1. Einleitung

Datenschutzkonformes Löschen in IT-Systemen ist auch mehr als fünf 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 ohne Beachtung des Datenschutzes gewachsene IT-Systeme betroffen, andererseits liegen Daten ausgelagert bei einem Dienstleister oder „in der Cloud“, ohne dass im Zeitpunkt der Auslagerung über das Löschen ernstlich nachgedacht worden ist. 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 häufig 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 a.F. bestehenden Löschpflichten haben schließlich die bislang mangelnden Sanktionen und die durch das BDSG a.F. 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 Kernpflichten 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 schon 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

Die 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 erforderlich sind, verstößt gegen den Grundsatz der Zweckbindung, Art. 5 Abs. 1 Buchst. a DS-GVO. Zugleich werden hierdurch die Grundsätze der Datenminimierung und der Speicherbegrenzung verletzt, Art. 5 Abs. 1 Buchst. c und d DS-GVO, die von dem Verantwortlichen bei jeder Verarbeitung zu beachten sind.

Hinweis: Rechenschaftspflicht führt zur Beweislast des Verantwortlichen

Der EuGH hat in zwei Urteilen klargestellt, dass die Pflicht des Verantwortlichen aus Art. 5 Abs. 2 DS-GVO, die Einhaltung der DS-GVO nachzuweisen (sog. Rechenschaftspflicht oder Accountability), in Auseinandersetzungen mit betroffenen Personen oder der Aufsichtsbehörde zu einer Beweislast des Verantwortlichen führt.[2] Damit muss der Verantwortliche im Ernstfall beweisen, dass er noch zur Speicherung der personenbezogenen Daten berechtigt ist (und diese deshalb noch nicht gelöscht 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

2 EuGH, Urteil vom 24.2.2022 – C-175/20, Rz. 77, 81; Urteil vom 4.5.2023 – C-66/22, Rz. 53.

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).

