

ACHIM GRÜNDEL

# Ermittlung des Löscharbedarfs bei unstrukturierten Datenbeständen

Eine praxisnahe Herangehensweise für die routinemäßige Datenlöschung

Aufbewahrungsfristen  
Berechtigte Interessen  
Routinemäßige Löschung  
Organisatorische Maßnahmen

■ Die Ermittlung des Löscharbedarfs für personenbezogene Daten und die Festlegung der dazu relevanten Arbeitsabläufe ist ein komplexes Vorhaben. Es bietet sich daher an, das Thema in einzelne, möglichst einfach handhabbare Bausteine aufzuteilen, wobei als Abgrenzungskriterien der Anlass für Löschungen und die Art der Datenhaltung dienen können. Dies erleichtert es den Verantwortlichen, für jeden Baustein maßgeschneiderte interne Arbeitsanweisungen zur Datenlöschung zu erstellen und unspezifische Vorgaben an die Mitarbeiter zu vermeiden. Der vorliegende Aufsatz veranschaulicht exemplarisch für unstrukturiert gehaltene personenbezogene Daten, wie die Zuständigkeiten und Abläufe zur routinemäßigen Ermittlung des Löscharbedarfs festgelegt werden können.

■ It is a complex endeavor to ascertain the need to delete personal data and the determination of the related relevant sequences of operations. Thus, it lends itself to dividing the issue into smaller, easier to handle blocks, whereby the delineation criterion could be the reason for the occasion of deletion and the type of retention of data. This would make it easier for the responsible parties to compile bespoke internal working guidelines for the deletion of data and to avoid unspecific orders for the employees. The article at hand will demonstrate in a showcase manner how the competence and procedure can be determined for a routine assessment of the need for deletion in unstructured stored personal data.

Lesedauer: 22 Minuten

## I. Einleitung

Die DS-GVO umfasst Regelungen zur Verarbeitung von personenbezogenen Daten, was gem. Art. 4 Nr. 2 DS-GVO auch das Löschen einbezieht. Die Methoden des Löschens, also des Löschvorgangs an sich, sind in der DS-GVO nicht vorgegeben. Stattdessen finden sich Gründe für eine Löschung, so etwa direkt in Art. 17 DS-GVO (Recht auf Löschung) oder indirekt in Art. 5 DS-GVO (Speicherbegrenzung)<sup>1</sup> und Art. 6 DS-GVO (Rechtmäßigkeit der Verarbeitung)<sup>2</sup>. Neben der DS-GVO gibt es weitere Rechtsnormen, z.B. das SGB oder das TKG, in denen bestimmte Gründe für eine Löschung explizit definiert sind.<sup>3</sup>

Als Folge dieser Rechtsnormen müssen Verantwortliche in der Lage sein, für die von ihnen gespeicherten personenbezogenen Daten zu ermitteln, ob es einen konkreten Löschanlass gibt und welcher Löschanlass sich daraus ableitet. Es geht also darum, die dem eigentlichen Löschvorgang vorausgehenden technischen und organisatorischen Maßnahmen, mit denen der Löschbedarf für jedes personenbezogene Datum ermittelt werden kann, festzulegen. Diesbezüglich wird auch der Begriff „Löschkonzept“ verwendet.<sup>4</sup> Damit eng verbunden ist die Anforderung aus Art. 30 Abs. 1 lit. f DS-GVO, wonach – wenn möglich – die vorgesehenen Löschrufen je Datenkategorie im Verzeichnis der Verarbeitungstätigkeiten anzugeben sind. Der Begriff der Kategorie personenbezogener Daten findet sich noch an weiteren Stellen der DS-GVO<sup>5</sup>; insofern stellt die Bildung von Datenkategorien ein wichtiges Prinzip dar. Allerdings ist auch zu berücksichtigen, dass personenbezogene Daten nach Art. 17 Abs. 1 DS-GVO bei Vorliegen der dort genannten Gründe unverzüglich zu löschen sind, sodass es unabhängig von den pro Datenkategorie vorgesehenen (Soll-)Löschrufen auf den konkreten Einzelfall ankommt.<sup>6</sup> Das bedeutet dann auch, dass es zu Ausnahmen von eben diesen Fristen kommen kann. Ein Löschkonzept muss also auch für derartige Fälle Vorkehrungen treffen. Dies ist auch insofern von Relevanz, als nicht nur Verstöße gegen Löschpflichten bußgeldbewehrt sind (Art. 83 Abs. 5 DS-GVO)<sup>7</sup>, sondern auch gem. Art. 83 Abs. 4 DS-GVO Versäumnisse in Bezug auf technische und organisatorische Maßnahmen – also auch Löschkonzepte –<sup>8</sup> und das Verzeichnis der Verarbeitungstätigkeiten.<sup>9</sup>

## II. Thematische Eingrenzung

In der Praxis besteht eine Vielfalt an Datenbeständen, Arbeitsabläufen, Verarbeitungszwecken, Aufbewahrungsfristen und weiteren Faktoren, die die Identifizierung und Festlegung des Löschbedarfs beeinflussen. Daher wird man für die Ermittlung des Löschbedarfs oftmals keine allgemein geltenden Aussagen treffen können.<sup>10</sup> Vielmehr erscheint es sinnvoll, das Thema in einzelne Bausteine aufzuteilen, um die Komplexität auf ein handhabbares Maß zu reduzieren. Insofern verfolgt dieser Beitrag nicht das Ziel, das Thema Löschbedarf in Gänze abzuhandeln, sondern beschäftigt sich mit einem konkreten Teilbereich: der routinemäßigen Ermittlung des Löschbedarfs von unstrukturiert gehaltenen personenbezogenen Daten. Beide Begriffe „routinemäßig“ und „unstrukturiert“ werden nachfolgend erläutert.

