10 Datenminimierung

Wissenschaftliche Forschung zielt regelmäßig auf das **Erkennen von allgemeinen Gesetzmäßigkeiten**, nicht auf die Beschreibung einer bestimmten Person. Das Forschungsergebnis soll möglichst vom Einzelfall unabhängig sein, d.h. anonym und verallgemeinerungsfähig.

Kein datenschutzrechtlicher Eingriff ist gegeben, wenn vor der Erhebung oder der Weitergabe personenbezogener Daten an die Forschungsstelle eine **Anonymisierung** erfolgt. Erfolgte eine personenbezogene Erhebung, so sind zum frühestmöglichen Zeitpunkt Maßnahmen zur Datenminimierung zu ergreifen (Art. 5 Abs. 1 lit. c DSGVO).

Gemäß Art. 89 Abs. 1, 2 DSGVO ist die Privilegierung der Datenverarbeitung für Forschungszwecke vom Bestehen bestimmter **geeigneter Bedingungen und Garantien** abhängig. Über diese Garantien soll ein Ausgleich zwischen den tangierten Grundrechten, insbesondere der Forschungsfreiheit und dem Grundrecht auf Datenschutz, hergestellt werden. Art. 89 Abs. 1 S. 2–4 DSGVO nennt als vorrangige Garantie *„die Achtung des Grundsatzes der Datenminimierung"*. Prominent wird die Pseudonymisierung genannt, *„sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen"*.

Eine Verbesserung des kontrollierten Zugangs zu ursprünglich personenbezogenen Daten kann durch die Entwicklung von **Verfahren und Standards** der Anonymisierung und der Pseudonymisierung erreicht werden, die geeignete Betroffenengarantien sicherstellen.[591]

591 Datenethikkommission, 21 (These 20), zu den Methoden 129ff.; Health Ethics Policy Lab, 74, 78.

10.1 Biomaterial und Personenbezug

Für die Anwendung des Datenschutzrechtes ist Voraussetzung, dass die personenbezogenen Daten *„in einem Dateisystem gespeichert sind oder gespeichert werden sollen"* (Art. 2 Abs. 1 DSGVO). Was ein **Dateisystem** ist, wird in Art. 4 Nr. 6 DSGVO definiert:

> *„[…] jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird."*

Biomaterialproben sind durch biotechnische Verfahren analysierbar. Die darin enthaltenen Daten sind geordnet und strukturiert erfassbar. Zwar fehlt es für die Annahme eines Dateisystems bei reinen Proben daran, dass es für deren Analyse zusätzlicher technischer Verfahren bedarf.[592] Doch genügt es für die Anwendung der DSGVO, dass die Verarbeitung **in einem Dateisystem geplant** ist. Diese Voraussetzung ist bei Biomaterialproben gegeben, die für Zwecke der Forschung genutzt werden sollen. Es kommt insofern darauf an, zu welchem Zeitpunkt die Entscheidung getroffen wird, dass Biomaterial analysiert und dateimäßig gespeichert werden soll. Ein zielgerichtetes Verhalten ist nicht erforderlich. Es genügt die Aussicht, dass die Daten in ein Dateisystem aufgenommen werden, dass nach den Umständen und der Lebenserfahrung im Regelfall mit einer Aufnahme in ein Dateisystem zu rechnen ist.[593] Die Art des Speichermediums ist unerheblich. Die DSGVO ist darauf angelegt, so weit wie möglich technologieneutral zu sein (ErwGr 15 S. 1). Als Datenträger kommen auch Biomaterialien in Betracht.[594]

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO Informationen einer **identifizierten oder identifizierbaren natürlichen Person** – des Betroffenen. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.

Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden können, sollen **alle objektiven Faktoren**, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (ErwGr 26 S. 4). Subjektive Faktoren, also z. B. die Motivation oder Intention, sich die Mittel zur Identifizierung zu verschaffen, sind unbeachtlich.[595] Für den Schutzzweck nach der DSGVO kommt es also nicht darauf an, wann ein Datenträger unter welchen Umständen entstanden ist. Relevant ist ausschließlich, dass personenbezogene Daten verarbeitet werden. Der Personenbezug kann somit vom **aktuellen technischen Stand** der Verarbeitungsmöglichkeiten abhängen.[596]

592 Weichert in DWWS, Art. 4 Rn. 84.
593 Roßnagel in SHS, Art. 2 Rn. 16; Dammann/Simitis, Art. 3 Rn. 5; Weichert in DWWS, Art. 2 Rn. 13.
594 Weichert DuD 2002, 134; Weichert in DKWW, § 3 Rn. 16.
595 Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 23.
596 Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 24.

