1. Einleitung

Datenschutzkonformes Löschen in IT-Systemen ist auch mehr als zwei Jahre nach dem Wirksamwerden der DS-GVO ein Dauerbrenner. Die DS-GVO ordnet zwar eine Löschpflicht an und gewährt betroffenen Personen ein „Recht auf Vergessenwerden“, schweigt sich zu den Details aber aus.

In der Praxis ist das Etablieren von Löschkonzepten zur Umsetzung der Löschpflicht ein schwieriges Unterfangen:[1] Einerseits sind komplexe, z.T. über Jahrzehnte gewachsene IT-Systeme und deren Datenbestände betroffen, andererseits werden alle Fehler der Vergangenheit beim Aufbau von IT-Systemen offensichtlich. Das fortwährende Speichern personenbezogener Daten ist immer noch der Normalfall.

Anders als in Zeiten knapper Ressourcen und beschränkter Performance von IT-Systemen spielt der Mehraufwand für das Speichern und Durchsuchen auch riesiger Datenbestände in der unmittelbaren Kostenbetrachtung heute nur noch eine untergeordnete Rolle. Nur so ist erklärlich, dass beim Neuaufsetzen oder Migrieren von IT-Systemen auf eine Datenbereinigung verzichtet und gerne „as is“ der vorhandene Datenbestand vollständig aus dem alten Quellsystem in das neue Zielsystem übernommen wird.

Hinzu kommt, dass gesetzliche, satzungsgemäße oder vertragliche Aufbewahrungspflichten vielfach undifferenziert auf alle personenbezogenen Daten erstreckt werden und hinter der vermeintlich zwingenden, revisionssicheren Langzeitarchivierung der Datenschutz zurücktritt. Beigetragen zu diesem fehlenden Bewusstsein für die auch schon unter dem BDSG bestehenden Löschpflichten haben schließlich die bislang mangelnden Sanktionen und die durch das BDSG legitimierte Möglichkeit zur „Flucht in die Sperrung“ personenbezogener Daten statt einer Löschung.

Dieser Ratgeber stellt systematisch das erforderliche Wissen zur datenschutzkonformen Umsetzung der Löschpflicht sowie zum Umgang mit Löschansprüchen betroffener Personen für die Praxis zur Verfügung. Er erklärt, welche Prozesse beim allein oder gemeinsam Verantwortlichen und Auftragsverarbeiter implementiert sein müssen und beschreibt den Weg zu einem datenschutzkonformen Löschkonzept. Denn das Löschen personenbezogener Daten ist keine lästige Pflichtaufgabe des Verantwortlichen, sondern eine seiner Kerndatenschutzpflichten aus der DS-GVO, deren Erfüllung für den Verantwortlichen erheblichen Aufwand bedeutet. Ohne die Einführung und Umsetzung von Löschkonzepten sowie die Dokumentation der vorgenommenen Löschungen geht der Verantwortliche ein erhebliches Haftungs- und Sanktionsrisiko ein.

Maßgeblich abgestellt wird in diesem Ratgeber auf die DS-GVO, das BDSG und in den Beispielen auch auf nationales Sonderrecht. Ergänzend kann es sein, dass der Anwender in der Praxis auch Landesdatenschutzgesetze oder andere Spezialgesetze zu beachten hat.

Für Verantwortliche bzw. verantwortliche Stellen und Auftragsverarbeiter im Anwendungsbereich des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz oder DSG-EKD) sowie des Gesetzes über den Kirchlichen Datenschutz (KDG) und der Kirchlichen Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) gelten die Ausführungen in diesem Ratgeber entsprechend, wobei vereinzelt Besonderheiten im jeweils anwendbaren kirchlichen Datenschutzrecht zu beachten sind.

1 Die Landesbeauftragte für Datenschutz und Informationsfreiheit des Saarlandes hat in ihrem Tätigkeitsbericht 2019 die Umsetzung der Löschpflichten zu den Aufgaben gezählt, welche die „meisten Probleme“ bereitet, siehe 28. Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes 2019, S. 130.

Wenn in diesem Ratgeber geschlechtsspezifische Bezeichnungen genutzt werden (wie der Verantwortliche und der Auftragsverarbeiter), ist damit stets auch jedes andere biologische und soziale Geschlecht gemeint. Wo möglich, werden neutrale Begriffe genutzt. Im Übrigen wird auf eine vollständige Sichtbarmachung sämtlicher Geschlechter verzichtet.

2. Löschen als Verarbeitung

Das Löschpflicht des Verantwortlichen und das Löschrecht der betroffenen Person aus Art. 17 Abs. 1 DS-GVO dienen der Umsetzung der Grundsätze aus Art. 5 Abs. 1 DS-GVO: Eine Speicherung personenbezogener Daten, die nicht mehr für einen festgelegten, eindeutigen und legitimen Zweck notwendig sind, verstößt gegen den Grundsatz der Zweckbindung, Art. 5 Abs. 1 Buchstabe a DS-GVO. Zugleich werden hierdurch die Grundsätze der Datenminimierung und der Speicherbegrenzung verletzt, Art. 5 Abs. 1 Buchstaben c und d DS-GVO, die von dem Verantwortlichen bei jeder Verarbeitung zu beachten sind.

2.1 Löschen als Abschluss jeder Verarbeitungstätigkeit

Das Löschen ist eine Verarbeitung personenbezogener Daten i.S.d. Art. 4 Nr. 2 DS-GVO:

> *„Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie […] das Löschen oder die Vernichtung;*

Abb. 1: Begriff Verarbeitung

Hinweis: Kein Verarbeiten ohne Löschen

Ein Verarbeiten personenbezogener Daten ohne abschließendes Löschen gibt es nicht. Wer als Verantwortlicher die Zwecke und Mittel einer Verarbeitung festlegt oder eine Verarbeitung durchführt, ohne zuvor die für ein datenschutzkonformes Löschen geeigneten technischen und organisatorischen Maßnahmen getroffen zu haben, verstößt gegen die Verpflichtung zum Datenschutz durch Technikgestaltung aus Art. 25 Abs. 1 DS-GVO.