### 1. Routinemäßige Ermittlung des Löschbedarfs

Bei der Löschung von personenbezogenen Daten sind zwei grundsätzlich verschiedene Kategorien von Anlässen zu unterscheiden. Eine Kategorie ist, wie eingangs erwähnt, die Löschung nach einer Aufforderung durch den Betroffenen gem. Art. 17 DS-GVO. Der konkrete Grund zur Löschung entsteht, wenn ein Löschesuchen eines Betroffenen beim Verantwortlichen eingeht und berechtigt ist. Aus Komplexitätsgründen wird in diesem Beitrag auf die Darstellung der dazu erforderlichen Prüf- und Bearbeitungsprozesse nicht näher eingegan-

gen. Der Fokus soll vielmehr auf der zweiten Kategorie von Anlässen, der routinemäßigen Ermittlung des Löschbedarfs, liegen. Art. 17 Abs. 1 DS-GVO sieht vor, dass Verantwortliche neben der antragsbasierten Löschung auch eine Löschung von sich aus durchzuführen haben, sofern die dort genannten Gründe zutreffen.<sup>11</sup> Verantwortliche müssen also laufend prüfen, ob die Voraussetzungen für eine Verarbeitung noch gegeben oder weggefallen sind.<sup>12</sup> Die Ermittlung des Löschbedarfs für personenbezogene Daten muss gewissermaßen routinemäßig, d.h. ohne Aufforderung eines Betroffenen, erfolgen.

### 2. Unstrukturierte Datenbestände

Ein wesentliches Problem für die Ermittlung des Löschbedarfs ist, dass personenbezogene Daten in unterschiedlichsten Systemen und Formaten vorliegen können und womöglich auch redundant vorhanden sind.

■ **Beispiel:** Die Verkaufsabteilung eines Logistikunternehmens erfasst den Inhalt eines per E-Mail eingehenden Transportauftrags in einem Auftragsverwaltungssystem. Die E-Mail selbst wird zur Einhaltung steuerlicher Vorschriften für mind. sechs Jahre im E-Mail-Programm archiviert. Zusätzlich wird die E-Mail samt Anhängen an die Dispositionsabteilung weitergeleitet. Zudem speichert die eingesetzte Software beim Öffnen von E-Mail-Anhängen eine Kopie der Anhänge im sog. Cache-Speicher des jeweiligen Arbeitsplatzrechners ab.

Das o.g. Beispiel zeigt, dass es zwei gänzlich unterschiedliche Kategorien von Datenbeständen gibt. Personenbezogene Daten können einerseits in Form von Datensätzen in einer Datenbank enthalten sein, welche z.B. die Grundlage einer Unternehmenssoftware zur Abwicklung von Finanzen, Einkauf und Verkauf ist.<sup>13</sup> Ein derartiger Datenbestand hat eine fest definierte Ordnung, die von Anwendern üblicherweise nicht eigenständig geändert werden kann. Andererseits gibt es Datenbestände, deren Struktur die Anwender wesentlich beeinflussen können. Ein Beispiel sind Verzeichnisse auf Laufwerken oder anderen Datenträgern, in denen Dateien mit Texten, Tabellen, Präsentationen, Fotos oder Videos gespeichert werden. Auch wenn der Inhalt einzelner Dateien durchaus strukturiert sein kann – man denke z.B. an Excel-Tabellen –, so hat diese Art der Datenhaltung dennoch insgesamt einen unstrukturierten Charakter. Ausschlaggebend ist hierbei, dass die Anwender die Möglichkeit haben, so-

