten nicht verarbeitet wissen wollen. Umgekehrt steht es ihnen frei, darauf zu verzichten.

Wo eine Einwilligung notwendig ist, aber nicht erfolgt oder eingeschränkt wird (z.B. durch Streichungen in einem Formular), kann eine Datenverarbeitung nicht bzw. nur soweit die Einwilligung gegeben wurde erfolgen.

Eine Einwilligung stellt allerdings nur eine Möglichkeit für den Verantwortlichen dar, Daten rechtmäßig zu verarbeiten. Nicht in jedem Falle ist von ihm gefordert, eine solche von der betroffenen Person einzuholen. Nach Inkrafttreten der DS-GVO war vielfach zu beobachten, dass Verantwortliche geradezu hektisch Einwilligungen für alle möglichen Formen der Datenverarbeitung einforderten. Dabei hätte es vielfach ausgereicht, die betroffenen Personen über die Verarbeitung transparent zu informieren, weil sich die Verarbeitung auf eine andere Rechtsgrundlage hätte stützen lassen, bspw. die Vertragserfüllung.

An eine Einwilligung sind relativ hohe Anforderungen zu stellen. Eine Einwilligung muss nach Art. 4 Nr. 11 DS-GVO „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich“ ab-

gegeben werden. Erforderlich ist eine Erklärung oder eine sonstige eindeutige bestätigende Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Freiwillig ist eine Einwilligung nur dann abgegeben, wenn sie ohne jeden Zwang oder Druck abgegeben wird. An der Freiwilligkeit einer Einwilligung, bei der der betroffenen Person nur wenig Zeit bleibt, um den Umfang der von ihr abgegebenen Erklärung zu erfassen, wird man bezweifeln müssen. Auch wenn dem Verantwortlichen ersichtlich ist, dass sich die betroffene Person in einer Zwangslage befindet und die Einwilligungserklärung nur deswegen abgibt, weil es von ihr erwartet wird, wird diese nicht wirksam sein. Besteht zwischen dem Verantwortlichen und der betroffenen Person ein Ungleichgewicht, insbesondere im Arbeitsverhältnis, wird ebenfalls sehr genau zu prüfen zu sein, ob die Einwilligung ohne Zwang und Druck abgegeben wurde.

Die Einwilligung bezieht sich auf **bestimmte Zwecke** der Verarbeitung. Unzulässig ist es daher, wenn eine Einwilligung „auf Vorrat" verlangt wird. Gleiches gilt, wenn eine Einwilligungserklärung eine Vielzahl von Zwecken auflistet, konkret aber nur einige wenige relevant sind.

Darüber hinaus muss der betroffenen Person der Umfang ihrer Einwilligung klar sein. Die Zwecke der Verarbeitung, die die Dauer der Speicherung, etc. müssen gegebenenfalls durch den Verantwortlichen transparent erläutert werden. Vor allem, wenn die betroffene Person aufgrund ihres Alters oder sprachlicher Barrieren erkennbar nicht in der Lage ist zu verstehen, was er erklärt, kann es an der nach Art. 5 Abs. 1 Buchst. a) DS-GVO geforderten Transparenz fehlen.

Eine bestimmte **Form** der Einwilligung ist nicht vorgesehen, allerdings muss die betroffene Person eine Erklärung aktiv abgeben. Ein bloßes Schweigen genügt nicht. Dies gilt selbst dann, wenn der Verantwortliche darauf hingewiesen hat, dass er ein Schweigen als eine Bewilligung wertet.

Eine Einwilligung von **Minderjährigen** ist möglich, wenn sie einsichtsfähig sind und die Tragweite ihrer Entscheidung abschätzen können. Andernfalls bedarf es einer Einwilligung der Sorgeberechtigten.

Die Einwilligung kann ohne Angabe von Gründen mit Wirkung für die Zukunft ganz oder teilweise **widerrufen** wird, Art. 7 Abs. 3 DS-GVO. Mit dem Widerruf entfällt die Rechtsgrundlage für die Verarbeitung, es sei denn sie lässt sich auf eine andere Rechtsgrundlage stützen. Fehlt es an einer Rechtsgrundlage, so sind die Daten unverzüglich zu löschen.