Das Löschen beendet den Lebenszyklus eines personenbezogenen Datums („**Data Lifecycle**“) als letzten Schritt in einer Reihe von Verarbeitungsvorgängen. Eine Reihe von Verarbeitungsvorgängen ist dabei gleichbedeutend mit der Verarbeitungstätigkeit, die vom Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO im Verzeichnis von Verarbeitungstätigkeiten („VVT“) zu dokumentieren ist (zur Angabe der Löschfristen im VVT siehe unten).

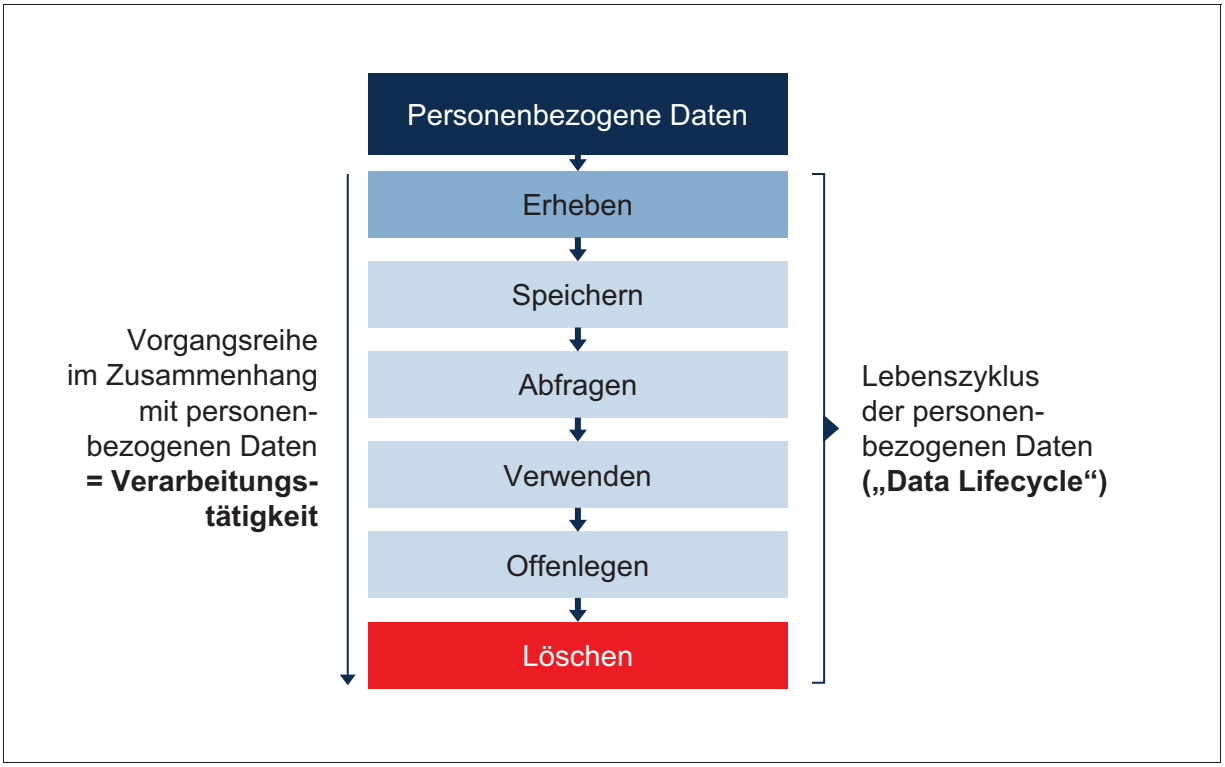

Abb. 2: Lebenszyklus Verarbeitungstätigkeit

Ziel des Verarbeitungsvorgangs „Löschen“ ist die Unmöglichkeit der (weiteren) Wahrnehmung der (zu löschenden) personenbezogenen Daten, unabhängig davon, welche Schritte zur Erreichung dieses Ziels vorgenommen werden.

Hinweis: Löschen ist das Ergebnis einer Verarbeitung

Der Begriff „Löschen“ wird nicht über den Inhalt des Verarbeitungsvorgangs „Löschen“ definiert, sondern über das Ergebnis dieses Vorgangs. Löschen ist das Ziel, nicht der Weg dorthin. Welcher Weg beschritten wird, ist egal, solange die personenbezogenen Daten im Ziel nur gelöscht sind.

2.2 Verschiedene Arten des Löschens

Das Löschen personenbezogener Daten umfasst jede Maßnahme, an deren Ende die personenbezogenen Daten nicht mehr wahrnehmbar sind, darunter auch das Vernichten der Datenträger, auf denen sich die personenbezogenen Daten befinden (z.B. Blätter in einer Papierakte, Festplatte in einem Server). Das Vernichten ist nach dem eindeutigen Wortlaut von Art. 4 Nr. 2 DS-GVO jedoch nur eine besondere Art des Löschens, aber eben nicht die einzige Art.

Tipp: GDD-Praxishilfe „Datenschutzgerechte Datenverträgervernichtung“ beachten

2019 wurde die 4. Auflage der GDD-Praxishilfe „Datenschutzgerechte Datenträgervernichtung“ veröffentlicht, kostenfrei abrufbar unter *https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/datenschutzgerechte-datentraegervernichtung-2*. Die Praxishilfe enthält viele Checklisten für die praktische Umsetzung einer datenschutzkonformen Datenträgervernichtung. Sie berücksichtigt jetzt auch die neue internationale Norm zur Datenträgervernichtung (ISO/IEC 21964), die DS-GVO, das neue BDSG sowie die Änderungen des § 203 StGB.

Ein Löschen ist jede unumkehrbare Unkenntlichmachung personenbezogener Daten, z.B. durch

- ⇨ Überschreiben personenbezogener Daten („Wipe“), z.B. mit Nullen oder Zufallszahlen,
- ⇨ Entmagnetisieren von Datenträgern (physikalischer „Wipe“),
- ⇨ Sicheres Verschlüsseln personenbezogener Daten und Löschen des Schlüssels,
- ⇨ Physikalisches Zerstören des Datenträgers, z.B. durch Schreddern oder Schmelzen, oder
- ⇨ Auflösen der Personenbeziehbarkeit von Daten durch Löschen der Relation, z.B. durch Entfernen eines eindeutigen Identifizierungsmerkmals wie einer Personalkennziffer in einer Auswertung.