- <sup>1</sup> Vgl. *Herbst*, in: Kühlung/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rdnr. 66.
- <sup>2</sup> S. hierzu *Keppeler/Berning*, ZD 2017, 315, bei denen die Löschpflicht nach Art. 17 DS-GVO als ein Spiegelbild der Erlaubnistatbestände u.a. aus Art. 6 Abs. 1 DS-GVO angesehen wird; vgl. auch *Paal*, in: *Paal/Pauly*, DS-GVO/BDSG, 2. Aufl. 2018, Art. 17 Rdnr. 26.
- <sup>3</sup> U.a. § 276 Abs. 2 Satz 4 SGB V, § 97 Abs. 3 Satz 3 und 4 TKG, § 25a Abs. 3 Nachweisverordnung.
- <sup>4</sup> S. die ausführliche Darstellung bei *Koglin*, in: *Koreng/Lachenmann*, Formularhdb. Datenschutzrecht, 2. Aufl. 2018, Kap. D.IV.; vgl. *Scheja/Quael/Conrad/Hausen*, in: *Forgó/Helfrich/Schneider*, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil IV Kap. 2 Rdnr. 29 ff.
- <sup>5</sup> Z.B. in Art. 14 DS-GVO (Informationspflichten), Art. 15 DS-GVO (Auskunftsrecht), Art. 33 DS-GVO (Meldung von Datenschutzverletzungen).
- <sup>6</sup> Vgl. *Hartung*, in: Kühlung/Buchner (o. FuBn. 1), Art. 30 Rdnr. 23; auch *Arning*, in: *Moos/Scheffig/Arning*: Die neue Datenschutz-Grundverordnung, 2018, Kap. 6 Rdnr. 195.
- <sup>7</sup> Vgl. *Koglin* (o. FuBn. 4), dort Anm. 4.
- <sup>8</sup> Vgl. *Nolte/Werkmeister*, in: *Gola*, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 25 Rdnr. 33 mit Rdnr. 17.
- <sup>9</sup> Vgl. *Dietze*, in: *Schwartzmann/Jaspers/Thüsing/Kugelmann*, DS-GVO/BDSG, Art. 30 Rdnr. 87.
- <sup>10</sup> Ähnl. argumentiert *Keppeler*, RDV 2018, 72 f., der auf die Betrachtung des jeweiligen Einzelfalls abstellt und bei der Frage nach dem Eintritt der Löschpflicht erhebliche Unwägbarkeiten sieht.
- <sup>11</sup> *Paal* (o. FuBn. 2), Art. 17 Rdnr. 20; auch *Nolte/Werkmeister* (o. FuBn. 8), Art. 17 Rdnr. 9.
- <sup>12</sup> *Paal* (o. FuBn. 2); zur Klärung, was „laufend“ bedeutet, s. weiter unten Kapitel „Prüfrhythmus“.
- <sup>13</sup> *Geisler*, Datenbanken: Grundlagen und Design, 5. Aufl. 2014, S. 495.

wohl Verzeichnisse und Unterverzeichnisse als auch die enthaltenen Dateien nach eigenem Bedarf individuell zu erstellen und deren Anordnung jederzeit abzuändern.<sup>14</sup>

Hinzu kommt, dass personenbezogene Daten in einem unstrukturierten Datenbestand vom Grundsatz her unterschiedlichster Art sowie Gegenstand diverser Verarbeitungstätigkeiten und -zwecke sein können. So kann an einem Arbeitstag die erste Nachricht, die eine Vertriebsmitarbeiterin per E-Mail versendet, für einen Kunden bestimmt sein, während die unmittelbar darauffolgende Nachricht an die Personalabteilung gerichtet sein kann, um einen Urlaubsantrag einzureichen. Beide Arten von Daten sind jedoch in dem gleichen Datenbestand, nämlich dem E-Mail-Postfach, enthalten. Ähnliches gilt für Dateien, die in den Verzeichnissen eines Unternehmensnetzwerks gespeichert werden: Allein der Verzeichnisname gibt noch keine Gewährleistung, dass die enthaltenen Dateien auf Grund desselben Zwecks entstanden sind und dass eine einheitliche Methode zur Ermittlung des Löscharbeitsbedarfs angewendet werden kann.

### III. Ausgangspunkte für die Ermittlung des Löscharbeitsbedarfs

#### 1. Gründe für eine Löschung

Im Rahmen der routinemäßigen Ermittlung des Löscharbeitsbedarfs sind in der Praxis verschiedene Löscharbeitsgründe zu berücksichtigen. Zu nennen ist insbesondere Art. 17 Abs. 1 lit. a DS-GVO hinsichtlich des Wegfalls des Zwecks, zu dem personenbezogene Daten erhoben oder verarbeitet wurden.<sup>15</sup> Weiterhin ist zu prüfen, ob personenbezogene Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 lit. d DS-GVO). Außerdem ist hinsichtlich der routinemäßigen Ermittlung des Löscharbeitsbedarfs Art. 17 Abs. 1 lit. e DS-GVO relevant, wonach eine Löschung zu erfolgen hat, wenn dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Dies betrifft u.a. die eingangs erwähnten Spezialgesetze, die einen maximal zulässigen Aufbewahrungszeitraum vorgeben.<sup>16</sup> Ist dieser abgelaufen, besteht eine unmittelbare Pflicht zur Löschung. So müssen z.B. Krankenkassen laut § 304 SGB V bestimmte Daten über Kassenleistungen nach spätestens zehn Jahren zwingend löschen, sofern die relevanten Bedingungen erfüllt sind.

#### 2. Berücksichtigung von Zusatzinformationen

Ob ein Grund für eine Löschung tatsächlich vorliegt, lässt sich möglicherweise nicht direkt aus den betrachteten personenbezogenen Daten ablesen. Vielmehr kann es erforderlich sein, Zusatzinformationen zu berücksichtigen, darunter die unterschiedlichen Verarbeitungszwecke und potenziellen berechtigten Interessen. Dies soll nachfolgend anhand eines Beispiels erläutert werden.

■ **Beispiel:** Die Einkaufsabteilung eines Industrieunternehmens möchte einen Handwerker (Einzelunternehmer) mit einer dringenden notwendigen Maschineninstandsetzung beauftragen. Da-

zu wird der Auftrag mit einem Textverarbeitungsprogramm erstellt, dann ausgedruckt und mit zwei Unterschriften versehen. Der unterschriebene Auftrag wird vor dem postalischen Versand eingescannt (als PDF-Datei) und auf dem Abteilungslaufwerk digital archiviert, da Wiedergaben abgesandter Handelsbriefe nach § 257 HGB mind. sechs Jahre aufbewahrungspflichtig sind.