Identifizierbarkeit ist weit auszulegen. Es muss kein direkter Personenbezug bestehen; es genügt, wenn dieser, u.U. über mehrere Zwischenschritte, hergestellt werden kann. Das ist der Fall, wenn im Umfeld der verantwortlichen Stelle Zusatzwissen vorhanden ist, das abgefragt werden könnte. Verfügt die speichernde Stelle nicht über die Zuordnungsmöglichkeit zu einem Pseudonym (s.u. Kap. 10.2), wohl aber eine andere Stelle, sind die pseudonymisierten Daten personenbezogen, wenn es nicht völlig unrealistisch ist, dass die andere Stelle ihre Kenntnisse zur Verfügung stellt. Die Möglichkeiten der Zuordnung **von Datenbeständen** zwecks Identifizierung nehmen mit der technischen Entwicklung immer weiter zu. Ein Personenbezug wird nur dann nicht angenommen, wenn Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeit einer natürlichen Person zugeordnet werden können und damit als anonym behandelt werden können (ErwGr 26 S. 5). Eine Rechtsänderung hat sich insofern mit der DSGVO nicht ergeben, wohl aber eine gewisse Klärung.

Sind von Altproben keine direkt identifizierenden Daten einzelner Personen mehr greifbar oder gespeichert, so kommt es für die Frage der Anwendbarkeit des Datenschutzrechts darauf an, wie groß der Aufwand ist, um eine Identifizierung vorzunehmen. Nach dem Willen des Gesetzgebers soll relevant sein, ob der Einsatz der Mittel zur Identifizierung nach ***„allgemeinem Ermessen wahrscheinlich"*** ist (ErwGr 26 S. 4). Daraus lässt sich ableiten, dass das Wissen eines beliebigen Dritten bzw. das gesamte „Weltwissen" nicht zugrunde gelegt werden können.[597] Es ist aber auch nicht nötig, dass die Individualisierung aufgrund einer Informationsquelle tatsächlich erfolgt. Entscheidend ist, über welches Zusatzwissen der Verantwortliche verfügen könnte.[598] Berücksichtigt werden müssen auch Informationen aus unterschiedlichen Quellen, die in ihrem Zusammenspiel die Identifizierung ermöglichen.[599]

Waren also Biomaterialproben nach früherer Ansicht als anonym anzusehen und haben sich inzwischen die **technischen Möglichkeiten weiterentwickelt**, sodass Biomaterialproben einer natürlichen Person zugeordnet werden können, dann sind diese als personenbezogen anzusehen mit der Folge, dass die DSGVO sowie das BDSG zur Anwendung kommen. Damit sind sie aber der Forschung nicht entzogen. Vielmehr kommt dann die Privilegierung für Forschungszwecke zur Anwendung mit der Folge, dass eine Weiternutzung erlaubt ist, wenn geeignete Garantien nach Art. 89 Abs. 1 DSGVO bestehen (s.o. Kap. 9). Geeignete Maßnahmen können auch solche einer weitergehenden Datenminimierung sein (s. in vorliegendem Kapitel).

Entsprechendes gilt, wenn Biomaterialproben aus einem Land stammen, in dem nach dem dort geltenden Recht ein **weiteres Verständnis von Anonymität** gilt und die Proben in Europa verarbeitet werden (s.u. Kap. 13.6).

Dies hat zur Folge, dass eindeutig identifizierende biometrische Merkmale, wie sie bei genetisch analysierbaren Biomaterialproben erlangt werden können, grundsätzlich zu einem Personenbezug führen, da z.B. über den genetischen Code generell eine Zuordnung zu einer natürlichen Person möglich ist.[600] Durch die weltweite Verfügbarkeit von genetischen Zuordnungsmöglichkeiten eröffnen sich in immer stärkerem

597 Klar/Kühling in Kühling/Buchner, Art. 4 Nr. 1 Rn. 24; weitergehend Klabunde in Ehmann/Selmayr, Art. 4 Rn. 17.
598 Mit ausführlicher Herleitung Roßnagel/Geminn in Dierks/Roßnagel, 157ff.
599 Karg in SHS, Art. 4 Nr. 1 Rn. 52.
600 So Karg in SHS, Art. 4 Nr. 1 Rn. 71.

Maße die Möglichkeiten zur Identifizierung eines Probengebers. Kein Personenbezug ist anzunehmen, wenn im konkreten Fall die **Identifizierung sehr unwahrscheinlich** ist.

10.2 Anonymisierung

Am wirksamsten wird die Datenminimierung durch Anonymisierung umgesetzt (ErwGr 26). Diese führt dazu, dass ein **Personenbezug vollständig beseitigt** wird und dann keine weiteren datenschutzrechtlichen Restriktionen bei der Verarbeitung beachtet werden müssen. Anonymisieren bedeutet das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (s.o. Kap. 10.1).[601]

Anders als zur Pseudonymisierung (s.u. Kap. 10.3) wird der Begriff der Anonymisierung im Normtext der **DSGVO** nicht verwendet oder definiert.[602] auf. In ErwGr 26 S. 5, 6 DSGVO wird im Rahmen der Definition von „personenbezogene Daten" darauf hingewiesen, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten, also *„für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke."*

Anonymisierung wird vereinzelt im allgemeinen deutschen Datenschutzrecht in den Forschungsklauseln definiert.[603] Eine explizite **Anonymisierungspflicht**, „sobald dies nach dem Forschungszweck möglich ist", gilt teilweise für alle Forschungsdaten,[604] teilweise explizit nur für solche sensitiven Daten.[605] Auf Bundesebene gilt § 27 Abs. 3 S. 1 **BDSG**:

> *„Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert."*

601 So § 3 Abs. 6 BDSGaF.
602 Hansen in SHS, Art. 4 Nr. 5 Rn. 11; Roßnagel/Geminn in Dierks/Roßnagel, 166; Weichert in DWWS, Art. 4 Rn. 74.
603 § 9 Abs. 2 S. 1 DSG M-V, § 28 Abs. 3 S. 1 ThürDSG, dazu Weichert in DWWS § 27 Rn. 28f.
604 Art. 25 Abs. 2 S. 1 BayDSG, § 25 Abs. 2 S. 1 BbgDSG, § 9 Abs. 2 S. 1 DSG M–V, § 13 Abs. 2 S. 1 NDSG, § 17 Abs. 3 S. 1 DSG NRW, § 23 Abs. 1 S. 2 DSG Saar, § 13 Abs. 2 S. 1 LDSG SH, § 28 Abs. 3 S. 1 ThürDSG.
605 § 27 Abs. 2 S. 1 BDSG, § 13 Abs. 2 S. 1 LDSG BW, § 24 Abs. 3 S. 1 HDSIG, § 17 Abs. 2 S. 2 DSG NRW, § 22 Abs. 4 S. 1 LDSG RP.

Das Anonymisieren von personenbezogenen Daten ist als eine **besondere Form der Datenverarbeitung** anzusehen und bedarf daher einer rechtlichen Grundlage.[606] Diese kann in der Einwilligung des Betroffenen erfolgen. Bei einer Anonymisierung, die das Ziel verfolgt, mit den anonymisierten Daten einen anderen Zweck, etwa Forschungszwecke, zu verfolgen, liegt die Rechtsgrundlage in der ursprünglichen Rechtsgrundlage in Verbindung mit Art. 6 Abs. 4 DSGVO.[607]

Eine Forschungsverarbeitung von personenbezogenen Daten ist unzulässig, wenn deren Zweck mit anonymen Daten erreicht werden kann.[608] Die **Erforderlichkeit einer personenbeziehbaren Verarbeitung** ist zu dokumentieren.[609]

Ob eine Anonymisierung wirksam ist, hängt von den Erkenntnisquellen ab, die der speichernden Stelle als **Zusatzwissen** zur personenbezogenen Zuordnung direkt oder indirekt zur Verfügung stehen bzw. stehen können.[610] Für die **Verfügbarkeit des Zusatzwissens** genügt die theoretische Möglichkeit. Relevant ist, ob das Zusatzwissen vernünftigerweise bei einer Einheit der verarbeitenden Stelle verfügbar sein kann.[611] Nicht beachtlich ist, dass diese Möglichkeit nicht in Anspruch genommen werden soll oder will (s.o. Kap. 10.1). Oft genügen einige Merkmalsdaten, um eine Zuordnung von Datensätzen zu konkreten Personen zu ermöglichen, selbst wenn deren Stammdaten gelöscht sind.[612] Eine absolute Anonymisierung ist bei hochkomplexen und umfangreichen Datensätzen zumeist praktisch nicht möglich. Wenn das Zusatzwissen nur unter einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft beschafft werden kann, genügt dies für die Anonymisierung. Es ist ein objektiver Maßstab anzulegen; nicht beachtlich ist, wenn der Aufwand nur für die speichernde Stelle unverhältnismäßig ist; auch das Interesse der Stelle ist nicht erheblich.[613]

Bei einer Vielzahl von Datenkategorien, die insbesondere im medizinischen Forschungsbereich von Relevanz sind, ist eine **vollständige Anonymisierung nicht möglich**.[614] Auf eine Anonymisierung kann verzichtet werden, wenn dies für eine privilegierte Zweckverfolgung gem. Art. 9 Abs. 2 DSGVO zwingend erforderlich ist. Dies muss einschränkend in die Regelung mit hineingelesen werden.[615] Eine personen-

606 Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 8.

607 BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 20.06.2020, 6ff. m.w.N; gemäß S. 8f. ist bei einer Pflicht zur Löschung die Rechtsgrundlage Art. 6 Abs. 1 i.V.m. Art. 17 Abs. 1 DSGVO.

608 Roßnagel in SHS, Art. 5 Rn. 108; Golla in Specht/Mantz, § 23 Rn. 29, 48, 53; Albrecht/Jotzo, Teil 3 Rn. 74; Paal/Pauly, Art. 89 Rn. 12; Johannes in Roßnagel 2017, § 4 Rn. 93.

609 Werkmeister/Schwaab CR 2019, 86; zur Erforderlichkeit generell Graf von Kielmansegg in TMF, 104ff.

610 Anders noch BFH, NJW 1994, 2247 = RDV 1995, 32, der meinte, dass Re-Identifizierung durch Branchenkenntnisse für eine Behandlung von Daten unschädlich ist.