Nicht ausreichend sind für ein Löschen demgegenüber die folgenden Handlungen:[2]

- ⇨ Bloßes Austragen von Verweisen auf die weiterhin gespeicherten personenbezogenen Daten aus elektronischen Verzeichnissen,
- ⇨ Schnellformatierung von Datenträgern, die lediglich das Inhaltsverzeichnis des Datenträgers löschen, die personenbezogenen Daten aber unverändert auf dem Datenträger belassen,
- ⇨ Verbot der weiteren Verarbeitung gegenüber Beschäftigten, Auftragsverarbeitern und Dritten ohne Löschung der gespeicherten personenbezogenen Daten, *oder*
- ⇨ Versprechen des Verantwortlichen gegenüber der betroffenen Person oder der Aufsichtsbehörde, die personenbezogenen Daten nicht länger zu verarbeiten.

Tipp: Löschen durch Verschlüsselung

Sollen verschlüsselte personenbezogene Daten gelöscht werden, ist es ausreichend, wenn der Schlüssel unwiderruflich gelöscht wird, die verschlüsselten Daten aber unverändert gespeichert bleiben. Voraussetzung ist aber, dass (1) das Verschlüsselungsverfahren nicht kompromittiert und unter Berücksichtigung des Stands der Technik sicher ist, sowie (2) vor dem Verlust der Sicherheit der Verschlüsselung der Datenträger mit den weiterhin gespeicherten personenbezogenen Daten gelöscht wird, z.B. durch Überschreiben der Daten (soweit möglich) und Vernichtung der Festplatte.

2 Beispiele nach Baustein 60 (Löschen und Vernichten) in der Version 1.0 vom 30.6.2020 zum Standard-Datenschutzmodell, abrufbar unter *https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Löschen_und_Vernichten_V1.0.pdf*.

2.3 Sperren oder Einschränken der Verarbeitung statt Löschen

2.3.1 Sperren nach dem BDSG a.F.

§ 3 Abs. 4 S. 2 BDSG a.F. kannte das Sperren personenbezogener Daten:

> *Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken, […]*

Aus § 35 Abs. 3 ff. BDSG a.F. ergab sich, wann eine Sperrung personenbezogener Daten statt einer Löschung verpflichtend von der verantwortlichen Stelle vorzunehmen war und in welchem Umfang gesperrte personenbezogene Daten weiterhin verarbeitet werden durften:

> *An die Stelle einer Löschung tritt eine Sperrung, soweit*
>
> *1. […] einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, 2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder 3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.*

Die wesentliche Rechtsfolge der Sperrung personenbezogener Daten ergab sich dann aus § 35 Abs. 8 BDSG a.F.:

> *Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.*

2.3.2 Einschränkung der Verarbeitung

Mit der DS-GVO ist die frühere Pflicht zur Sperrung personenbezogener Daten durch das **Recht der betroffenen Person auf Einschränkung der Verarbeitung** gemäß Art. 18 DS-GVO ersetzt worden. Nur in wenigen Ausnahmefällen wie z.B. § 35 Abs. 1 und Abs. 2 BDSG gibt es auch eine **Pflicht zur Einschränkung der Verarbeitung** (dazu unten).

Art. 18 Abs. 1 DS-GVO zählt die Fälle auf, in denen die betroffene Person eine Einschränkung der Verarbeitung verlangen kann:

- ⇨ Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten bis zum Abschluss der Überprüfung der Richtigkeit durch den Verantwortlichen (Buchst. a);
- ⇨ die betroffene Person lehnt bei einer unrechtmäßigen Verarbeitung die Löschung ab und verlangt stattdessen die Einschränkung der Verarbeitung vom Verantwortlichen (Buchst. b);
- ⇨ der Verantwortliche müsste die personenbezogenen Daten gemäß Art. 17 Abs. 1 Buchst. a DS-GVO wegen Wegfall des Verarbeitungszwecks löschen, die betroffene Person benötigt die personenbezogenen Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Buchst. c); oder
- ⇨ die betroffene Person hat Widerspruch gemäß Art. 21 Abs. 1 DS-GVO eingelegt bis zum Abschluss der Prüfung durch den Verantwortlichen, ob der Widerspruch berechtigt ist (Buchst. d).

Weitere Fälle können sich ggf. aus dem nationalen Recht ergeben (z.B. § 35 Abs. 1 und Abs. 2 BDSG, siehe unten).

Die Einschränkung der Verarbeitung bewirkt gemäß Art. 18 Abs. 2 DS-GVO, dass die hiervon betroffenen personenbezogenen Daten für die Dauer der Einschränkung vom Verantwortlichen nur gespeichert werden dürfen. Andere Verarbeitungen sind für die Dauer der Einschränkung der Verarbeitung nur möglich, wenn

- ⇨ die betroffene Person eingewilligt hat,
- ⇨ dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist,
- ⇨ dies zum Schutz der Rechte einer anderen natürlichen oder juristischen Person erfolgt, oder
- ⇨ aus Gründen eines wichtigen öffentlichen Interesses der EU oder eines Mitgliedstaates erforderlich ist.

Ist die Einschränkung der Verarbeitung durch den Verantwortlichen erfolgt, muss dieser gemäß Art. 18 Abs. 3 DS-GVO die betroffene Person vor deren Aufhebung unterrichten. Dies soll der betroffenen Person die Möglichkeit geben, sich gegen die Aufhebung der Einschränkung der Verarbeitung zu wehren.

2.3.3 Sperren oder Einschränkung der Verarbeitung als Alternative zum Löschen

Das Sperren personenbezogener Daten als ausdrückliche Pflicht des Verantwortlichen ist mit der DS-GVO weggefallen. Gleichwohl kann ein Sperren durch den Verantwortlichen weiterhin sinnvoll sein, dies dann als eine mögliche technische Maßnahme zur wirksamen Umsetzung der Grundsätze der Verarbeitung im Sinne des Art. 25 Abs. 1 DS-GVO („Datenschutz durch Technikgestaltung“ oder „Data Protection by Design“) oder zur Sicherheit der Verarbeitung im Sinne des Art. 32 Abs. 1 DS-GVO.