Vertragserfüllung und vorvertragliche Maßnahmen

Nach Art. 6 Abs. 1 Satz 1 Buchst. b) DS-GVO ist eine Verarbeitung personenbezogener Daten zulässig, wenn und soweit dies für die Durchführung des Vertrages erforderlich ist. Der Umfang richtet sich nach dem Vertragsgegenstand und den Vereinbarungen der Beteiligten. Wäre dies anders, wäre ein Austausch von Leistungen und Gütern nicht möglich[35].

Erforderlich ist eine Verarbeitung, wenn der Vertrag ohne die Verarbeitung nicht in der Weise erfüllt werden könnte, wie es der Vereinbarung der Beteiligten entspricht. Dabei werden immer auch die Interessen der Beteiligten im Blick zu behalten sein.

[35] *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 6 Rn. 29.

Rechtliche Verpflichtung

Besteht eine rechtliche Verpflichtung, ist eine Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Buchst. c) DS-GVO zulässig. Diese rechtliche Verpflichtung muss sich nach Abs. 3 aus einer Rechtsvorschrift ergeben, wobei neben Gesetzen der Union oder eines Mitgliedstaates auch Gesetze im materiellen Sinn, zum Beispiel Verordnungen oder Satzungen, zählen[36].

Eine Verarbeitung muss zur Erfüllung dieser rechtlichen Verpflichtung des verantwortlichen erforderlich sein. Sie muss daher streng auf die Daten begrenzt bleiben, die zur Erfüllung der Verpflichtung tatsächlich benötigt werden.

Lebenswichtige Interessen

Um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, können nach Art. 6 Abs. 1 Satz 1 Buchst. d) DS-GVO personenbezogene Daten verarbeitet werden. Die Verarbeitung muss zum Schutz lebenswichtiger Interessen erforderlich sein. Lebenswichtige Interessen sind insbesondere die körperliche Unversehrtheit und das Leben, eine Lebensgefahr muss allerdings nicht bestehen[37]. Dies könnte beispielsweise der Fall sein, wenn eine Person mit HIV z.B. im künstlichen Koma liegt. Um die lebenswichtige Versorgung durch die Antiretrovirale Therapie zu gewährleisten, wird diese Information an die Ärzte weitergeben werden. (lebenswichtige Interessen können auch bei besonderen Kategorien personenbezogener Daten in Ansatz gebracht werden, → Siehe Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO)).

Sowohl öffentliche als auch nicht-öffentliche Stellen können sich auf den Schutz lebenswichtiger Interessen als Rechtsgrundlage berufen. Art. 6 Abs. 1 Buchst. d) DS-GVO soll aber nur dann anzuwenden sein, wenn sich eine Verarbeitung nicht auf eine andere Rechtsgrundlage stützen lässt[38]. Insgesamt ist festzustellen, dass lebenswichtigen Interessen als Rechtsgrundlage nur ein enger Anwendungsbereich verbleibt[39].

Erfüllung öffentlicher Aufgaben

Ist eine Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, kann eine solche nach Art. 6 Abs. 1 Satz 1 Buchst. e) DS-GVO zulässig sein. Die Aufgabe muss dem Verantwortlichen nach Abs. 3 durch eine Rechtsvorschrift übertragen worden sein und der Verantwortliche muss im Rahmen dieser Aufgabe tätig werden[40]. Ein Beispiel wäre eine Verarbeitung von Daten durch das Jugendamt oder die Schule.

Die Datenverarbeitung ist nur dann erforderlich, wenn sie verhältnismäßig ist[41]. Lässt sich die Belastung der betroffenen Person durch ein milderes Mittel reduzieren, ist dieses vorrangig zu wählen. Die Datenverarbeitung ist insoweit auf das unbedingt Notwendige zu beschränken[42].

---

[36] *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 6; Rn. 16; *Schulz* in Gola, DS-GVO, Art. 6 Rn. 41
[37] *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 6 Rn. 36.
[38] *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 6 Rn. 36.
[39] *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 6 Rn. 22.
[40] *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 6 Rn. 41
[41] *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 6 Rn. 23.
[42] *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 6 Rn. 23.