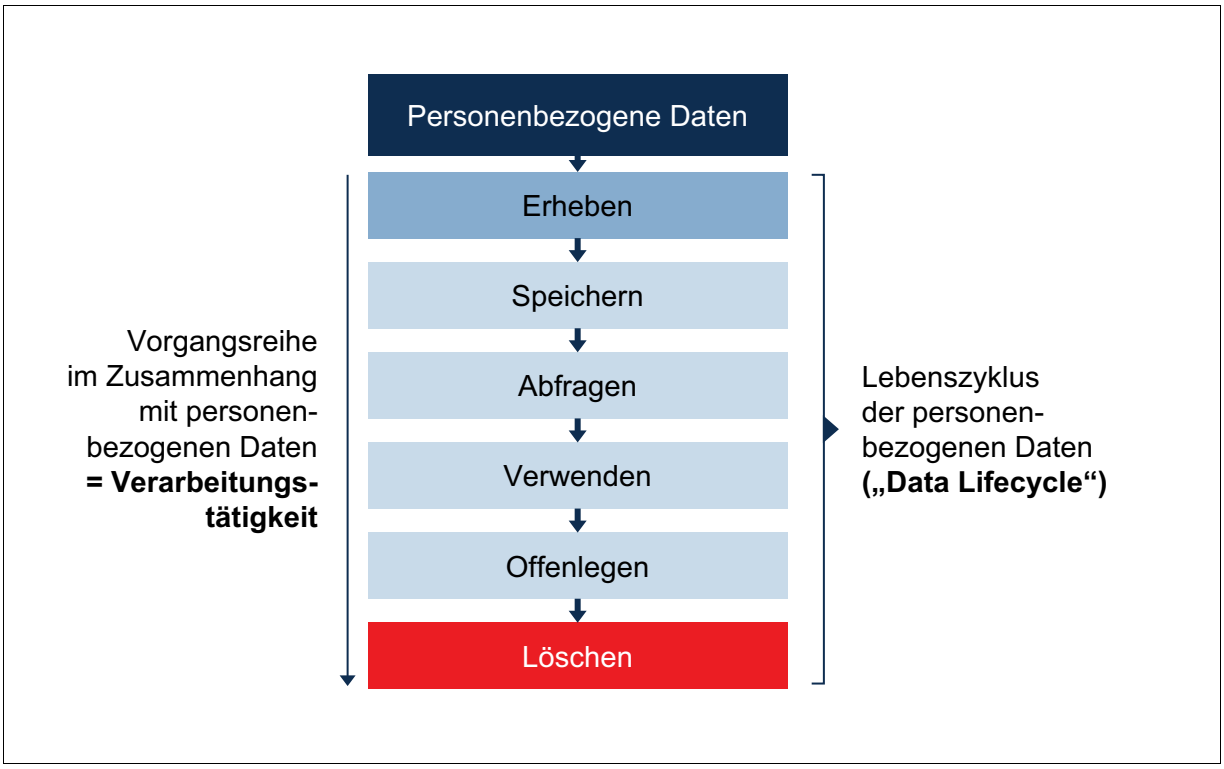

Abb. 2: Lebenszyklus Verarbeitungstätigkeit

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 am Ende 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 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 Datenträgervernichtung“ 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 auch die internationale Norm zur Datenträgervernichtung (ISO/IEC 21964), die DS-GVO, das BDSG sowie § 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:[3]

- ⇨ 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 Unkenntlichmachen des Personenbezugs bei den gespeicherten 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

3 Beispiele nach Baustein 60 (Löschen und Vernichten) in der Version 1.0a vom 2.9.2020 zum Standard-Datenschutzmodell, abrufbar unter *https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Löschen_und_Vernichten_V1.0a.pdf*.

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.

2.3 Sperren oder Einschränken der Verarbeitung statt Löschen

2.3.1 Sperren nach dem BDSG a.F.

§ 3 Abs. 4 Satz 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.*

Das Sperren war mithin im BDSG a.F. ein Recht des Verantwortlichen als Alternative zur Löschung, welches in der Praxis als Begründung genutzt wurde, um löschpflichtige Daten niemals löschen zu müssen.

2.3.2 Einschränkung der Verarbeitung

Mit der DS-GVO ist die frühere Möglichkeit zur Sperrung personenbezogener Daten durch das **Recht der betroffenen Person auf Einschränkung der Verarbeitung** gemäß Art. 18 DS-GVO verdrängt 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; Einschränkung dann 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; Einschränkung dann 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 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 zu erfolgen hatte, wenn eine Löschung der personenbezogenen Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist (zur fortbestehenden Ausnahme beim Sonderfall einer nicht automatisierten 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 Satz 1 KDG (Gesetz über den Kirchlichen Datenschutz) und in § 19 Abs. 4 Satz 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 Satz 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. 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 betroffenen Daten nach Eintritt der Löschpflicht gemäß § 35 Abs. 2 Satz 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.

Vorsicht: Bußgeld wegen nicht löschfähiger Archivsysteme

Am 5.11.2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit in einer Pressemitteilung erklärt, gegen die Deutsche Wohnen SE ein Bußgeld in Höhe von 14 500 000 EUR verhängt zu haben.[4]

Bei zwei Vor-Ort-Prüfungen sei festgestellt worden, dass personenbezogene Daten von Mietern in einem Archivsystem gespeichert wurden, welches keine Möglichkeit zur Löschung vorsehe. In diesem Archivsystem hätten sich auch personenbezogene Daten befunden, die unrechtmäßig verarbeitet wurden oder bei denen der Speicherzweck zwischenzeitlich entfallen sei. Trotz der 2017 ausgesprochenen Empfehlung der Berliner Datenschutzbeauftragten sei bis zum März 2019 weder eine Bereinigung der Datenbestände erfolgt noch seien Maßnahmen ergriffen worden, die zur Herstellung eines rechtmäßigen Zustands hätten führen können.