Mit der Pflicht zur Sperrung ist auch der frühere § 35 Abs. 3 Nr. 3 BDSG a.F. entfallen, wonach eine Sperrung personenbezogener Daten verpflichtend zu erfolgen hatte, wenn eine Löschung der personenbezogenen Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist (zur fortbestehenden Ausnahme bei Sonderfällen nicht automatisierter Verarbeitung siehe unten).

Vorsicht: Sonderregeln im kirchlichen Datenschutzrecht

Anders ist dies im Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz oder DSG-EKD). In § 21 Abs. 4 DSG-EKD ist § 35 Abs. 3 Nr. 3 BDSG a.F. inhaltsgleich übernommen worden. In § 19 Abs. 4 S. 1 KDG (Gesetz über den Kirchlichen Datenschutz) und in § 19 Abs. 4 S. 1 KDR-OG (Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts) ist die Ausnahme von der Löschpflicht ebenfalls normiert, allerdings mit dem Zusatz in § 19 Abs. 4 S. 2 KDG bzw. KDR-OG, wonach die Ausnahme von der Löschpflicht bei einer unrechtmäßigen Verarbeitung nicht greift. Alle Regelungen dürften jedoch europarechtswidrig sein und sollten daher nicht oder allenfalls in einem § 35 Abs. 3 Abs. 1 BDSG entsprechenden Umfang angewendet werden.

Das BDSG a.F. ließ ausdrücklich zu, dass es bei der Verarbeitung personenbezogener Daten dazu kommen kann, dass die personenbezogenen Daten am Ende der Verarbeitung nicht oder nur mit unverhältnismäßigem Aufwand gelöscht werden können. Für diesen Fall sollten die be-

troffenen Daten nach Eintritt der Löschpflicht gemäß § 35 Abs. 2 S. 2 BDSG a.F. wenigstens durch eine Sperrung geschützt sein.

Nach der DS-GVO ist das Sperren personenbezogener Daten oder die Einschränkung der Verarbeitung jedoch keine Alternative zur Löschung mehr. Durch die zusätzlichen Pflichten aus Art. 25 Abs. 1 DS-GVO („Datenschutz durch Technikgestaltung“ oder „Data Protection by Design“) werden Anschaffung, Einführung und Betrieb nicht löschfähiger Verarbeitungsmittel (insbesondere Hardware, Software) untersagt:

> *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche* **sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung** *geeignete technische und organisatorische Maßnahmen […], die dafür ausgelegt sind,* **die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen** *und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.*

Eine Verarbeitung personenbezogener Daten, an deren Ende bei Eintritt der Löschpflicht gemäß Art. 17 Abs. 1 DS-GVO (dazu unten) eine Löschung der personenbezogenen Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, ist also stets verordnungswidrig und nur unter Verletzung anderer Datenschutzpflichten des Verantwortlichen möglich.

Wichtig: Migration nicht löschfähiger IT-Systeme

Setzt der Verantwortliche selbst (oder bei seinen Auftragsverarbeitern) nicht löschfähige Verarbeitungsmittel (insbesondere Hardware, Software) für seine Verarbeitungstätigkeiten ein, muss ein unverzüglich umzusetzender Migrationspfad zu einem löschfähigen IT-System erarbeitet und umgesetzt werden, der eine datenschutzkonforme Löschung ermöglicht. Anderenfalls drohen Sanktionen wie im Fall der Deutsche Wohnen SE, die im Oktober 2019 von der Berliner Beauftragten für Datenschutz und Informationsfreiheit mit einem Bußgeldbescheid von 14,5 Millionen Euro belegt worden ist (nicht rechtskräftig). Hintergrund war, dass bei der Deutsche Wohnen SE ein nicht löschfähiges Archivsystem genutzt wurde und nicht in angemessener Zeit Maßnahmen zur Überführung in einen DS-GVO-konformen Zustand umgesetzt worden sind.

2.4 Anonymisieren, Pseudonymisieren oder Verschlüsseln als Löschen

Der sachliche Anwendungsbereich der DS-GVO und damit auch die Datenschutzpflichten im Zusammenhang mit dem Löschen erstrecken sich auf die Verarbeitung personenbezogener Daten gemäß Art. 2 Abs. 1 DS-GVO:

> *Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem[3] gespeichert sind oder gespeichert werden sollen.*

3 Zu den Anforderungen an ein Dateisystem siehe EuGH, Urteil vom 10.7.2018 – C-25/17 („Zeugen Jehovas“).

Gelingt es also, den Personenbezug zu entfernen, sodass keine personenbezogenen Daten mehr vorliegen, erfolgt auch keine Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO mit der Folge, dass auch keine Löschung mehr erforderlich ist. Das De-Personalisieren personenbezogener Daten durch Anonymisieren kann damit ebenfalls eine Löschart sein. Abzugrenzen ist die Anonymisierung jedoch von der Pseudonymisierung. Zudem bedarf es einer Einordnung von verschlüsselten Daten.[4]

2.4.1 Personenbezogene Daten

Der Begriff „personenbezogene Daten“ wird in Art. 4 Nr. 1 DS-GVO definiert:

> *„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; […]*

Für die Personenbeziehbarkeit genügt damit eine Identifizierbarkeit der betroffenen Person (zu pseudonymen Daten siehe unten). Gemäß Art. 4 Nr. 1 DS-GVO ist eine natürliche Person identifizierbar,

> *die* **direkt oder indirekt**, *insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen* **identifiziert werden kann**, *die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;*

Über welche Merkmale die Identifizierbarkeit ermöglicht wird, ist ohne Bedeutung. Die DS-GVO nennt in Art. 4 Nr. 1 DS-GVO nur Beispiele in einer nicht abschließenden Aufzählung.

Beispiel: Online-Kennungen zur Identifizierbarkeit

Online-Kennungen sind neben Benutzernamen auch IP-Adressen[5], Identifizierungsnummern (Identifier oder ID, z.B. eines Endgeräts) und Cookie-Kennungen (ebenfalls ein Identifier, z.B. eine ID in einem Werbenetzwerk), wie Erwägungsgrund 30 ausführt.