Eine unmittelbare, automatische Löschung der PDF-Datei direkt nach Ablauf der Mindestaufbewahrungsfrist ist problematisch, wenn es zu dem Zeitpunkt noch rechtliche Auseinandersetzungen gibt, für die das Auftragschreiben relevant sein könnte. Mit Verweis auf Art. 17 Abs. 3 lit. e DS-GVO wäre dann ein Verzicht auf eine Löschung zulässig.<sup>17</sup>

Auch könnte sich aus der einmaligen Beauftragung eine dauerhafte Wartung dergestalt ergeben haben, dass bei Folgeaufträgen auf Klauseln des ursprünglichen Auftragschreibens verwiesen wird. Eine weitere Speicherung könnte dann zur Vertragserfüllung erforderlich und durch Art. 6 Abs. 1 lit. b DS-GVO gerechtfertigt sein.<sup>18</sup>

#### 3. Wahl der passenden Vorgehensweise

Verantwortliche stehen in der Praxis vor dem Problem, eine angemessene Vorgehensweise zur Ermittlung des Löscharbeitsbedarfs zu etablieren. Diese Vorgehensweisen können grundsätzlich in zwei Kategorien unterschieden werden. Einerseits kann es sein, dass ein Teil der unstrukturiert gehaltenen personenbezogenen Daten einen so individuellen Charakter hat, dass keine standardisierten Löscharbeitsregeln anwendbar sind.<sup>19</sup> Die jeweilige Person, in deren Zuständigkeitsbereich z.B. E-Mails und Dateien liegen, würde dann eine einzelfallbezogene Einschätzung über das Vorliegen eines Löscharbeitsbedarfs treffen, ggf. unter Berücksichtigung von Zusatzinformationen, die sie bei anderen Abteilungen erfragt. Andererseits könnten sich für bestimmte E-Mails und Dateien Regeln zur Einschätzung des Löscharbeitsbedarfs finden lassen.<sup>20</sup> Dies soll anhand eines Beispiels erläutert werden.

■ **Beispiel** (mit zwei Abteilungen in einem Unternehmen): Abteilung A holt über Kaufinteressenten Bonitätsauskünfte ein und speichert diese als PDF-Datei auf ihrem Abteilungslaufwerk. Abteilung B erstellt Angebote in Abhängigkeit von der Bonität entweder mit der Zahlungsbedingung „Vorkasse“ oder „auf Rechnung“. Abteilung B erfasst die Angebotsinformationen für Zwecke des Vertriebscontrollings in einer tabellarischen Übersicht und ergänzt für jedes Angebot im Zeitablauf den passenden Status („Auftrag erhalten“, „Keinen Auftrag erhalten“).

Bei diesem Szenario können je nach Kombination aus Angebotsstatus und Zahlungsbedingung unterschiedliche Regeln für die Löschung der Bonitätsauskünfte definiert werden. Eine Regel könnte z.B. folgendermaßen lauten: Wenn ein Interessent ein Angebot mit Zahlungsbedingung Vorkasse akzeptiert hat, wird die Bonitätsauskunft spätestens zwei Wochen nach Auftragserteilung gelöscht, da sie ihren Zweck erfüllt hat. Damit Abteilung A in der Lage ist, zu prüfen, ob eine Bonitätsauskunft unter diese Regel fällt, könnte festgelegt werden, dass Abteilung B die Angebotsliste im Zwei-Wochen-Rhythmus an Abteilung A bereitstellt.

#### IV. Maßnahmen zur Ermittlung des Löscharbeitsbedarfs

Verantwortliche sind gem. Art. 24 DS-GVO dazu verpflichtet, geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DS-GVO erfolgt. Dies schließt somit auch Maßnahmen hinsichtlich der Löschung personenbezogener Daten ein. Während der Löscharbeitsvorgang

<sup>14</sup> Ähnl. argumentiert Geisler (o. Fußn. 13), S. 496.

<sup>15</sup> Arning (o. Fußn. 6), Rdnr. 194, sowie Rdnr. 196, wo ergänzend darauf hingewiesen wird, dass eine Zweckänderung zulässig sein kann, sodass zunächst kein Löscharbeitsgrund entsteht.

<sup>16</sup> Stollhoff, in: Auernhammer, DS-GVO/BDSG, 6. Aufl. 2018, Art. 17 Rdnr. 33, mit Bsp. aus TKG und UrhG.

<sup>17</sup> Vgl. Stollhoff (o. Fußn. 16), Art. 17 Rdnr. 66.

<sup>18</sup> Vgl. Kramer, in: Auernhammer (o. Fußn. 16), Art. 6 Rdnr. 29.

<sup>19</sup> Ähnl. Hammer/Fraenkel, DuD 2011, 892, die von Sonderfällen sprechen.

<sup>20</sup> Hammer, DuD 2016, 529 f., auch wenn dort eher die strukturierten Daten im Vordergrund stehen; s.a. Hammer/Schuler, Leitlinie zur Entwicklung eines Löscharbeitskonzepts mit Ableitung von Löscharbeitsfristen für personenbezogene Daten, Version 1.0.3, 2015, abrufbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Leitlinie\\_zur\\_Entwicklung\\_eines\\_Loeschkonzpts.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Leitlinie_zur_Entwicklung_eines_Loeschkonzpts.html).

selbst eher technischen Charakter hat, stehen für die Ermittlung des Löscharbedarfs organisatorische Maßnahmen im Vordergrund.