4 Der Bußgeldbescheid wird noch gerichtlich überprüft. Das LG Berlin, Beschluss vom 18.2.2021 – (526 OWi LG) 212 Js-OWI 1/20 (1/20), hat das Bußgeldverfahren eingestellt. Das KG, Beschluss vom 6.12.2021 – 3 Ws 250/21 – 161 AR 84/21, hat auf die Beschwerde der Aufsichtsbehörde hin dem EuGH im Vorabentscheidungsverfahren verschiedene Rechtsfragen zu den Voraussetzungen für die Verhängung eines Bußgeldes vorgelegt. Beim EuGH ist das Verfahren unter dem Az. C-807/21 anhängig; mit einem Urteil wird spätestens Anfang 2024 gerechnet.

Wichtig: Migration nicht löschfähiger IT-Systeme

Setzt der Verantwortliche selbst (oder bei seinen Auftragsverarbeitern) nicht löschfähige Verarbeitungsmittel für seine Verarbeitungstätigkeiten ein (insbesondere Hardware, Software), muss ein unverzüglich umzusetzender Migrationspfad zu einem löschfähigen IT-System erarbeitet und umgesetzt werden, der eine datenschutzkonforme Löschung ermöglicht. Diese Pflicht ergibt sich aus Art. 25 Abs. 1 DS-GVO (Datenschutz durch Technikgestaltung), der dem Verantwortlichen „auch zum Zeitpunkt der eigentlichen Verarbeitung" auferlegt, „geeignete technische und organisatorische Maßnahmen [zu treffen], die dafür ausgelegt sind, die Datenschutzgrundsätze […] 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.

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*[5] *gespeichert sind oder gespeichert werden sollen.*

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 keine weitere 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.[6]

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; […]*

Personenbezug besteht damit bei jeder 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;*

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

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

Über welche Merkmale die Identifizierung 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[7], 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 Identifizierung mit den beim Handelnden vorhandenen Merkmalen hat, sondern allein, ob dem Verantwortlichen selbst oder anderen Stellen (etwa Auftragsverarbeitern) die Identifizierung einer natürlichen Person mit den ihm zur Verfügung stehenden Merkmalen und vernünftigerweise nutzbaren Mitteln möglich ist. So kann es passieren, dass Daten für den Verantwortlichen noch unter die DS-GVO fallen, weil er den Personenbezug mit vertretbarem Aufwand (wieder)herstellen kann, hingegen für andere Stellen der Personenbezug fehlt, weil sie keinen Zugriff auf jene Mittel haben, die die Daten personenbeziehbar machen. Es gilt mithin ein **relativer Personenbezug**.

Beispiel: Datenbanken in Unternehmen[8]

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 Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO und hat alle Datenschutzpflichten wegen der personenbezogenen Daten in den Datenbanken einzuhalten.

7 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.