Für die Identifizierbarkeit ist außerdem von Bedeutung, über welche Mittel der Verantwortliche verfügt und welcher Aufwand betrieben werden müsste, um Merkmale einer natürlichen Person zuzuordnen, wie Erwägungsgrund 26 konkretisiert:

> *[…] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten 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, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten 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. […]*

Einen **absoluten Personenbezug** kennt die DS-GVO damit nicht. Entscheidend ist nicht, ob irgendwo irgendjemand die Möglichkeit zur Identifizierbarkeit mit den beim Handelnden vorhan-

4 Ausführlich zur Abgrenzung auch Artikel-29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ vom 20.6.2007 (WP 136).

5 Zur Personenbeziehbarkeit auch dynamischer IP-Adressen siehe EuGH, Urteil vom 19.10.2016 – C-582/14; BGH, Urteil vom 16.5.2017 – VI ZR 135/13.

denen Merkmalen hat, sondern allein, ob dem Handelnden selbst die Identifizierbarkeit einer natürlichen Person mit den ihm zur Verfügung stehenden Merkmalen und vernünftigerweise nutzbaren Mitteln möglich ist. Es gilt mithin ein **relativer Personenbezug**.

Beispiel: Datenbanken in Unternehmen[6]

Bei einem Unternehmen sind Daten in mehreren, separaten Datenbanken gespeichert. Erst durch die Zusammenführung dieser Datenbanken werden natürliche Personen identifizierbar. Das Unternehmen könnte auch unter Berücksichtigung der im Markt verfügbaren Technologien (z.B. Analysetools) und mit vertretbarem Aufwand die Zusammenführung der Daten vornehmen. Damit handelt es sich bei den Daten in den Datenbanken um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO, ohne dass es darauf ankommt, ob diese tatsächlich zusammengeführt werden oder nicht. Das Unternehmen ist damit Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO und hat alle Datenschutzpflichten wegen der personenbezogenen Daten in den Datenbanken einzuhalten.

Zur Bewertung der Identifizierbarkeit natürlicher Personen in vorhandenen Daten kann folgendes Prüfschema genutzt werden:

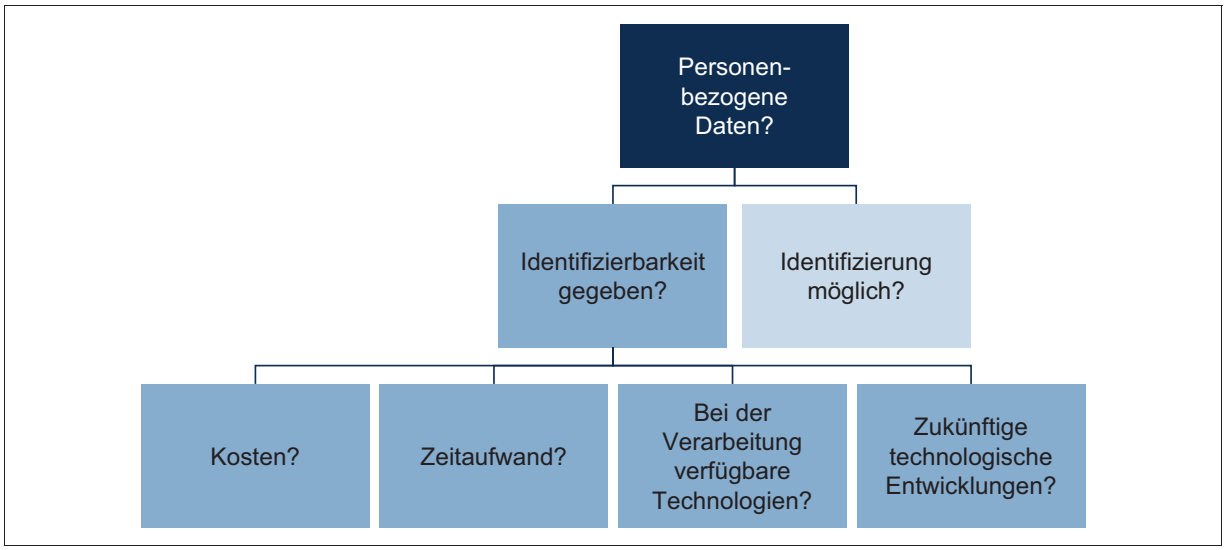

Abb. 3: Prüfschema zur Identifizierbarkeit natürlicher Personen

2.4.2 Pseudonymisierte Daten

Erwägungsgrund 26 stellt klar, dass auch pseudonymisierte Daten wegen der Möglichkeit zur Identifizierbarkeit einer natürlichen Person personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO sind:

> *Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer na-*

6 Beispiel nach *Laue*, in Laue/Kremer: Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 1 Rn. 16.

türlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.

Dabei definiert Art. 4 Nr. 5 DS-GVO die Pseudonymisierung wie folgt:

> *„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.*

Wichtig: Neue Definition gegenüber BDSG a.F.

In § 3 Abs. 6a BDSG a.F. war eine andere Definition der Pseudonymisierung enthalten: „Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." Es genügte, wenn ein Identifizierungsmerkmal durch ein Kennzeichen mit dem Zweck ersetzt wurde, die Bestimmung der betroffenen Person wesentlich zu erschweren. Besondere technische und organisatorische Maßnahmen sah die Pseudonymisierung nach dem BDSG a.F. demgegenüber nicht vor, es genügte ein entsprechender Verarbeitungszweck des Verantwortlichen. Da der Begriff der Pseudonymisierung in der DS-GVO enger gefasst ist, sollte sorgfältig geprüft werden, ob tatsächlich eine Pseudonymisierung von Daten stattgefunden hat.