Organisatorische Maßnahmen können u.a. darin bestehen, Richtlinien bzw. Handlungsanweisungen festzulegen.<sup>21</sup> Die Leitungsebene eines Verantwortlichen – bei Unternehmen z.B. Geschäftsführung oder Vorstand – könnte also eine interne Anweisung für die Ermittlung des Löscharbedarfs bei unstrukturiert gehaltenen personenbezogenen Daten herausgeben.

Dabei sollte Folgendes berücksichtigt werden: Unstrukturierte Datenbestände können, wie oben erläutert, eine große Vielfalt an personenbezogenen Daten enthalten. Insofern wäre es schon aus Gründen der Praktikabilität wenig zielführend, eine allumfassende Direktive zu erstellen, die detaillierte Vorgaben für alle Arten von unstrukturiert gehaltenen personenbezogenen Daten macht. Vorteilhafter wäre – aus Sicht der Leitungsebene des Verantwortlichen – die Erstellung einer Rahmenrichtlinie, die allgemeine Prinzipien zur Ermittlung des Löscharbedarfs beinhaltet. Wesentliche Kernbestandteile einer solchen Rahmenrichtlinie werden nachfolgend genauer erläutert. Zudem ist jeweils ein Vorschlag (Musterformulierung) enthalten, den die geeigneten Leser in ihre eigenen Dokumente übernehmen können.

### 1. Grundsatz und Verfahrensabläufe

Eine Rahmenrichtlinie kann aus den o.g. Gründen nur allgemeine Regeln, aber keine Details für die Ermittlung des Löscharbedarfs vorgeben. Es ist daher sinnvoll, wenn die Ausarbeitung der Details an untergeordnete Ebenen – z.B. Abteilungsleitungen bzw. Geschäftsprozessverantwortliche (GPV) – delegiert wird.<sup>22</sup> Die untere Ebene sollte dann eine Konkretisierung für ihren jeweiligen Verantwortungsbereich vornehmen. Dabei ist es zweckmäßig, wenn diese Konkretisierung schriftlich erfolgt.

#### Musterformulierung:

Als Grundsatz gilt: Jede Abteilung und jede/-r Mitarbeiter/-in hat regelmäßig die unstrukturiert gehaltenen personenbezogenen Daten in seinem/ihrer Verantwortungsbereich dahingehend zu überprüfen, ob es Gründe für eine Löschung gibt (routinemäßige Ermittlung des Löscharbedarfs). Als unstrukturiert gelten u.a. Nachrichten in E-Mail-Postfächern und Dateien auf Netzlaufwerken; eine nicht abschließende Übersicht findet sich in einer Anlage zu dieser Rahmenrichtlinie. Um eine angemessene Überprüfung zu gewährleisten, hat jede Abteilungsleitung bzw. jede/r GPV dafür angemessene Verfahrensabläufe in schriftlicher Form zu definieren. Die einzelnen Abteilungen haben sich untereinander über die geeigneten Verfahrensabläufe abzustimmen.

### 2. Kenntnis der Mindestaufbewahrungsfristen

Ein wesentliches Kriterium für die Ermittlung des Löscharbedarfs sind die Mindestaufbewahrungsfristen, die für die jeweiligen personenbezogenen Daten gelten. Die Fristen können dabei je nach Verarbeitungszweck variieren. Es ist daher einerseits notwendig, für jede Kombination aus Daten und Zweck die Fristen zu kennen, und andererseits sinnvoll, diese Informationen in verständlicher Form zu dokumentieren und intern zu kommunizieren.

#### Musterformulierung:

Jede Abteilungsleitung bzw. jede/r GPV hat für die in seinem/ihrer Verantwortungsbereich liegenden personenbezogenen Daten die unterschiedlichen Einsatzzwecke der Daten-

haltung zu definieren. Für jede Kombination aus Einsatzzweck und Art der Daten sind die Mindestaufbewahrungsfristen, die sich aus den für den Zweck bzw. Prozess anwendbaren Rechtsnormen ergeben, sowie deren Berechnungsmethoden zu identifizieren. Dabei sind neben den Fristen des Steuerrechts auch andere Rechtsnormen (Gesetze, Verordnungen etc.) zu berücksichtigen. Jede Abteilungsleitung bzw. jede/r GPV hat diese Informationen schriftlich festzuhalten und den Mitarbeitern seines/ihrer Verantwortungsbereichs in geeigneter Weise zu vermitteln. Dabei ist sicherzustellen, dass auch neu ins Unternehmen kommende Mitarbeiter diese Informationen erhalten. Sofern keine Mindestaufbewahrungsfristen anwendbar sind, ist dies ebenfalls festzuhalten und den Mitarbeitern zu vermitteln.

