Baustein 60 „Löschen und Vernichten“

Version: V1.0a
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V2.0_Löschen_und_Vernichten_V1.0	30. Juni 2020	1. September 2020
SDM-V2.0_Löschen_und_Vernichten_V1.0a	2. September 2020	

1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDM-V2b-Methodik-Handbuch, Teil B):

Anforderungen der DS-GVO	Gewährleistungsziele
Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)	Nichtverkettung
Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)	Datenminimierung
Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)	Integrität
Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO)	Datenminimierung
Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO)	Vertraulichkeit
Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO)	Intervenierbarkeit

2. Beschreibung

Der Begriff „Löschen“ beschreibt das Unkenntlichmachen gespeicherter personenbezogener Daten. Der Vorgang des Löschens muss also bewirken, dass nach dem Löschen keine Daten mehr vorhanden sind, mit denen eine natürliche Person identifiziert werden kann. Der personenbezogene Informationsgehalt gelöschter Daten darf daher nicht, oder nach allgemeinem Ermessen nur unwahrscheinlich (Erwägungsgrund 26 der DS-GVO), reproduzierbar sein. Art. 17 Abs. 3 DS-GVO bleibt davon unberührt. Die Löschung eines Datums ist erst dann vollzogen, wenn auch keine Kopie oder Replikation dieses Datums mehr bei dem Verantwortlichen oder einem möglichen Auftragsverarbeiter gespeichert ist.

Der Begriff „Vernichtung“ beschreibt hingegen die Zerstörung des Datenträgers, unabhängig davon, ob es sich um analoge Datenträger oder digitale Datenträger handelt. Vernichtung stellt somit eine unwiderrufliche Form des Löschens dar.

Das Löschen dient der Umsetzung mehrerer Gewährleistungsziele. So unterstützt das Löschen von Daten die Gewährleistungsziele Datenminimierung und Vertraulichkeit. Gelöschte Daten stehen zudem auch nicht mehr für mögliche personenbezogene Verkettungen zur Verfügung (Nichtverkettung). Das Löschen dient auch der Gewährleistung der Intervenierbarkeit, weil betroffenen Personen die Möglichkeit gegeben wird, falsche oder unzulässige bzw. zu lange gespeicherte Daten löschen zu lassen und sie so der dann unrechtmäßigen Verarbeitung zu entziehen.

Personenbezogene Daten MÜSSEN auf Verlangen der betroffenen Person gelöscht werden, sofern die Voraussetzungen des Art. 17 Abs. 1 DS-GVO vorliegen. Darüber hinaus sind diese Daten unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig durch den Verantwortlichen unverzüglich zu löschen. Eine Löschung hat zu erfolgen, wenn

- die Notwendigkeit der Verarbeitung zur Zweckerreichung entfallen ist,
- eine Einwilligung widerrufen wurde und es keine anderweitige Rechtsgrundlage für die Verarbeitung gibt,
- die betroffene Person in bestimmten Fällen Widerspruch gegen die Verarbeitung eingelegt hat und – außer bei Direktwerbung – keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen,
- die personenbezogenen Daten unrechtmäßig verarbeitet wurden,
- die Löschung zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, dem der Verantwortliche unterliegt, oder
- die personenbezogenen Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben wurden.

Wenn es gesetzlich vorgegebene maximale Speicherfristen gibt, MÜSSEN Verantwortliche und Auftragsverarbeiter die Daten nach Ablauf der Fristen unaufgefordert löschen. Andernfalls sind solche Fristen soweit möglich festzulegen und umzusetzen.

Das „Recht auf Vergessenwerden“ gemäß Art. 17 Abs. 2 DS-GVO bezieht sich, obwohl der Begriff im ErwGr. 65 als Synonym für „Löschung“ verwendet wird, auf die Tilgung (von Spuren) personenbezogener Daten, die durch Veröffentlichungen, insbesondere im Internet, der Öffentlichkeit zugänglich sind. Der Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat und der gemäß Art. 17 Abs. 1 DS-GVO zunächst selbst zu deren Löschung verpflichtet ist, MUSS unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten (gleichfalls) verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung alle Verweise zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Die Pflicht zur Löschung betrifft nicht nur den aktiven Datenbestand sondern grundsätzlich auch personenbezogene Daten in **Sicherungskopien**. Soweit Protokolldaten personenbezogene Daten enthalten, unterliegen auch diese der Löschpflicht. Die Speicherung von **Protokolldaten** basiert häufig auf anderen Rechtsgrundlagen als die der Daten, die in der eigentlichen Verarbeitung verwendet werden (siehe Baustein Protokollierung). Sie sind an besondere Zweckbindungen und in der Regel auch an gesonderte Speicherfristen geknüpft. In Protokolldaten können bspw. Daten von Beschäftigten des Verantwortlichen oder des Auftragsverarbeiters enthalten sein, für die weitere rechtliche Regelungen zu beachten sind. Schließlich ist auch darauf zu achten, dass aus verarbeitungstechnischen Gründen erzeugte **temporäre Daten** gelöscht werden, soweit diese nicht ohnehin ihrer temporären Natur gemäß vorher automatisch gelöscht wurden.