611 Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 10; Dierks in Dierks/Roßnagel, 29f.; zu einem „modifizierten Verständnis der Anonymisierung S. 30ff. m.w.N., wobei es sich dabei um eine Pseudonymisierung handelt. Die Anonymisierungspflicht in § 287 Abs. 2 SGB V muss in europarechtskonformer Auslegung als Pseudonymisierungspflicht verstanden werden.

612 Hurtz, Von wegen anonym, SZ 29.07.2019, 1 mit Verweis auf Rocher/Hendrickx/de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications Vol. 10, Art. Nr. 3069 (2019), Kauß (Fn. 56), 594ff.

613 Roßnagel/Geminn in Dierks/Roßnagel, 164–167; Kühling/Buchner/Klar, Art. 4 Nr. 1 Rn. 32; Weichert in DWWS, Art. 4 Rn. 75; Schaar ZD 2016, 225; a.A. Gola/Schomerus, § 3 Rn. 44; Gola in Gola, Art. 2 Rn. 11.

614 Schaar ZD 2016, 225; Riechert DANA 2019, 211; Weichert in Kühling/Buchner, Art. 4 Nr. 13 Rn. 5 m.w.N.; zu den Methoden Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 13ff.

615 A.A. Johannes/Richter, DuD 2017, 304, die darin eine Verordnungswidrigkeit der Regelung sehen.

beziehbare Verarbeitung kann z.B. erforderlich sein zum Schutz lebenswichtiger Interessen des Betroffenen (Art. 9 Abs. 2 lit. c DSGVO).[616] Eine wirksame Anonymisierung ist oft bei Biomaterialproben, Bilddaten oder Stimmaufnahmen nicht möglich. Ist eine vollständige Anonymisierung nicht möglich oder auch nicht gewünscht, weil z.B. eine spätere Zuordnung von Datensätzen erfolgen muss, hat eine **Pseudonymisierung** zu erfolgen (s.u. Kap. 10.2).

Bei der Pflicht zur Anonymisierung und Pseudonymisierung müssen nicht sämtliche hierfür bestehenden Mittel eingesetzt werden, sondern nur solche, die dem aktuellen **Stand der Technik** entsprechen. Sind die Methoden der Datenminimierung für den Forscher nicht zugänglich und ist ihm deren Einsatz nicht zuzumuten, so kann der Einsatz dieser Methoden auch nicht gefordert werden.[617]

Mit einer Anonymisierung kann ein forschungsrelevanter **Informationsverlust** verbunden sein. Dies gilt z.B. für eine Aggregierung von Datensätzen, bei der Einzelangaben zusammengeführt werden (sog. K-Anonymität). Auch bei anderen Methoden der Anonymisierung, etwa der Verschleierung, der Merkmalsaggregierung, durch das gezielte Einführen von Merkmalsfehlern (z.B. Hinzufügung von Dummy-Datensätzen) oder das Vertauschen von Daten[618] können Inhaltsverluste entstehen, die die Wertigkeit des Forschungsergebnisses beeinträchtigen können.[619]

Von einer Anonymisierung kann abgesehen werden, wenn berechtigte **Interessen der betroffenen Personen** dies erfordern. Dies kann dann der Fall sein, wenn der Betroffene ein individuelles Interesse an den Resultaten hat, die z.B. im medizinischen Bereich in eine Behandlung einfließen sollen. Ein Betroffeneninteresse kann auch darin bestehen, dass die Rechtmäßigkeit der Verarbeitung zur eigenen Person überprüft werden soll. In solchen Fällen ist regelmäßig eine Pseudonymisierung mit File-Trennung angezeigt.

10.3 Pseudonymisierung

Um Inhaltsverluste zu vermeiden, wird bei Forschungsprojekten anstelle einer Anonymisierung oft die **Pseudonymisierung** gewählt. Diese Datenveränderung im Interesse der Datenminimierung wird in Art. 4 Nr. 5 DSGVO definiert. Danach ist

„Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden."[620]

616 Johannes/Richter, DuD 2017, 304.
617 Weichert in DWWS, § 27 BDSG Rn. 31.
618 Wiebe 534; 23. TB LDI NRW 2017, Kap. 13.2 (S. 100); zur sog. K-Anonymität 23. TB LDI NRW 2017, Kap. 13.2 (S. 100); Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 19ff.
619 Weichert in DWWS, Art. 4 Rn. 77; Schäfer in Kipker/Voskamp, 343ff.
620 Zur Begriffsdefinition und zu den Unterschieden zwischen Art. 4 Nr. 5 und ErwGr 26, S. 2 DSGVO Roßnagel/Geminn in Dierks/Roßnagel, 175ff.