Berechtigte Interessen des Verantwortlichen oder Dritter

Eine Verarbeitung ist nach Art. 6 Abs. 1 Buchst. f) DS-GVO zulässig, wenn sie 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, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Eine Verarbeitung nach Art. 6 Abs. 1 Buchst. f) DS-GVO setzt eine Interessenabwägung voraus. Dabei sind die aufseiten des Verantwortlichen bestehenden rechtlichen, wirtschaftlichen und ideellen Interessen denen der betroffenen Person gegenüberzustellen. Dabei ist in drei Schritten[43] vorzugehen:

- Welche berechtigten Interessen des Verantwortlichen bestehen?
- Ist die Datenverarbeitung erforderlich?
- Kein Überwiegen der berechtigten Interessen der betroffenen Person?

„Berechtigte Interessen" können rechtliche, wirtschaftliche und ideelle Interessen sein. Illegale oder diskriminierende Beweggründe sind nicht berechtigt im Sinne des Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO. Im Rahmen der Interessenabwägung werden die „vernünftige(n) Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen"[44] in Ansatz zu bringen sein. Im Rahmen der Interessenabwägung sind die jeweiligen Rechtspositionen einander gegenüberzustellen und zu gewichten. Ergibt sich, dass die betroffene Person ein überwiegendes Interesse geltend machen kann, ist ein Widerspruch gegen die Verarbeitung möglich (→Siehe 5. Betroffenenrechte).

Im Zusammenhang mit HIV besonders hervorzuheben ist, dass in aller Regel eine Datenübermittlung auf der Grundlage eines berechtigten Interesses nicht möglich sein wird, weil es sich bei dem HIV-Status um besondere Kategorien personenbezogener Daten handelt. Derartige besonders sensible Daten sind einer Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchst. f) DS-GVO nicht zugänglich, eine Verarbeitung kann nur nach Art. 9 DS-GVO erfolgen.

Besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO)

Datenschutz-Grundverordnung geht davon aus, dass besondere Kategorien personenbezogener Daten, unter anderem Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung, grundsätzlich nicht verarbeitet werden dürfen. Nur in den Fällen, die in Art. 9 Abs. 2 DS-GVO geregelt sind, ist eine Verarbeitung ausnahmsweise zulässig.

Gesundheitsdaten sind alle Daten, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand hervorgehen[45]. Dazu gehört die Information über eine Krankheit oder eine medizinische Behandlung. Im Kontext von HIV wird die Rechtmäßigkeit einer Datenverarbeitung regelmäßig nach Art. 9 DS-GVO zu bestimmen sein.

[43] Vgl. *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, DS-GVO, Art. 6 Rn. 27.
[44] Erw. Gr. 47.
[45] Erw. Gr. 35.

Daten zum **Sexualleben** betreffen unter anderem Angaben zum Geschlechtsverkehr, darunter auch die Anzahl und Identität der Sexualpartner_innen[46].

Sexuelle Orientierung meint die Angabe, ob jemand hetero-, bi-, homo-, trans- oder auch asexuell ist[47].

Die wichtigsten Gründe, um besondere Kategorien von Daten verarbeiten zu können, sind insbesondere:

- Das Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person (Buchst. a))
- Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben (Buchst. c))
- die betroffene Person hat die Daten offensichtlich öffentlich gemacht (Buchst. e))
- die Verarbeitung ist für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufes erforderlich (Buchst. h))

Im Falle einer Verarbeitung nach Art. 9 Abs. 2 Buchst. h) DS-GVO muss nach Abs. 3 eine Datenverarbeitung von Fachpersonal, dass dem Berufsgeheimnis unterliegt, erfolgen bzw. unter dessen Verantwortung. § 22 Abs. 1 Nr. 1 Buchst. b) BDSG übernimmt den Wortlaut der DS-GVO[48].

Bei einer Verarbeitung von Gesundheitsdaten ist stets darauf zu achten, ob es ein milderes Mittel zu einer Verarbeitung gibt, wenn nicht eine Einwilligung der betroffenen Person vorliegt.

Den Arbeitgeber in **Fall 3** (WhatsApp-Nachricht) geht der HIV-Status des Kochs nichts an. Denn eine Gefährdung für Gäste ist nicht ersichtlich. Die Ex-Ehefrau kann die Übermittlung auf keine Rechtsgrundlage stützen, sodass diese unzulässig ist. Auch für eine weitere Speicherung der Nachricht auf dem Smartphone des Arbeitgebers fehlt es an einer Rechtsgrundlage.