### 3. Verarbeitung nach Ablauf der Mindestaufbewahrungsfrist

Eine Mindestaufbewahrungsfrist, z.B. sechs Jahre gemäß Steuerrecht für Handelsbriefe, besagt zunächst lediglich, über welchen Zeitraum hinweg keine Löschung erfolgen darf. Sie besagt jedoch nicht, dass direkt nach Ablauf der Frist eine Löschung zwingend erforderlich ist. Eine weitere Verarbeitung bzw. Speicherung kann u.a. aus berechtigtem Interesse, zur Erfüllung eines Vertrags oder einer rechtlichen Pflicht erforderlich sein. Demzufolge besteht die Aufgabe, das Vorliegen dieser Erfordernisse zu prüfen.<sup>23</sup>

#### Musterformulierung:

Zusätzlich zu den Mindestaufbewahrungsfristen hat jede Abteilungsleitung bzw. jede/r GPV für jede Kombination aus Verarbeitungszweck und Art der Daten die berechtigten Interessen und vertragliche oder rechtliche Pflichten zu ermitteln, die eine Verarbeitung bzw. Speicherung auch nach Ablauf einer Mindestaufbewahrungsfrist erlauben bzw. erforderlich machen. Diese Informationen sind schriftlich festzuhalten und den Mitarbeitern in geeigneter Weise zu vermitteln. Ggf. ist die Dauer, nach der ein berechtigtes Interesse hinfällig wird, samt Berechnungsmethode festzulegen und zu kommunizieren.

### 4. Vorübergehende Löschsperren und deren Informationsaustausch

In der Praxis kann es Sachverhalte geben, die eine Löschung hemmen. Diese Sachverhalte können in einer Abteilung entstehen, die nicht zwingend identisch mit derjenigen Abteilung ist, die die zur Löschung vorgesehenen personenbezogenen Daten vorhält. Dazu folgendes Beispiel: Die Produktionsabteilung eines Industrieunternehmens macht Garantieansprüche gegenüber einem Handwerksbetrieb wegen mangelhafter Maschinenwartung geltend. Dann ist es wichtig, dass die Einkaufsabteilung die eigentlich zur Löschung vorgesehenen Bestellungen und Lieferscheine sowie weiteren relevanten Schriftverkehr mit dem Handwerksbetrieb bis auf weiteres gem. Art. 17 Abs. 3 lit. e DS-GVO nicht löscht.<sup>24</sup> Dies setzt einen angemessenen Informationsaustausch zwischen den einzelnen Abteilungen voraus.

<sup>21</sup> Vgl. *Schefzig*, in: Moos/Schefzig/Arning (o. FuBn. 6), Kap. 11 Rdnr. 15 f.

<sup>22</sup> Vgl. *Schefzig* (o. FuBn. 21), Kap. 11 Rdnr. 17 im Hinblick auf die unternehmensinterne Zuweisung von Zuständigkeiten, sowie Rdnr. 41 hinsichtlich Delegation.

<sup>23</sup> *Abel* (Hrsg.), Datenschutz, Grundwerk einschließlich 119. (letzter) Aktualisierungs- und Ergänzungslieferung Sept. 2014, Teil 6/2.4.1, S. 7.

<sup>24</sup> Vgl. *Stollhoff* (o. FuBn. 16), die darauf hinweist, dass die Ausnahme nicht nur für gerichtliche, sondern auch für außergerichtliche Verfahren gilt.

#### Musterformulierung:

Jede Abteilungsleitung bzw. jede/r GPV hat Informationen über Ereignisse, die sich auf die Festlegung des Löscharbeitsbedarfs auswirken können, an andere Abteilungen weiterzugeben, wenn davon auszugehen ist, dass andere Abteilungen personenbezogene Daten vorhalten, die von diesem Ereignis betroffen sein können. Ggf. ist eine vorübergehende Löscharbeitsbarriere auszusprechen. Dies betrifft insbesondere, jedoch nicht ausschließlich folgende Sachverhalte: Rechtsstreitigkeiten mit Kunden, Lieferanten, Mitarbeitern und anderen Parteien; Geltendmachung von Gewährleistungs- und Garantiesprüchen; Bearbeitung von Schadensfällen und Geltendmachung von Versicherungsansprüchen; Aufklärung von Betrugshandlungen.

## 5. Kenntnis der maximalen Aufbewahrungszeiträume

Wie bereits unter III.1. geschildert, können die anwendbaren Rechtsnormen anstelle von oder ergänzend zu Mindestaufbewahrungsfristen auch maximale Aufbewahrungszeiträume vorsehen. Das bedeutet, dass bei Erreichen des Endzeitpunkts eine weitere Verarbeitung bzw. Speicherung grundsätzlich nicht zulässig ist und die personenbezogenen Daten zwingend zu löschen sind. Jede Fachabteilung sollte sich also darüber informieren, ob es eine derartige Obergrenze gibt, und diese in angemessener Weise intern dokumentieren und kommunizieren.

#### Musterformulierung:

Zusätzlich zu den Mindestaufbewahrungsfristen hat jede Abteilungsleitung bzw. jede/r GPV für jede Kombination aus Einsatzzweck und Art der Daten zu ermitteln, ob die für den Zweck bzw. Bearbeitungsprozess anwendbaren Rechtsnormen einen maximalen Aufbewahrungszeitraum vorschreiben. Sofern eine derartige Vorschrift besteht, sind der Zeitraum und seine Berechnungsmethode zu dokumentieren und den relevanten Mitarbeitern in angemessener Weise zu vermitteln.