Die Pseudonymisierung wird sowohl in der DSGVO (Art. 6 Abs. 4 lit. e, 25 Abs. 1, 32 Abs. 1 lit. a, 40 Abs. 2 lit. d, 89 Abs. 1 S. 3)[621] als auch im BDSG (§ 22 Abs. 2 Nr. 6) als eine wichtige Garantiemaßnahme aufgeführt.[622] Wegen der Definition in der DSGVO verzichtet das deutsche Datenschutzrecht auf eine eigene Begriffsbestimmung. Ist eine Pseudonymisierung möglich, ohne dass die Erreichung des Forschungszwecks beeinträchtigt wird, so muss sie – als Ergebnis der Risikobewertung – grundsätzlich auch vorgenommen werden.[623] Eine gängige Form der Pseudonymisierung bei Forschungsprojekten besteht darin, dass die eine natürliche Person identifizierenden Daten (Stammdaten) durch ein per **Zuordnungsfunktion** definiertes Merkmal (Pseudonym) ersetzt werden und bei der Auswertung für Forschungszwecke statt der Stammdaten ausschließlich das Pseudonym verwendet wird.

Eine **Pseudonymisierung von Einzeldatensätzen** ermöglicht bei Langzeitstudien das Verfolgen von Einzelfällen. Mit dieser Methode können auch Daten zu einer Person aus unterschiedlichen Quellen zu unterschiedlichen Zeiten in einem geschützten Raum verarbeitet werden. Der Einsatz von Pseudonymen mit der Möglichkeit der Reidentifizierung von Einzelfällen ist dann geboten, wenn Forschungsergebnisse, z.B. bei medizinischen Spätfolgen, im Nachhinein überprüft werden können müssen. Durch die Pseudonymisierung soll ermöglicht werden, dass trotz Verzicht auf einen direkten Personenbezug keine falschen Datensatzzuordnungen und Verwechslungen erfolgen.

Pseudonymisierung gemäß der DSGVO muss ein bestimmtes Maß an **Qualität** vorweisen.[624] Soll die Pseudonymisierung eine Zuordnung für Dritte ausschließen, sodass sie für diese als anonym behandelt werden können, dann muss eine Identifizierung der Betroffenen für diese nach allgemeinem Ermessen ausgeschlossen sein. Dabei ist neben dem Ersetzen der identifizierenden Daten darauf zu achten, dass mit den Merkmalsdaten im Datensatz keine Reidentifizierung durch den Dritten möglich ist.[625] Dient dagegen die Pseudonymisierung zur Risikominimierung als Garantie für den Betroffenen, so bleiben sie für den Verantwortlichen personenbezogene Daten.[626]

Die Zuordnung der Datensätze kann technisch (z.B. Einwegverschlüsselung) oder über Pseudonymlisten vorgenommen werden. Im letztgenannten Fall sind gemäß § 27 Abs. 3 S. 3 u. 4 BDSG die **identifizierenden Angaben gesondert aufzubewahren**. Durch diese technisch-organisatorische Maßnahme soll vermieden werden, dass bei der Auswertung ein Personenbezug hergestellt wird (**File-Trennung**). Eine solche File-Trennung war im alten BDSG (§ 30a Abs. 3 S. 2) für die Markt- und Meinungsforschung vorgesehen.[627] Eine Reidentifizierung ist nur in Ausnahmefällen (wenn für Forschungszweck erforderlich, § 27 Abs. 2 S. 3 BDSG; bei Wahrnehmung von Betroffenenrechten) zulässig. Referenzlisten können beim Verantwortlichen gesondert oder bei einem Datentreuhänder (s.u. Kap. 10.4) gespeichert werden. Die Trennung erfolgt im Statistikrecht durch die Unterscheidung zwischen Hilfs- und Erhebungsmerk-

621 Roßnagel/Geminn in Dierks/Roßnagel, 174.
622 Überblick über die Landesdatenschutzgesetze bei Bernhardt/Ruhmann/Weichert, 8.
623 Johannes/Richter, DuD 2017, 302.
624 Roßnagel/Geminn in Dierks/Roßnagel, 174; Marnau DuD 2016, 430; zu den Methoden Artikel 29-Datenschutzgruppe, Stellungnahme 5/2014 v. 10.04.2014, WP 216, 24ff.
625 Roßnagel/Geminn in Dierks/Roßnagel, 182f.; Graf von Kielmansegg in TMF, 91.
626 Roßnagel/Geminn in Dierks/Roßnagel, 183f.
627 Hornung/Hofmann ZD-Beilage 4/2017, 10.

malen (vgl. § 10 BStatG). Die Trennung zwischen identifizierenden Daten und Merkmalsdaten ist in vielen Krebsregistergesetzen sowie im Arzneimittelrecht[628] gesetzlich konkretisiert. Die Identifizierungsmerkmale dürfen nur genutzt werden, soweit dies für den Forschungs- oder Statistikzweck erforderlich ist. Ist eine Individualisierung oder eine individuelle Zuordnung der Forschungsdatensätze nicht mehr nötig, sind die identifizierenden Referenzdaten zu löschen.[629]

Mit einer wirksamen Verschlüsselung oder einer Pseudonymisierung liegt keine Offenbarung von **Berufsgeheimnissen** vor, wenn die Stelle, die die Daten erhält, keine Möglichkeit zur Entschlüsselung bzw. zur Reidentifizierung hat (s.o. Kap. 6.7 am Ende).[630]