Die Jugendamtsmitarbeiterin in **Fall 4** (Klassenfahrt) muss die Übermittlung auf eine Rechtsgrundlage stützen können. Als Vormund hat sie nach § 1793 Abs. 1 BGB das Recht und die Pflicht, für den Jugendlichen zu sorgen, insbesondere ihn zu vertreten. Daher kann sie für diesen wirksam eine Einwilligung erteilen. Da es sich um Gesundheitsdaten handelt, muss sie ausdrücklich einwilligen. Die Schule darf die Daten verarbeiten, allerdings nur für den Zweck, für den sie erhoben wurden (medizinische Notfälle im Rahmen der Klassenfahrt). Mitschüler_innen oder andere Personen dürfen nicht informiert werden. Die Jugendamtsmitarbeiterin kann die Einwilligung jederzeit widerrufen.

[46] *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO Art. 9 Rn. 43.
[47] *Albers/Veit*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO Art. 9 Rn. 43.
[48] Die Norm hat keinen normativen Eigenwert, *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, BDSG § 22 Rn. 6.

3.5. Informationspflichten

Den Verantwortlichen treffen nach Art. 12 ff. DS-GVO zahlreiche Informationspflichten, denen dieser in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren Sprache“ nachkommen muss.

Die betroffene Person muss, in der Regel durch schriftliche oder elektronische Hinweise zum Datenschutz, über die Verarbeitung informiert werden. Um die betroffene Person ausreichend über den Umgang mit ihren Daten in Kenntnis zu setzen, müssen die Informationen so aufbereitet und die organisatorischen Abläufe des Verantwortlichen so gestaltet sein, dass unter normalen Umständen eine Kenntnisnahme erfolgen kann.

> **Beispiel:**
> Werden der betroffenen Person bspw. in einer Arztpraxis mehrere Seiten eng bedruckter Datenschutzhinweise ausgehändigt, die nur mit einer Lupe zu lesen sind, während das Praxispersonal drängelt, die Kenntnisnahme durch eine Unterschrift zu bestätigen, dürfte einsichtig sein, dass der Verantwortliche seiner Verpflichtung nicht gerecht wird.

Der Umfang der erforderlichen Informationen richtet sich danach, ob die Daten bei der betroffenen Person erhoben werden oder nicht. Werden personenbezogene Daten betroffenen Person erhoben, so teilt der Verantwortliche ihr zum Zeitpunkt der Erhebung die in Art. 13 Abs. 1 und ggf. Abs. 2 und 3 DS-GVO genannten Informationen mit, darunter die Kontaktdaten, den Zweck der Verarbeitung und die Rechtsgrundlage. Werden die Daten nicht bei der betroffenen Person erhoben, ist die Information nach Art. 14 DS-GVO vorzunehmen.

Eine Verletzung von Informationspflichten hat zur Folge, dass die Datenverarbeitung nicht rechtmäßig ist. Die betroffene Person kann sich in diesem Falle an die Aufsichtsbehörde wenden oder nach Art. 79 DS-GVO sogar unmittelbar gerichtlich gegen den Verantwortlichen vorgehen.

4. Prüfung datenschutzrechtlicher Vorgänge

Für die Prüfung eines datenschutzrechtlichen Sachverhalts ist ein schrittweises Vorgehen erforderlich (→ Siehe Checkliste). Zunächst ist zu überlegen, welches Gesetz heranzuziehen ist, bevor die zu prüfenden Normen ausgewählt werden kann.

In einem ersten Schritt ist zu prüfen, ob eine Verarbeitung personenbezogener Daten stattfindet und wer für die Verarbeitung verantwortlich ist.

Als zweiter Schritt folgt die Auswahl der gesetzlichen Grundlage der Verarbeitung. Steht eine Offenbarung von Privatgeheimnissen im Raum, ist an § 203 StGB zu denken. Im Übrigen ist der Anwendungsbereich der DS-GVO in den Blick zu nehmen.