Dabei muss darauf geachtet werden, dass das automatisierte Löschen von temporären Dateien in der Regel nur ein Austragen aus dem Dateisystem ist.

Der Verantwortliche muss zudem sicherstellen, dass die Löschpflichten auch für die Datenbestände eingehalten werden, die bei seinen Auftragsverarbeitern verarbeitet werden.

In Abhängigkeit vom Risiko, das aus der Verarbeitung der zu löschenden Daten resultiert, der Menge der zu löschenden Daten und der Art der Datenträger kommen daher verschiedene Methoden in Betracht (Die folgende Liste ist als abgestufte Aufzählung zu verstehen. In der Reihenfolge nimmt der Aufwand für die Rekonstruierung zu.):

- Austragen aus elektronischen Verzeichnissen bzw. Tabellen und anschließender Reorganisation bspw. durch Datenbank-Löschbefehle mit anschließender Reorganisation der Datenbank, soweit gesichert ist, dass im Zuge der Reorganisation die zu löschenden Daten überschrieben werden,
- Überschreiben der Informationen einzelner Datenfelder (Daten oder Attribute von Daten), die auf elektronischen Datenträgern gespeichert wurden, mit Hilfe von Löschprogrammen (bspw. so genannte Wipe-Tools),
- komplettes Überschreiben ganzer Datenträger mit speziellen Lösch- oder Anwendungsprogrammen (Dabei ist auch sicherzustellen, dass diese für die Verwendung mit den jeweiligen Datenträgern geeignet sind und z. B. Wear-Levelling-Algorithmen von Flashspeichern berücksichtigen.),
- physikalische Zerstörung (Vernichtung) des Datenträgers (bspw. Papier, Festplatten, SSD-Speicher) durch mechanisches Zerkleinern (Schreddern), Einschmelzen oder Verbrennen.

Um einer Löschverpflichtung zu entsprechen, reichen bspw. folgende Maßnahmen nicht aus:

- in Abhängigkeit vom Einzelfall: Austragen aus elektronischen Verzeichnissen bzw. Tabellen bspw. durch Löschbefehle von Betriebssystemen (z. B. Kommandos wie Delete, Erase),
- Schnellformatieren von Datenträgern,
- Freigabe von Datenträgern (z. B. eines USB-Sticks) zur Wiederverwendung durch Organisationsanweisung,
- Aussprechen eines Verbots der Kenntnisnahme und Nutzung der Daten an Mitarbeiter/-innen der Verantwortlichen oder
- Zusage des Verantwortlichen, Daten nicht mehr verwenden zu wollen.

Um Daten wirksam löschen zu können, sind Maßnahmen auf der Ebene der Daten, der technischen Systeme und der dazugehörigen Prozesse erforderlich.

Daten

Die Struktur der Daten und die Art der Speicherung müssen so gestaltet sein, dass das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten mit beherrschbarem Aufwand möglich ist (M60.D01). Das Löschen muss möglich sein,

ohne die Integrität des verbleibenden Datenbestandes und ohne besondere Zweckbindungsregelungen (bspw. von Protokolldaten, die der Datenschutzkontrolle dienen) zu beeinträchtigen (M60.D02). Die Granularität, in der Daten gespeichert werden und vor allem löschbar sind, hängt maßgeblich vom Risiko, das aus der Verarbeitung der Daten resultiert, vom Zweck der Erhebung und von der weiteren Verwendung der Daten ab. Je höher das Risiko für betroffene Personen ist, desto präziser müssen Daten löschbar sein. Das schließt jedoch nicht aus, dass etwa besonders hohes Risiko auch ein summarisches Löschen aller auf eine Person bezogener Daten erfordern kann, das ein feingranulares Differenzieren entbehrlich macht.

Systeme und Dienste

Die technischen Systeme zur Umsetzung der vom Verantwortlichen angeordneten Löschung hängen neben dem Schutzbedarf maßgeblich von der Art und Weise des jeweiligen Datenträgers ab, auf dem die Daten gespeichert sind. Sie müssen in jedem Fall so gestaltet sein, dass sie die gesetzlich geforderten Löschvorgänge technisch realisieren können. Im Ergebnis müssen die technischen Systeme sicherstellen, dass der vom Gesetz verlangte und vom Verantwortlichen oder vom Auftragsverarbeiter mit der Löschung angeordnete Informationsverlust auch tatsächlich wirkt. Auf die Details der einzelnen Verarbeitungstätigkeiten zur Löschung personenbezogener Daten bzw. Vernichtung der entsprechenden Datenträger wird hier nicht näher eingegangen (M60.S01, M60.S02, M60.S03). Hierzu wird auf die entsprechenden Maßnahmen des IT-Grundschutz-Kompendiums des BSI in der jeweils aktuellen Fassung verwiesen, z. B. „Auswahl geeigneter Verfahren zur Löschung und Vernichtung von Daten“. Auch auf konkrete Empfehlungen zu verwendbaren Löschprogrammen wird an dieser Stelle verzichtet. Stattdessen wird auf verschiedene Veröffentlichungen des BSI verwiesen. So gibt das IT-Grundschutz-Kompendium einen Überblick über Methoden zur Löschung von Daten und zur Vernichtung von Datenträgern und differenziert dabei nach dem Schutzbedarf der zu löschenden Daten. Die Erläuterungen des BSI zum richtigen Löschen in seinem Online-Angebot „BSI für Bürger“ richten sich zwar vorwiegend an Bürgerinnen und Bürger, sind aber auch im hier geltenden Kontext lesenswert.