10.4 Datentreuhänderschaft u.a.

Die Pseudonyme mit den Merkmalsdaten und die Zuordnung der Pseudonyme zu den Stammdaten sind grundsätzlich getrennt zu halten (sog. **File-Trennung**). Über die Zuordnungsfunktion können die Stammdaten und das Pseudonym zusammengeführt werden (vgl. § 27 Abs. 3 S. 2 BDSG). Dadurch besteht die Möglichkeit, Datensätze aus unterschiedlichen Quellen oder aus unterschiedlichen Entstehungszeiten für Forschungszwecke ohne Namensnennung für Forschungszwecke zusammenzuführen und gemeinsam auszuwerten. Möglich ist es auch, in definierten Fällen den pseudonymisierten (Forschungs-)Datensatz wieder den Stammdaten zuzuordnen. Dies kann z.B. sinnvoll bzw. nötig sein, wenn sich aus Forschungserkenntnissen medizinische Behandlungsmöglichkeiten für eine konkrete Person ergeben und diese Daten in die Behandlung wieder eingeführt werden sollen.[631] Eine weitere Funktion eines Treuhänders bzw. einer Vertrauensstelle kann darin bestehen, Forschungsdaten treuhänderisch zu verwalten oder Einwilligungserklärungen von Betroffenen zu verwalten und deren Beachtung sicherzustellen.[632] Durch die Unabhängigkeit des Treuhänders wird gewährleistet, dass bei der Zuordnung pseudonymisierter Daten eine – idealerweise unabhängige – Drittkontrolle stattfindet.

Eine Verstärkung der Pseudonymisierungsmaßnahmen kann bei Forschungsprojekten dadurch erfolgen, dass bei **Verarbeitungsketten** für einzelne Verarbeitungsstadien (Erhebung, Speicherung, Zusammenführung, Nutzung) jeweils separate Pseudonyme genutzt werden. Dies kann notwendig sein bei hoch sensiblen Daten, die für unterschiedliche Zwecke und langfristig genutzt werden sollen, so wie dies z.B. bei Biobanken oft der Fall ist.[633]

628 Bischoff/Wiencke ZD 2019, 12.
629 Weichert in DWWS, § 27 Rn. 32.
630 Fechtner/Haßdenteufel CR 2017, 357f.; Dierks in Dierks/Roßnagel, 64; unsicher Graf von Kielmansegg in TMF, 115.
631 Weichert in DWWS, Art. 4 Rn. 67f.
632 Datenethikkommission, 127, 135; RfII, 13; Roßnagel ZD 2019, 161; Wiebe,550; Sachverständigenrat, 233f.; Martini/Hohmann NJW 2020, 3575; Metschke/Wellbrock, 44.
633 ULD, Datentreuhänderschaft in der Biobank-Forschung, Schlussbericht, Teilprojekt 2, 30.04.2009, 52ff., https://www.datenschutzzentrum.de/uploads/projekte/bdc/1-20090630-datentreuhaender-biobankenforschung-endbericht.pdf; Weichert 2018, Kap. 10.9; Wiebe, 535f.

Zu den Maßnahmen der Datenminimierung gehört es auch, dass Daten zum frühestmöglichen Zeitpunkt gelöscht oder anonymisiert werden (**Speicherbegrenzung**, Art. 5 Abs. 1 lit. e DSGVO).[634] Diese Maßnahme kommt in Betracht, wenn für Forschungszwecke von einem bestimmten Zeitpunkt an die Identifizierung von Datensätzen nicht mehr benötigt wird (Art. 89 Abs. 1 S. 4 DSGVO).[635] Eventuell genügt es, dass lediglich die Pseudonyme oder die Zuordnungsfunktionen gelöscht werden.

Mit der Einschaltung eines Treuhänders wird eine **informationelle Gewaltenteilung** erreicht. Das BVerfG hat anlässlich des Volkszählungsurteils 1983 festgestellt, dass eine solche informationelle Gewaltenteilung „unerlässlich" ist bei der Verarbeitung von Statistikdaten im kommunalen Bereich.[636] Demgemäß ist eine organisatorische Abschottung zur Wahrung der spezifischen statistischen Zweckbindung gefordert.

Diese nach nationalem Verfassungsrecht entwickelten Grundsätze lassen sich uneingeschränkt auf den europäischen Rechtsrahmen übertragen.[637] Die Notwendigkeit einer informationellen Gewaltenteilung kann auch aus der Definition der Pseudonymisierung in Art. 4 Nr. 5 DSGVO und den Grundsätzen der Datenminimierung und der Speicherbegrenzung des Art. 5 Abs. 1 lit. c und e DSGVO abgeleitet werden. Die Daten minimierende „Pseudonymisierung" erfolgt in einer Weise, *„dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden"*. Informationelle Gewaltenteilung lässt sich also durch **technisch-organisatorische Maßnahmen** umsetzen.[638]

Informationelle Gewaltenteilung kann auch **räumlich und personell** realisiert werden.[639] Die Notwendigkeit informationeller Gewaltenteilung besteht im öffentlichen wie im privaten Bereich.[640] Die allgemeinen Feststellungen gelten auch für die Umsetzung der Zweckbindung im Forschungsbereich. Es ist wünschenswert, dass insofern weitere gesetzliche Konkretisierungen erfolgen (s.u. Kap. 15.2).