## 6. Prüfrhythmus

Grundsätzlich wäre es sinnvoll, wenn bereits bei Entstehung der personenbezogenen Daten, d.h. bei Eintreffen oder Absenden einer E-Mail oder beim Abspeichern einer Datei, das Löscharbeitsdatum ermittelt werden könnte. Allerdings wird zu diesem Zeitpunkt das Löscharbeitsdatum vielfach noch nicht ermittelbar sein, da die Einflussfaktoren entweder noch nicht feststehen oder sich im Zeitablauf ändern können. Ein ursprünglich zeitlich befristeter Dienstleistungsvertrag könnte z.B. verlängert werden, sodass damit in Verbindung stehende Unterlagen über den ursprünglich vorhergesagten Zeitpunkt hinaus aufbewahrt werden können oder müssen. Es stellt sich also die Frage, zu welchen Zeitpunkten oder in welchen Abständen der Löscharbeitsbedarf zu ermitteln ist.

<sup>25</sup> Vgl. Arning (o. Fußn. 6), der eine tägliche Überprüfung schon aus Praktikabilitätsgründen verwirft; Brüggemann, in: Auernhammer (o. Fußn. 16), Art. 25 Rdnr. 19 gesteht Verantwortlichen einen Gestaltungsspielraum bei der Ausgestaltung eines Löscharbeitskonzepts zu.

<sup>26</sup> S. hierzu Erwägungsgrund 39 Satz 10 DS-GVO, wonach Verantwortliche Fristen für eine regelmäßige Überprüfung vorsehen sollten; bei Kühling/Seidell/Sivridis, Datenschutzrecht, 3. Aufl., S. 226 Rdnr. 536 wird – noch in Bezug auf das BDSG a.F. – von einer turnusmäßigen Prüfung gesprochen.

<sup>27</sup> Plath, DS-GVO/BDSG, 3. Aufl. 2018, Art. 5 Rdnr. 18 hält aus Zumutbarkeitsgründen „typisierte Regelprüffristen“ für angebracht.

Gem. Art. 24, 25 und 32 DS-GVO muss der Verantwortliche seine technischen und organisatorischen Maßnahmen, also auch die Maßnahmen zur Ermittlung des Löscharbeitsbedarfs, an der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen orientieren.

Insofern erscheint es angebracht, wenn die Ermittlung des Löscharbeitsbedarfs nicht für jedes personenbezogene Datum permanent durchgeführt wird<sup>25</sup>, sondern in regelmäßigen Abständen.<sup>26</sup> Das bedeutet auch, dass es unterschiedliche Prüfrhythmen geben kann.<sup>27</sup> Eine interne Rahmenrichtlinie sollte zumindest einen für alle Abteilungen und personenbezogenen Daten einheitlichen Mindestrhythmus vorschreiben, um zu vermeiden, dass Abteilungen unverhältnismäßig lange Prüfrhythmen festlegen.

#### Musterformulierung:

Jede Abteilungsleitung bzw. jede/r GPV hat für die in seinem/ihrer Verantwortungsbereich liegenden personenbezogenen Daten festzulegen, in welchen Abständen der Löscharbeitsbedarf ermittelt wird. Bei der Festlegung sind u.a. die folgenden Kriterien zu berücksichtigen: Kosten, Verarbeitungszweck und Sensibilität der personenbezogenen Daten. Ggf. sind für unterschiedliche Arten von Daten oder für unterschiedliche Verarbeitungszwecke individuelle Prüfrhythmen zu definieren. Eine Überprüfung ist mindestens einmal jährlich für sämtliche unstrukturiert gehaltenen personenbezogenen Daten durchzuführen; kürzere Intervalle sind möglich und ggf. notwendig.

## 7. Zuständigkeiten und Delegation

Hinsichtlich der Ermittlung des Löscharbeitsbedarfs ist eine eindeutige Festlegung der Zuständigkeiten notwendig, da ansonsten die Gefahr besteht, dass die erforderlichen Überprüfungen nicht stattfinden. Unter IV.1. wurde bereits erläutert, wie die Leitungsebene des Verantwortlichen eine grundsätzliche Delegation an Abteilungen und Mitarbeiter vornehmen kann. Allerdings macht es Sinn, in Abhängigkeit von den Zugriffsmöglichkeiten auf bestimmte Datenbestände eine weitere Konkretisierung vorzunehmen. Gleichzeitig kann die Möglichkeit eingeräumt werden, eine Unterdelegation vorzunehmen.

#### Musterformulierung:

Die Zuständigkeit für die Überprüfung der unstrukturiert gehaltenen personenbezogenen Daten hinsichtlich ihres Löscharbeitsbedarfs wird wie folgt geregelt: Für Daten, die nur einem Mitarbeiter persönlich zugänglich bzw. zugeordnet sind, führt jeder Mitarbeiter die Überprüfung selbst durch. Dies betrifft insbesondere, aber nicht ausschließlich Nachrichten im eigenen E-Mail-Postfach, Dateien in lokalen Speichern auf dem persönlichen Arbeitsplatzrechner bzw. Mobilgerät, Dateien in den persönlichen Laufwerken im Firmennetz und Dateien auf mobilen Datenträgern, die einer Person direkt zugeordnet sind.