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

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

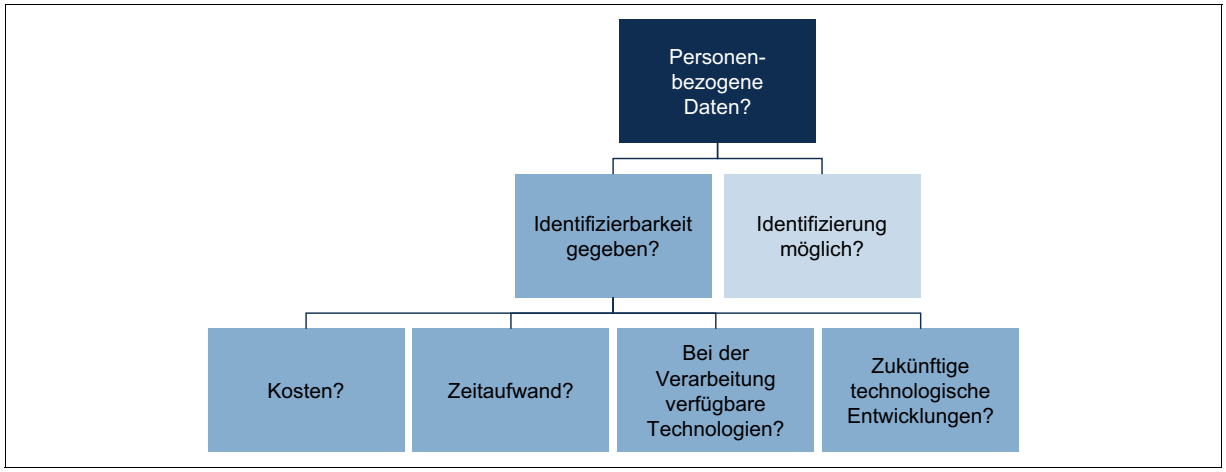

Abb. 3: Prüfschema zur Identifizierbarkeit natürlicher Personen

2.4.2 Pseudonymisierte und anonymisierte Daten

Während es nicht schwerfällt, einen vollständigen, dechiffrierten und lesbaren Datensatz zu Personen als datenschutzrelevant zu identifizieren, kann es insbesondere bei einer komplexen, separierten Verarbeitung an verschiedenen Stellen zu Problemen bei der Ermittlung kommen. Dies hängt insbesondere damit zusammen, dass das Datenschutzrecht keine klare Trennung zwischen personenbezogenen Daten und nicht personenbezogenen Daten macht. Vielmehr lässt sich die Personenbeziehbarkeit, damit also auch die Datenschutzrelevanz, als eine gleitende Skala beschreiben, an deren einen Ende der bestehende Personenbezug, in deren Mitte die Personenbeziehbarkeit und am anderen Ende der fehlende Personenbezug steht.

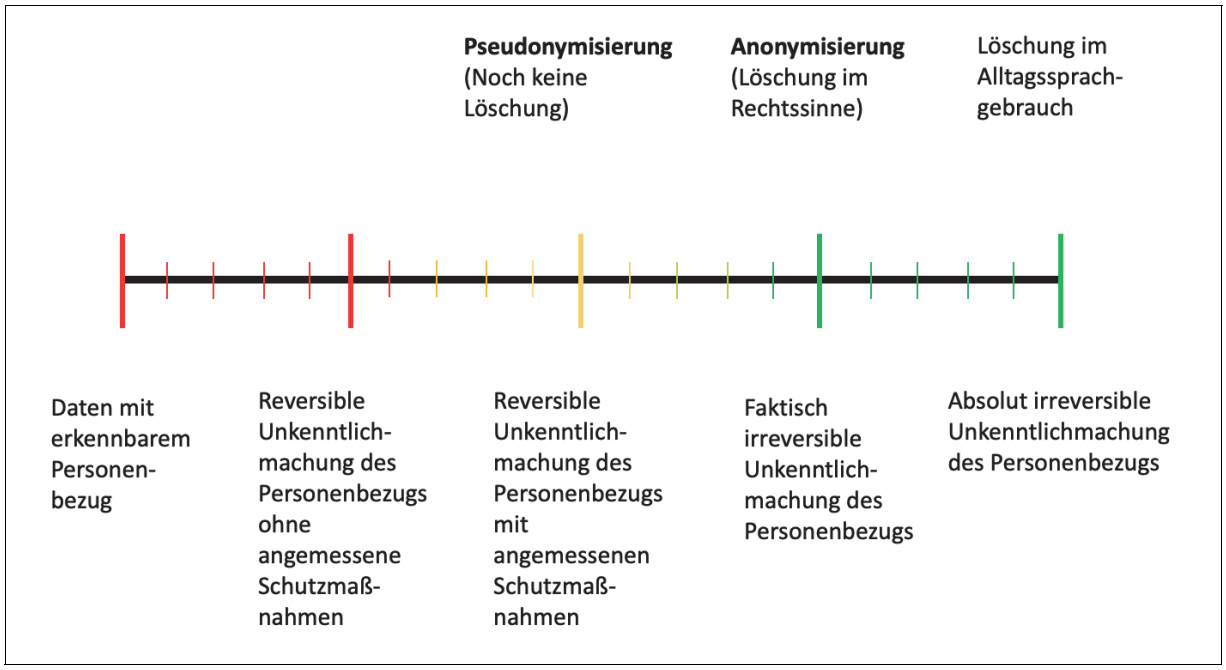

Abb. 4: Gleitende Skala Personenbezug

Stichwortverzeichnis