Informationelle Gewaltenteilung ist von besonderer Bedeutung bei Treuhändern als Organisationsteil einer verantwortlichen Stelle, die auch die Forschung selbst durchführt. Dabei ist darauf zu achten, dass keine **Interessenkonflikte** zwischen der Treuhänderfunktion und weiteren Aufgaben bestehen. So darf der Treuhänder selbst keine Forschung mit den anvertrauten Daten durchführen.[641]

Derartige Interessenkonflikte können z.B. auch beim **Datenschutzbeauftragten** (s.u. Kap. 11.1) bestehen, dessen zentralen Aufgaben die Datenschutzkontrolle und die Beratung sind (Art. 39 DSGVO). Art. 38 Abs. 6 S. 2 DSGVO verbietet ihm die Wahr-

634 Weichert in DWWS, Art. 5 Rn. 46.
635 Siehe aber den Hinweis von Roßnagel ZD 2019, 162 auf die Notwendigkeit der Nachprüfbarkeit der Forschungsergebnisse.
636 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., Rn. 153, NJW 1984, 428.
637 Von Lewinski in Auernhammer, Einl. BDSG Rn. 38.
638 Roßnagel, Review zum vorliegenden Gutachten, 30.
639 Vgl. § 290 Abs. 2 S. 2 SGB V zur Vertrauensstelle bzgl. der Krankenversicherungsnummer sowie § 303a Abs. 2 S. 1 SGB V zur Vertrauensstelle bei der „Datentransparenz"; Weichert DANA 2020, 21f.
640 Simitis/Hornung/Spiecker in SHS, Einl. Rn. 37; Bizer, 197.
641 Böhm/Wagner CR 1997, 625.

nehmung zusätzlicher Aufgaben und Pflichten, die zu einem Interessenkonflikt führen. Zwar sind sowohl Treuhänder wie auch Datenschutzbeauftragter unabhängig hinsichtlich der konkreten Durchführung ihrer Aufgaben im Rahmen des Forschungsvorhabens. Auch dient die Unabhängigkeit in beiden Fällen der Wahrung des Datenschutzes. Doch kann ein Datenschutzbeauftragter seine gesetzlich definierten Aufgaben der Beratung und Kontrolle nicht gegenüber sich selbst wahrnehmen. Die vertraglich definierten Aufgaben des Treuhänders liegen in der von anderen Beteiligten unabhängigen Datenverarbeitung in besonders sensiblen Bereichen. Nähme er zugleich die Aufgaben des Datenschutzbeauftragten wahr, so müsste er sich in einer zentralen Rolle bei der Datenverarbeitung selbst kontrollieren.[642]

Die Benennung eines Datenschutzbeauftragten ist unter bestimmten Voraussetzungen **gesetzliche Pflicht**, insbesondere für öffentliche Stellen sowie für nicht-öffentliche Stellen, bei denen mindestens 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind, bei denen eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO Pflicht ist, sowie bei solchen, deren Kerntätigkeit die umfangreiche Verarbeitung sensitiver Daten ist (Art. 37 DSGVO, § 38 Abs. 1 BDSG, s.u. Kap. 11.1). Besteht keine solche Benennungspflicht, so steht es einer Stelle frei, einen Datenschutzbeauftragten zu benennen (Art. 37 Abs. 4 DSGVO).[643] Eine solche Benennung ist eine organisatorische Maßnahme i.S.v. Art. 89 Abs. 1 S. 2 DSGVO.[644]

Ebenso wie in Art. 38 Abs. 6 S. 1 DSGVO ist in § 7 Abs. 2 S. 1 BDSG ausdrücklich für **öffentliche Stellen des Bundes** geregelt, dass der Datenschutzbeauftragte neben seiner Funktion gemäß der DSGVO andere Aufgaben und Pflichten wahrnehmen kann. In Satz 2 wird ausdrücklich Folgendes geregelt:

> *„Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen."*

Wird ein Datenschutzbeauftragter auf **freiwilliger Basis** ernannt, so ist streitig, ob dieser die gleichen Rechte und Pflichten wie ein obligatorisch zu benennender Datenschutzbeauftragter hat.[645] Da insofern keine verpflichtende gesetzliche Regelung besteht, kann es auch keinen rechtlichen Hinderungsgrund dafür geben, die Modalitäten bei einer freiwilligen Benennung selbst zu bestimmen.[646] Dies gilt in jedem Fall für die personellen Voraussetzungen eines Datenschutzbeauftragten, wozu auch die Frage nach der Unabhängigkeit und nach möglichen Interessenkonflikten, etwa zu einer Datentreuhänderschaft, gehört.[647]

Der zwischen den Funktionen des Treuhänders und des Datenschutzbeauftragten entstehende **Interessenkonflikt kann dadurch verringert** werden, dass der Treu-

642 Allgemein dazu Däubler in DWWS, Art. 37 Rn. 19; Drewes in SHS, Art. 38 Rn. 55f.; Heberlein in Ehmann/Selmayr, Art. 38 Rn. 21; Bergt in Kühling/Buchner, Art. 38 Rn. 40; Paal in Paal/Pauly, Art. 38 Rn. 14; Raum in Auernhammer, Art. 38 Rn. 49, 52, 54ff.; Jaspers/Reif in SJTK, Art. 38 Rn. 26f.