Für Daten, auf die mehrere Mitarbeiter gemeinsam als Abteilung oder Team Zugriff haben, liegt die Zuständigkeit bei der Abteilungsleitung bzw. Teamleitung. Eine Unterdelegation auf einzelne Mitarbeiter ist möglich; sie hat dann schriftlich zu erfolgen. Dies betrifft insbesondere, aber nicht ausschließlich Nachrichten in gemeinsam genutzten E-Mail-Postfächern sowie Dateien in Abteilungslaufwerken im Firmennetz oder auf gemeinsam genutzten Datenträgern.

## 8. Vorgehensweise nach der Ermittlung des Löscharbedarfs

Die Überprüfung unstrukturiert gehaltener personenbezogener Daten hinsichtlich ihres Löscharbedarfs kann zu verschiedenen Ergebnissen führen. So könnte z.B. festgestellt werden, dass ein bestimmtes personenbezogenes Datum sofort zu löschen ist. Für diesen Fall müssen entsprechende Vorgehensweisen zur Datenlöschung definiert sein, die dann zur Anwendung kommen.

Ein anderes Ergebnis der Überprüfung kann lauten, dass eine Löschung aus bestimmten Gründen noch nicht erfolgen darf. Dann bietet es sich an, anhand der bei der Überprüfung gewonnenen Erkenntnisse das voraussichtliche Löschardatum zu prognostizieren, sofern dies möglich ist. Auch die Gründe, die einer Löschung zum aktuellen Zeitpunkt entgegenstehen, sollten dokumentiert werden, sodass bei einer erneuten turnusmäßigen Überprüfung diese Informationen direkt verfügbar sind.

### Musterformulierung:

Wenn die Ermittlung des Löscharbedarfs ergeben hat, dass eine Löschung von personenbezogenen Daten unmittelbar vorzunehmen ist, sind die dieser Rahmenrichtlinie beigefügten Unterlagen zu beachten, in denen die technischen und organisatorischen Maßnahmen zur Durchführung der Löschung geregelt sind. Wenn eine Löschung noch nicht erfolgen darf, sollten die entgegenstehenden Gründe dokumentiert werden. Das Löschardatum sollte – wenn möglich – prognostiziert werden. Dabei ist nicht zwingend eine exakte Tagesangabe erforderlich. Eine näherungsweise Angabe wie z.B. „nach dem nächsten Jahresabschluss“ ist möglich. Die genauen Modalitäten zur Dokumentation hat die jeweilige Abteilungsleitung bzw. der/die GPV festzulegen. Sofern eine Löschung noch nicht erfolgen darf, sind die personenbezogenen Daten bei der nächsten routinemäßigen Überprüfung erneut zu betrachten.

Die Dokumentation des prognostizierten Löschardatums richtet sich danach, welche technischen Möglichkeiten bestehen bzw. welche Softwaresysteme eingesetzt werden. Bei bestimmten Windows-Dateitypen (z.B. jpg, xlsx, docx) ist es z.B. möglich, diese Information in den Dateieigenschaften zu hinterlegen. Die Dateieigenschaften können dann für spätere routinemäßige Über-

prüfungen im Windows-Dateiexplorer als Zusatzspalten eingeblendet werden. Alternativ besteht auch die Möglichkeit, Datei- bzw. Verzeichnisnamen mit einem Zusatz zu versehen wie etwa „ab ... zu löschen“. Vergleichbare Möglichkeiten bieten E-Mail-Programme wie Outlook und Gmail, in denen man E-Mails verschiedenen selbst definierten Kategorien zuordnen kann.

## 9. Flankierende Maßnahmen

Mit den o.g. Anweisungen der Unternehmensleitung werden die jeweiligen Abteilungsleitungen bzw. GPV dazu angehalten, die technischen und organisatorischen Maßnahmen festzulegen, sodass eine Einschätzung über die Notwendigkeit einer Datenlöschung im Einzelfall möglich wird.

Damit die Anweisungen tatsächlich eingehalten werden und nicht im Alltag unberücksichtigt bleiben, sollten von der Leitungsebene des Verantwortlichen entsprechende Vorkehrungen getroffen werden. So könnte die Einhaltung der Rahmenrichtlinie als Zielvereinbarung in die variable Vergütung der Führungskräfte aufgenommen werden, sofern die Einhaltung messbar ist. Weiterhin haben Datenschutzbeauftragte die Möglichkeit, eine Überprüfung i.S.d. Art. 39 Abs. 1 lit. b DS-GVO dahingehend durchzuführen, ob die Abteilungsleitungen bzw. GPV ihren Aufgaben nachgekommen sind.

## 10. Fazit

Das komplexe Thema der Löscharpflichten wird durch Fokussierung auf jeweils einzelne Bausteine praktikabel. Mit der Erstellung einer Rahmenrichtlinie für die routinemäßige Löschung unstrukturiert gehaltener personenbezogener Daten können einzelne Teilaufgaben an untere Ebenen delegiert werden. Auf diese Weise wird vermieden, dass Verantwortliche – quasi am grünen Tisch – praxisferne Vorgaben definieren, die dann im Alltag kaum handhabbar sind. Vielmehr werden alle Beteiligten in den Prozess eingebunden, sodass für jeden eine Teilaufgabe besteht, die bewältigt werden kann.



Dipl.-Kfm. (FH) Achim Gründel

ist langjähriger Interner Revisor bei Veolia Umweltservice in Hamburg und wurde dort zudem als Datenschutzbeauftragter für eine Konzerngesellschaft benannt.