Ist die DS-GVO nicht anwendbar, kommt eine Verletzung des allgemeinen Persönlichkeitsrechts in Betracht. Fällt die Verarbeitung unter die DS-GVO, sind die in dieser Checkliste geregelten Voraussetzungen zu prüfen.

Ausgehend von dem Zweck der Datenverarbeitung ist zu fragen, auf welche Rechtsgrundlage sie gestützt werden kann, ob die Datenschutzgrundsätze des Art. 5 DS-GVO eingehalten sind und ob die betroffene Person ausreichend über die Verarbeitung informiert wurde.

4.1 Checkliste

Prüfung von Datenschutzvorgängen nach der DS-GVO

1. **Werden personenbezogene Daten verarbeitet?**
   Ansprüche können nur dann geltend gemacht werden, wenn ein Personenbezug besteht, es reicht eine Identifizierbarkeit,
2. **Wer ist die betroffene Person?**
   Die betroffene Person oder ihr gesetzlicher Vertreter können eine Einhaltung des Datenschutzes verlangen, nicht aber Dritte.
3. **Welche gesetzliche Grundlage ist heranzuziehen?**
   1. **Ist die Datenschutzgrundverordnung anwendbar?**
      Der Sachverhalt muss in den sachlichen und räumlichen Anwendungsbereich gemäß Art. 4 DS-GVO fallen, insbesondere:
      1. **Ganz oder teilweise automatisierte Datenverarbeitung oder Speicherung in einem Dateisystem?**
      2. **Keine Verarbeitung ausschließlich zu persönlichen oder familiären Zwecken?**
      3. **Keine anderweitige Ausnahme?**
         z.B. Verarbeitung durch die Polizei oder die Justiz.
   2. **Falls nein: Welche andere Rechtsgrundlage kommt in Betracht?**
4. **Welchem Zweck dient die Datenverarbeitung?**
   z.B. Übermittlung von Daten zur Abwehr von Gefahren.
5. **Auf welche Rechtsgrundlage kann die Verarbeitung gestützt werden?**
   1. **Handelt es sich um besondere Kategorien von Daten?**
      In diesem Fall ist Art. 9 DS-GVO anzuwenden.
   2. **Handelt es sich um sonstige personenbezogene Daten?**
      Die Rechtmäßigkeit der Verarbeitung richtet sich nach Art. 6 DS-GVO.
6. **Sind die Datenschutzgrundsätze eingehalten?**
7. **Wurden die Anforderungen an die transparente Information nach den Art. 12 ff. DS-GVO beachtet?**

5. Betroffenenrechte

Jede betroffene Person kann gegen den Verantwortlichen eine Vielzahl von Rechten geltend machen. Im Folgenden werden die Betroffenenrechte behandelt, die bei Datenschutzfällen im Zusammenhang mit HIV von Relevanz sein können.

Der betroffenen Person steht nach Art. 15 DS-GVO ein Recht auf Auskunft zu. Es umfasst nicht nur den Umstand, ob Daten verarbeitet werden, sondern u.a. auch die Verarbeitungszwecke, die Kategorien der Daten und die Empfänger von Übermittlungen.

Das Recht auf Berichtigung nach Art. 16 DS-GVO soll die Verarbeitung unrichtiger Daten verhindern. Die betroffene Person kann von dem Verantwortlichen verlangen, dass dieser vorhandene Daten berichtigt, wozu auch eine Vervollständigung gehören kann[49].

Nach Art. 21 DS-GVO kann eine betroffene Person der Verarbeitung ihrer Daten jederzeit widersprechen, wenn sie auf die Rechtsgrundlage des Art. 6 Abs. 1 Buchst. e) oder f) DS-GVO gestützt wird. Sie muss dazu Gründe vorbringen, die sich aus seiner „besonderen Situation" ergeben. Überwiegen diese individuellen Gründe die Interessen des Verantwortlichen, darf dieser die Daten in Folge des Widerspruchs nicht mehr verarbeiten.