Pseudonymisierte Daten beschreiben damit einen Sonderfall der Identifizierbarkeit einer natürlichen Person: Die Zuordnung der personenbezogenen Daten zu einer spezifischen betroffenen Person ist ohne Hinzuziehung zusätzlicher Informationen nicht mehr möglich. Allerdings bewahrt nach einer Pseudonymisierung der Verantwortliche die zusätzlichen Informationen, die zur Zuordnung der Daten zu einer spezifischen betroffenen Person erforderlich sind, gesondert auf und stellt durch technische und organisatorische Maßnahmen sicher, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Mit anderen Worten:

Der Verantwortliche hat alle Merkmale zur Identifizierung oder Identifizierbarkeit der betroffenen Person vorliegen, diese aber von den Restdaten technisch und organisatorisch sauber getrennt. So kann der Verantwortliche mit den Restdaten arbeiten, ohne dass diese bei der Verarbeitung selbst einen Personenbezug aufweisen, aber jederzeit zu einem späteren Zeitpunkt die Daten über die von ihm genutzte „Zuordnungsregel" wieder identifiziert oder identifizierbar machen.

Die technischen und organisatorischen Maßnahmen müssen die Identifizierbarkeit durch Nutzung der Zuordnungsregel also nicht gänzlich ausschließen, sondern nur die ungewollte Identifizierbarkeit wirksam verhindern. Dies macht auch eine Pseudonymisierung innerhalb eines Verantwortlichen möglich, was Erwägungsgrund 29 bestätigt:

> *Um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um – für die jeweilige Verarbeitung – die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden. Der für die*

Verarbeitung der personenbezogenen Daten Verantwortliche sollte die befugten Personen bei diesem Verantwortlichen angeben.

Beispiel: Pseudonymisierte Beschäftigtendaten

Daten über Beschäftigte, die unter einer fiktiven Kennung ausgewertet werden, wobei die Rückschlüsselung der fiktiven Kennung zur Personalnummer und damit zum einzelnen Beschäftigten durch technische und organisatorische Maßnahmen unterbunden wird. Kein Pseudonym im Sinne des Art. 4 Nr. 5 DS-GVO ist die Personalnummer, wenn hiermit verknüpfte Daten von Beschäftigten verarbeitet werden und die Personalnummer jederzeit auflösbar ist, z.B. durch einen Blick in das Personalverzeichnis des Verantwortlichen. Nach § 3 Abs. 6a BDSG a.F. hätte dies jedoch noch für eine Pseudonymisierung ausreichen können (siehe oben)

Der Unterschied zwischen pseudonymisierten personenbezogenen Daten im Sinne des Art. 4 Nr. 5 DS-GVO und „normalen" personenbezogenen Daten gemäß Art. 4 Nr. 1 DS-GVO ist damit, dass der Verantwortliche die zur Identifizierbarkeit erforderlichen Merkmale von den restlichen Daten abgesondert und eine ungewollte Zusammenführung durch geeignete technische und organisatorische Maßnahmen unterbunden hat. Damit weisen pseudonymisierte Daten wegen der bereits getroffenen Maßnahmen eine niedrigere Eintrittswahrscheinlichkeit und Schwere von Risiken als nicht pseudonymisierte personenbezogene Daten auf, wie sich Erwägungsgrund 28 entnehmen lässt:

Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. […]

Daher finden sich verschiedene Stellen in der DS-GVO, wo sich eine Pseudonymisierung positiv auf die Erfüllung der Datenschutzpflichten insbesondere durch den Verantwortlichen auswirkt und rechtlich privilegiert ist:

- ⇨ Zweckändernde Weiterverarbeitungen werden gemäß Art. 6 Abs. 4 Buchst. e DS-GVO erleichtert, wenn die betroffenen personenbezogenen Daten pseudonymisiert sind.
- ⇨ Die Pseudonymisierung ist eine mögliche technische Maßnahme zur wirksamen Umsetzung der Datenschutzgrundsätze gemäß Art. 25 Abs. 1 DS-GVO („Datenschutz durch Technikgestaltung" oder „Data Protection by Design").
- ⇨ Die Pseudonymisierung ist eine mögliche technische Maßnahme zur Gewährleistung eines dem Risiko der Verarbeitung angemessenen Schutzniveaus gemäß Art. 32 Abs. 1 DS-GVO.

Zudem wirkt sich eine Pseudonymisierung zugunsten des Verantwortlichen auf die Rechtmäßigkeit einer Verarbeitung aus. Insbesondere bei Art. 6 Abs. 1 Buchst. f DS-GVO wird sich die Pseudonymisierung bei der Abwägung zwischen den berechtigten Interessen des Verantwortlichen einerseits und den schutzbedürftigen Interessen der betroffenen Person andererseits auszahlen.

Vorsicht: Pseudonymisieren ist nicht anonymisieren

Solange es beim Verantwortlichen noch die Möglichkeit gibt, die natürlichen Personen identifizierbar zu machen (siehe Prüfschema oben), sind die Daten nicht anonymisiert. Im Sprachgebrauch sollte deshalb sauber zwischen anonymisierten Daten (keine Identifizierbarkeit mehr gegeben) und pseudonymisierten Daten (Identifizierbarkeit zumindest mittelbar gegeben) differenziert werden. Regelmäßig sind dort, wo von anonymen Daten gesprochen wird, tatsächlich pseudonyme Daten gemeint, die in den Anwendungsbereich der DS-GVO fallen.

2.4.3 Anonymisierte Daten und aggregierte Daten

Eine Definition der Anonymisierung findet sich anders als Art. 4 Nr. 5 DS-GVO mit der Definition der Pseudonymisierung in der DS-GVO nicht. Lediglich in Erwägungsgrund 26 werden anonyme Informationen erwähnt:

> *Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. 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.*

Anonyme Daten sind also Daten, die sich entgegen Art. 4 Nr. 1 DS-GVO nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Auf anonyme oder anonymisierte Daten finden DS-GVO und Datenschutzrecht keine Anwendung.

Tipp: Kein Datenschutz für anonyme Daten

Die Nutzung anonymer Daten vollzieht sich außerhalb der DS-GVO und des Datenschutzrechts, sodass hierfür keinerlei Datenschutzpflichten zu erfüllen sind. Wo möglich, sollte deshalb auf den Personenbezug von Daten verzichtet werden. Andere Gesetze, z.B. das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) oder das Urheberrechtsgesetz (UrhG) mit dem Schutz von Datenbanken, sind jedoch abhängig von Art und Umfang der anonymen Daten trotzdem zu beachten. Ebenso kann sich aus der Informationssicherheit die Erforderlichkeit zu technischen und organisatorischen Maßnahmen zum Schutz von anonymen Daten ergeben.