643 Jaspers/Reif RDV 2016, 62; Däubler in DWWS, § 38 Rn. 8; Drewes in SHS, Art. 37 Rn. 37.

644 Vgl. Heberlein in Ehmann/Selmayr, Art. 37 Rn. 32, 35.

645 Dafür: Artikel 29-Datenschutzgruppe, WP 243 rev. 01 v. 0504.2017, 24; Raum in Auernhammer, Art. 37 Rn. 67; Heberlein in Ehmann/Selmayr, Art. 11, 37; Jaspers/Reif in SJTK, Art. 37 Rn. 38; unklar: Bergt in Kühling/Buchner, Art. 37 Rn. 26; differenzierend: Drewes in SHS, Art. 37 Rn. 37; dagegen: Däubler in DSSW, § 38 Rn. 8.

646 Däubler in DSSW § 38 Rn. 8.

647 Bergt in Kühling/Buchner, Art. 37 Rn. 26.

händer hinsichtlich seiner Aufgaben besonderen Rechenschaftspflichten und Kontrollen unterworfen wird. Die Art. 37–39 DSGVO sehen allerdings nicht vor, dass ein Datenschutzbeauftragter nur für Teile einer Stelle zuständig sein kann. Deshalb ist eine separate Datenschutzaufsicht des Treuhänders rechtlich nur bei einer externen Datentreuhänderschaft möglich. In seiner Treuhänderfunktion kann ein Datenschutzbeauftragter zudem nicht die gesetzliche Unabhängigkeit nach Art. 38 Abs. 3 DSGVO für sich in Anspruch nehmen.

10.5 Keine personenbezogene Veröffentlichung

Durch die Veröffentlichung der Forschungsergebnisse werden diese einem nicht mehr überschaubaren Empfängerkreis zugänglich gemacht mit der Folge, dass die Einhaltung von Zweckbindungsregelungen praktisch nicht mehr durchsetzbar ist. Da gerade im Forschungsbereich besonders hohe Anforderungen an die Zweckbindung bestehen, muss bei der Veröffentlichung grundsätzlich gewährleistet werden, dass diese **keine personenbezogenen Daten** enthält.

Dieser Grundsatz kann nicht eingehalten werden, wenn ein Forschungsvorhaben sich **auf eine konkrete Person** bezieht und der Schutz personenbezogener Daten mit dem Öffentlichkeitsgrundsatz der Forschung in Kollision gerät. Kommt es bei der Veröffentlichung nicht auf die Identität des Probanden an, so muss eine Veröffentlichung anonymisiert oder mit einer starken Pseudonymisierung erfolgen (s.o. Kap. 10.1, Kap. 10.2). Bei medizinischen Einzelfallstudien lässt sich manchmal eine auf eine natürliche Person bezogene Veröffentlichung nicht vermeiden. Die DSGVO enthält keine explizite Regelung zu dem Fall, dass eine Verschleierung der Probandenidentität im konkreten Fall nicht möglich ist. Es kann aber auf die Öffnungsklausel des Art. 85 Abs. 1 DSGVO zurückgegriffen werden, der die wissenschaftliche Kommunikation privilegiert (s.o. Kap. 4.4).[648] Dies aufgreifend regelt § 27 Abs. 4 BDSG:

> *„Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist."*

Die Forschungsklauseln der meisten Landesdatenschutzgesetze enthalten entsprechende Regelungen.[649] Entsprechendes gilt für Landeskrankenhausgesetze.[650] Einige dieser Gesetze sind offener, wenn die Veröffentlichung davon abhängig gemacht wird, dass die *„schutzwürdigen Interessen der betroffenen Person"* nicht überwiegen[651] bzw. nicht „erheblich" überwiegen.[652] Bei medizinischer Forschung geht es regelmäßig nicht um Ereignisse der Zeitgeschichte.[653]

648 Weichert in DWWS, § 27 Rn. 34.
649 § 13 Abs. 3 LDSG BW, Art. 25 Abs. 3 BayDSG, § 25 Abs. 3 BbgDSG, § 11 Abs. 3 HmbDSG, § 24 Abs. 4 HDSIG, § 9 Abs. 3 DSG M–V, § 13 Abs. 3 NDSG, § 13 Abs. 4 LDSG SH, § 28 Abs. 4 ThürDSG.
650 Dierks 2019, 62; zu den Regelungen vor Wirksamwerden der DSGVO Schneider 2015, 123ff.
651 § 17 Abs. 3 BlnDSG, § 12 Abs. 4 SächsDSDG, ähnlich § 22 Abs. 5 LDSG RP, § 23 Abs. 3 SDSG.
652 § 17 Abs. 4 DSG NRW.
653 Dazu Weichert in DWWS, § 27 Rn. 34.