Der Verantwortliche muss von ihm verarbeitete Daten nach Art. 17 DS-GVO unverzüglich löschen, wenn ein Löschungsgrund vorliegt. Gründe für eine Löschung sind in Art. 17 Abs. 1 DS-GVO benannt, insbesondere:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig;
- die betroffene Person widerruft ihre Einwilligung und es fehlt an einer anderen Rechtsgrundlage für die Verarbeitung;
- die betroffene Person legt einen Widerspruch nach Art. 21 DS-GVO ein und ihre Interessen überwiegen die des Verantwortlichen;
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

Das „Recht auf Vergessenwerden" ergänzt den Löschungsanspruch dahingehend, dass der Verantwortliche, wenn Daten von ihm veröffentlicht wurden, z.B. auf einer Webseite, andere Verantwortliche auf den Löschungsantrag hinweisen muss. Bei einer Veröffentlichung im Internet betrifft dies unter anderem Suchmaschinen und Archive.

Die betroffene Person hat unter bestimmten Voraussetzungen nach Art. 18 DS-GVO das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen. Dies wird dann der Fall sein, wenn eine Löschung oder Berichtigung nicht möglich ist. Auch wenn zwischen der betroffenen Person und dem Verantwortlichen keine Einigkeit besteht, ob eine solche vorzunehmen ist, muss die Verarbeitung eingeschränkt werden.

Für die Geltendmachung der Betroffenenrechte nach den Art. 15 bis 21 DS-GVO wird zumeist ein Nachweis über die Identität der betroffenen Person gefordert werden können, um sicherzustellen,

[49] *Worms*, in: Wolff/Brink, BeckOK Datenschutzrecht, DS-GVO, Art. 16 Rn. 57.

dass nicht Daten an Unbefugte herausgegeben werden. Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, kann er die Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Über die genannten Rechte hinaus kann sich die betroffene Person jederzeit an die zuständige Aufsichtsbehörde wenden, um den Verantwortlichen zu einer rechtmäßigen Datenverarbeitung anzuhalten. Die Aufsichtsbehörden, in Deutschland die jeweiligen Landesbeauftragten für den Datenschutz, haben ein umfangreiches Instrumentarium zur Verfügung, um Verstößen nachgehen zu können.

Flankierend zu der Möglichkeit, die Behörden einzuschalten, eröffnet Art. 79 DS-GVO den Rechtsweg, wenn Daten nicht im Einklang mit der Verordnung verarbeitet werden und dadurch Rechte der betroffenen Person verletzt wurden. Diese Rechte können im Falle, dass eine weitere Rechtsverletzung droht, auch im Wege eines Unterlassungsanspruchs für die Zukunft verfolgt werden[50].

Art. 82 DS-GVO regelt schließlich, dass bei Verstößen gegen die Verordnung sowohl materielle als auch immaterielle Schäden geltend gemacht werden können. Das heißt, dass nicht nur konkrete (finanzielle) Nachteile von dem Verletzer auszugleichen sind, sondern darüber hinaus auch ein „Schmerzensgeld“ für die mit der Datenschutzverletzung verbundenen Belastungen in Betracht kommt. Damit hat die DS-GVO die Möglichkeiten einer finanziellen Kompensation bei Verletzungen des Datenschutzes erweitert. Bisher haben die Gerichte einen immateriellen Schaden nur bei schwerwiegenden Verletzungen anerkannt.

[50]OLG Frankfurt am Main, GRUR 2018, 1283 (1285); OLG Dresden, ZD 2019, 172 (173 f.); LG Frankfurt am Main, Urteil vom 28.06.2019 – 2-03 O 315/17.

6. Vorgehen bei Datenschutzverletzungen

Wie ist vorzugehen, wenn eine Datenschutzverletzung im Raum steht? Zunächst sollte gemeinsam mit der Klientin/dem Klienten herausgearbeitet werden, welches Ziel mit einem weiteren Vorgehen erreicht werden soll. Denn von der Beantwortung dieser Frage hängt es maßgeblich ab, welche weiteren Schritte überhaupt in Betracht kommen und wie auf den Verletzer zugegangen werden sollte. Geht es darum, weitere Rechtsverletzungen zu verhindern, wird gegenüber dem Verantwortlichen anders aufzutreten sein, als wenn es um Genugtuung durch ein Eingeständnis des Fehlverhaltens geht.