Anonymisiert sind Daten, wenn nach der Anonymisierung die betroffene Person nicht (mehr) identifizierbar ist. Das Anonymisieren ist damit eine Art des Löschens, denn nach der Anonymisierung sind die personenbezogenen Daten nicht mehr wahrnehmbar (siehe oben). Allerdings führt nur ein unumkehrbares Anonymisieren zu einer Löschung der personenbezogenen Daten i.S.d. Art. 4 Nr. 2 DS-GVO. Besteht bereits beim Anonymisieren die Möglichkeit, dass die Daten durch das Verknüpfen weiterer Angaben wieder identifizierbar sind, sind die Daten nicht anonymisiert, sondern allenfalls pseudonymisiert und damit nicht gelöscht.

Vorsicht: Möglichkeit der De-Anonymisierung

Auch bei anonymisierten Daten besteht das Risiko einer späteren De-Anonymisierung. Grund hierfür können technologische Fortschritte sein, die es erlauben, aus weniger Angaben als früher oder aus anderen Angaben einen Personenbezug abzuleiten (Prüfschema siehe oben). Denkbar ist aber auch, dass durch später beim Verantwortlichen erlangtes Wissen und die Möglichkeit zum Zusammenführen zweier anonymer Datenbestände wieder personenbezogene Daten entstehen. Eine solche De-Anonymisierung führt dazu, dass der Verantwortliche erneut personenbezogene Daten erlangt und damit i.S.d. Art. 4 Nr. 2 DS-GVO verarbeitet. Es sind dann wegen dieser de-anonymisierten Daten wieder sämtliche Pflichten aus der DS-GVO zu beachten. Beim Nutzen anonymer Daten, insbesondere bei Big Data oder Business Intelligence-Tools („BI"), ist deshalb eine regelmäßige Prüfung und Bewertung erforderlich, ob eine De-Anonymisierung möglich ist (oder bereits stattgefunden hat) und deshalb das Datenschutzrecht (wieder) zu beachten ist.

Beim Anonymisieren sind wie oben beim Prüfschema zur Ermittlung der Personenbezogenheit von Daten beschrieben auch Zeit, Aufwand, verfügbare Technologien und zukünftige technologische Entwicklungen zu berücksichtigen, sodass die frühere Definition für das Anonymisieren in § 3 Abs. 6 BDSG a.F. weiterhin genutzt werden kann:

> *Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.*

Das Anonymisieren kann entweder so erfolgen, dass aus den personenbezogenen Daten diejenigen ohne Personenbezug und Identifizierbarkeit herausgefiltert, in einen neuen Datenbestand überführt und anschließend außerhalb des Anwendungsbereichs der DS-GVO genutzt werden, etwa für statistische Zwecke oder Benchmarks. Ebenso ist es möglich, in einem vorhandenen Datenbestand die zur Identifizierbarkeit geeigneten Merkmale zu entfernen oder zu überschreiben, um so den Personenbezug zu entfernen.[7]

Beispiel: Anonymisierte Daten aus Verkehrsordnungswidrigkeiten

Eine Gemeinde nimmt eine Geschwindigkeitskontrolle an einer Straße vor. Beim Überschreiten der zulässigen Höchstgeschwindigkeit werden die Täter mit Foto von Fahrzeug, Fahrer und Kennzeichen erfasst und ermittelt, um die Ordnungswidrigkeit zu ahnden. Anschließend werden die Merkmale Fahrer, Fahrzeug und Kennzeichen entfernt und statistisch die Ordnungswidrigkeiten nach Art und Umfang ausgewertet. Bei den verbleibenden Informationen handelt es sich um anonymisierte Informationen.

Schließlich ist auch das Erzeugen **aggregierter Daten** möglich. Hierbei werden die personenbezogenen Daten mehrerer betroffenen Personen in einem einheitlichen Datensatz zusammengeführt, ohne dass die Daten zu den einzelnen betroffenen Personen noch ausgewiesen werden. Ist die Anzahl betroffener Personen groß genug (Kleingruppe von in der Regel mindestens fünf betroffenen Personen) und sind die zusammengeführten Daten ggf. in Spannen überführt worden (z.B. durch Bildung geeigneter Altersgruppen), bewirkt auch eine solche Aggregation (auch als Aggregierung bezeichnet) eine Anonymisierung der personenbezogenen Daten.

2.4.4 Verschlüsselte Daten

Verschlüsselte Daten werden in der DS-GVO ebenfalls nicht definiert. Allerdings wird die Verschlüsselung in der DS-GVO mehrfach genannt:

- ⇨ Zweckändernde Weiterverarbeitungen werden gemäß Art. 6 Abs. 4 Buchst. e DS-GVO erleichtert, wenn die betroffenen personenbezogenen Daten verschlüsselt sind.
- ⇨ Die Verschlüsselung ist eine mögliche technische Maßnahme zur Gewährleistung eines dem Risiko der Verarbeitung angemessenen Schutzniveaus gemäß Art. 32 Abs. 1 DS-GVO.
- ⇨ Die Pflicht zur Benachrichtigung betroffener Personen über eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12, Art. 34 Abs. 1 DS-GVO („Datenschutzverletzung“, ausführlich dazu unten) kann entfallen, wenn der Verantwortliche durch Verschlüsselung die von der Datenschutzverletzung betroffenen Daten für unbefugte Personen unzugänglich gemacht hat.

7 Zu möglichen Anonymisierungstechniken siehe ausführlich Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken v. 10.4.2014 (WP216).

Verschlüsselung meint dabei jedes Verfahren, bei dem mittels kryptographischer Methoden Daten so verändert werden, dass diese nur mit Kenntnis des jeweiligen Schlüssels lesbar gemacht werden können. Dabei kann der Schlüssel ein Passwort, ein biometrisches Merkmal, ein Zertifikat oder eine Kombination mehrerer Merkmale sein.