Ist das Ziel definiert, stehen in einem zweiten Schritt die weitere Aufklärung des Sachverhalts und eine erste Bewertung der Rechtslage an. Auf der Grundlage der Schilderung der betroffenen Person und etwaiger weiterer vorhandene Unterlagen sollte anhand der Checkliste (→ Siehe Checkliste) eine Voreinschätzung vorgenommen werden. Sind akut weitere Datenschutzverletzungen zu erwarten oder kommt ein Schadensersatzanspruch in Betracht, ist die Hinzuziehung einer anwaltlichen Unterstützung zu empfehlen.

Kommt eine Verletzung des Datenschutzes in Betracht, ist mit dem Verantwortlichen in Kontakt zu treten. Zuvor sollte überlegt werden, ob anwaltlicher Rat eingeholt werden sollte. Insbesondere wenn weitere Nachteile zu befürchten sind, sollte dies geschehen. Dabei sollte nicht zu viel Zeit verloren gehen, denn die Gerichte gehen davon aus, dass eine einstweilige Verfügung zeitnah nach Kenntnis der anspruchsbegründenden Tatsachen beantragt werden muss. Wer mehr als einen Monat abwartet oder sich vertrösten lässt, läuft daher Gefahr, seine Rechte nicht effektiv durchsetzen zu können.

Falls bei dem Verantwortlichen ein betrieblicher Datenschutzbeauftragter bestellt ist, könnte (auch) dieser angesprochen werden. Der Datenschutzbeauftragte ist nach Art. 39 DS-GVO unter anderem dafür zuständig, die Einhaltung der Datenschutzvorschriften zu überwachen und sollte aus diesem Grunde über eine gewisse Sensibilität in Datenschutzfragen verfügen. In der Kommunikation mit dem Verantwortlichen kann ein Hinweis auf die Möglichkeit, die zuständige Aufsichtsbehörde einzuschalten, die Gesprächsbereitschaft erhöhen.

Die Aufsichtsbehörde von einem Vorgang in Kenntnis zu setzen bietet sich an, wenn die Kommunikation mit dem Verantwortlichen nicht zu befriedigenden Ergebnissen führt. Denn die Behörde hat weitreichende Befugnisse gegenüber dem Verantwortlichen bis hin zu einer Überprüfung vor Ort. Sie kann den Sachverhalt eingehend auf eine Verletzung des Datenschutzes hin untersuchen, den Verantwortlichen treffen dabei Mitwirkungspflichten. Bei strukturellen Mängeln, z.B. im Krankenhausbetrieb, kann die Aufsichtsbehörde auf eine künftige Einhaltung des Datenschutzes hinwirken. Nicht zuletzt kann die Aufsichtsbehörde ggf. empfindliche Bußgelder verhängen, insbesondere wenn der Verantwortliche seiner Pflicht zur Gewährleistung eines angemessenen Datenschutzes nicht nachkommt.

Im **Fall 1** (gelber Punkt) sollte der Datenschutzbeauftragte des Krankenhauses eingeschaltet und für die Problematik sensibilisiert werden. In Betracht kommt zudem ein Anspruch auf ein „Schmerzensgeld“, der ggf. gegenüber dem Krankenhaus geltend zu machen wäre. Dieser Anspruch kann auch in Ansatz gebracht werden, um die Verantwortlichen zu einer Änderung ihres Verhaltens zu motivieren.

Ein Vorgehen im **Fall 3** (WhatsApp-Nachricht) könnte wie folgt aussehen: Zur Verhinderung weiterer Datenübermittlungen durch die Ex-Ehefrau, könnte sie durch einen Rechtsanwalt dazu aufgefordert werden, ein solches Verhalten künftig zu unterlassen. Dies kann durch die Abgabe einer strafbewehrten Unterlassungserklärung abgesichert werden. Sollte eine solche nicht abgegeben werden, kann bei Gericht eine einstweilige Verfügung beantragt werden. In Betracht kommt zudem ein Anspruch auf Schadensersatz, der sowohl Ersatz erlittener materieller Schäden (z.B. Anwaltskosten) als auch Schmerzensgeld umfasst. Der Arbeitgeber sollte zur Auskunft über durch ihn verarbeitete Daten und zur Löschung aufgefordert werden. Ggf. sollte die Aufsichtsbehörde angeschrieben werden, um sicherzustellen, dass eine Löschung der Daten auch tatsächlich erfolgt.