Beispiel: Verschlüsselung von E-Mails[8]

Werden E-Mails bei der Übertragung zwischen dem Postausgangsserver des Absenders und dem Posteingangsserver des Empfängers auf dem Transportweg verschlüsselt („**Transportverschlüsselung**“) und geschieht dies mit einem aktuellen und sicheren Verschlüsselungsverfahren, sind die ggf. im Internet beim Transport „mitlesbaren“ Daten anonym. Die E-Mail ist dann gerade nicht mit der Postkarte vergleichbar. Da die Betreiber von Posteingangs- und Postausgangsserver die E-Mail jedoch im Klartext vorliegen haben handelt es sich dort um eine Verarbeitung personenbezogener Daten. Anders ist dies, wenn der Inhalt der E-Mail vom Absender selbst verschlüsselt und so an den Empfänger übersendet wird, der die E-Mail dann nach dem Erhalt entschlüsselt („**Inhaltsverschlüsselung**“ oder „**Ende-zu-Ende-Verschlüsselung**“). Wird hier ein aktuelles und sicheres Verschlüsselungsverfahren genutzt ist der Inhalt der E-Mail auch für die Betreiber von Posteingangs- und Postausgangsserver anonymisiert.

Verschlüsselte Daten bleiben personenbezogene Daten für den Verantwortlichen, solange er über den Schlüssel zur Entschlüsselung der Daten verfügt. Denn trotz der Verschlüsselung bleibt bei Kenntnis des Schlüssels die Identifizierbarkeit der natürlichen Personen erhalten, deren Daten verschlüsselt beim Verantwortlichen vorliegen. Die Verschlüsselung führt mithin beim Verantwortlichen nicht zu anonymisierten Daten. Abhängig davon, wie das zur Entschlüsselung erforderliche Wissen vom Verantwortlichen aufbewahrt wird, kann die Verschlüsselung jedoch zu pseudonymisierten Daten führen (dazu oben).

Legt der Verantwortliche die personenbezogenen Daten einem Empfänger im Sinne des Art. 4 Nr. 9 DS-GVO einschließlich Dritten im Sinne des Art. 4 Nr. 10 DS-GVO gegenüber offen (etwa durch Übermittlung), kann es sich für diesen Empfänger oder Dritten wegen des **relativen Personenbezugs** (dazu oben) bei den Daten um personenbezogene Daten, pseudonymisierte Daten oder anonymisierte Daten handeln.

Erlangt der Empfänger Kenntnis vom Schlüssel, sind die verschlüsselten Daten ebenso einzuordnen wie beim Verantwortlichen selbst.

Ohne Kenntnis des Schlüssels kommt es maßgeblich auf das Verschlüsselungsverfahren und die Sicherheit der Verschlüsselung an. Ist unter Berücksichtigung von Kosten, Aufwand, verfügbaren Technologien und zukünftigen technologischen Entwicklungen eine Entschlüsselung der Daten durch den Empfänger ausgeschlossen, handelt es sich für ihn um anonyme Daten, sodass Datenschutzpflichten nicht greifen. Erforderlich sind dann wie bei jeder anderen Anonymisierung eine fortlaufende Prüfung und Bewertung der Sicherheit der Verschlüsselung durch den Verantwortlichen und den Empfänger der Daten (dazu oben).

8 Ausführlich zur Pflicht zur Verschlüsselung von E-Mails Datenschutzkonferenz (DSK): Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail – Orientierungshilfe des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ vom 13.3.2020, abrufbar unter *https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf*; zum Sonderfall der E-Mail-Kommunikation bei Berufsgeheimnisträgern ausführlich *Kremer*: Unverschlüsselte E-Mail-Kommunikation mit Kunden und Mandanten, in: IT-Rechtsberater (ITRB) 2020, S. 35 bis 40.

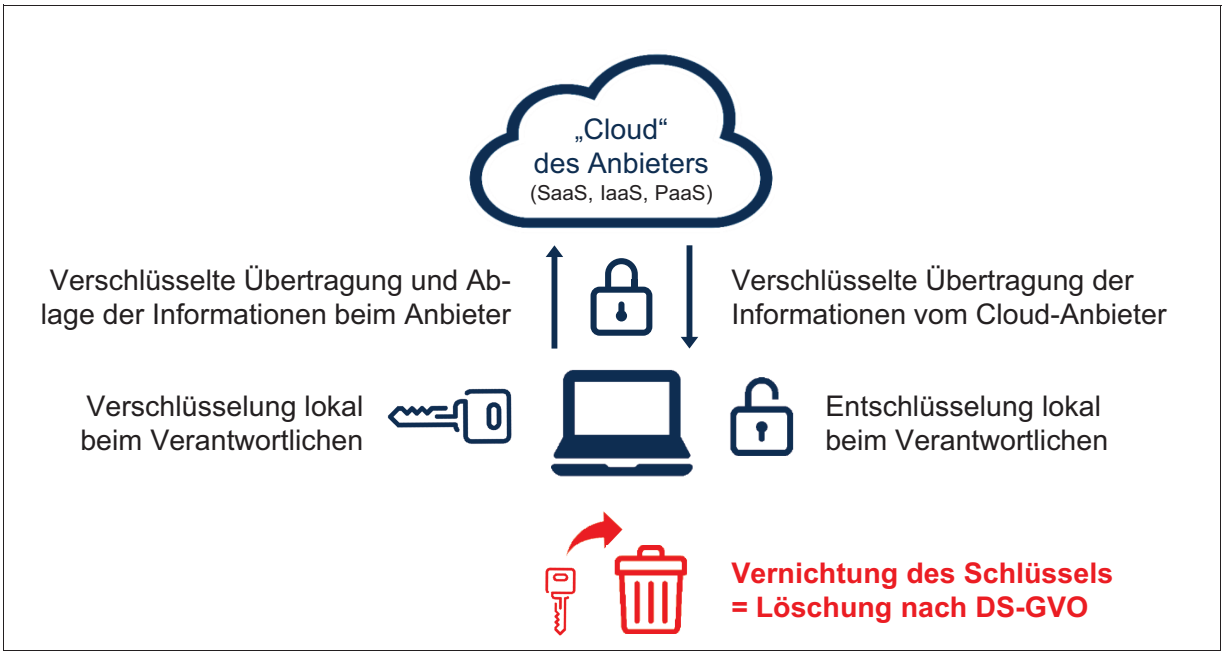

Abb. 4: Löschen durch Verschlüsselung in der Cloud

Stichwortverzeichnis