Die technischen Systeme müssen in der Lage sein, Löschungen durchzuführen, ohne die Integrität des verbleibenden Datenbestandes zu beeinträchtigen (M60.S04). Dazu gehört auch, dass die unbefugte Löschung verhindert wird oder zumindest die Tatsache der Löschung nachträglich nachweisbar ist (M60.S05). Soweit das Löschen selbst wieder protokolliert wird, dürfen in diesen Protokollen keine Daten enthalten sein, für die eine Löschverpflichtung besteht (M60.S06).

Um gesetzlich vorgegebene Löschfristen automatisiert überwachen zu können, sind technische Systeme geeignet, die entsprechende Zeitstempelsysteme beinhalten oder nutzen können (M60.S07). Zumindest sind solche Systeme erforderlich, die eine Zuordnung zwischen Daten, ggf. der Kategorie, der sie zuzuordnen sind, und dem zeitlichen Anknüpfungspunkt für die Löschverpflichtung speichern und nutzen können. Sind die zu löschenden Daten mit entsprechenden Attributen versehen, müssen die technischen Systeme geeignete Auswertungsmöglichkeiten bereitstellen, mit denen die Löschfristen überwacht werden (M60.S08).

Sofern Löschungen nach bestimmten systematischen Vorgaben erfolgen, sollten die technischen Systeme den Vorgang des Löschens automatisiert durchführen können (M60.S09).

Alle Forderungen in Bezug auf die Löschung von Daten müssen grundsätzlich auch bei allen Kopien und Datensicherungen umgesetzt werden können. Das bedeutet jedoch nicht, dass in jeder Kopie und jedem Backup Daten zum gleichen Zeitpunkt wie im Originaldatenbestand gelöscht werden muss, da das Löschen von Daten in Sicherungskopien in der Regel mit einem wesentlich höheren Zeitbedarf als das Löschen im aktiven Datenbestand verbunden ist. Falls der Zeitbedarf für ein unverzügliches und integritätssicherndes Löschen so hoch ist, dass der Zeitpunkt dieser Löschung mit einem planmäßigen Überschreiben oder der Vernichtung eines Datenträgers als Ganzem zusammen fallen würde, kann die Löschung in diesem Zuge erfolgen. In jedem Fall muss sichergestellt werden, dass nach einer Rücksicherung (etwa nach einem Havariefall) und einer damit verbundenen Wiederherstellung von Daten, die im aktiven Datenbestand bereits gelöscht waren, unmittelbar eine erneute Löschung dieser Daten erfolgt, und somit ausgeschlossen wird, dass diese Daten wieder für die Verarbeitung herangezogen werden (M60.S10).

Hinweise zur Auswahl technischer Systeme zur Vernichtung von Datenträgern können auch der technischen Norm DIN 66399-1 und DIN 66399-2 „Vernichten von Datenträgern“ entnommen werden. Für das Löschen personenbezogener Daten sind Maßnahmen der Sicherheitsstufe 4 oder höher dieser Norm geeignet.

Neben der maximalen Partikelgröße, die beim Vernichten erreicht wird, wird der Aufwand für die Rekonstruierbarkeit der Informationen auch durch weitere sicherheitstechnische Rahmenbedingungen des Vernichtungsprozesses beeinflusst. Hierzu zählen etwa Verwirbeln, Verpressen oder Verbrennen von Vernichtungsrückständen. Für die Materialklassen Papier und Film kann so durch Vermischen und Verpressen die Sicherheitsstufe 3 auf die Sicherheitsstufe 4 angehoben werden, wenn eine Mindestmenge von 100 kg an Datenträgern in einem Durchgang ununterbrochen in der Maschine oder Einrichtung vernichtet wird. Der Verantwortliche kann in diesem Fall die Sicherheitsstufe anheben, wenn aufgrund der sicherheitsrelevanten Rahmenbedingungen des Vernichtungsprozesses das Gesamtrisiko für die Wiederherstellung von Daten tolerierbar ist. Die ergänzenden sicherheitstechnischen Maßnahmen sind in diesen Fällen detailliert zu dokumentieren und sollten vertraglich festgeschrieben werden, wenn für die Aktenvernichtung ein Dienstleister (Auftragsverarbeiter) beauftragt wird.

Prozesse

Eine wesentliche Voraussetzung für die ordnungsgemäße Funktion von Löschprozessen ist die Festlegung von Löschfristen (M60.P01). Diese MÜSSEN schriftlich festgelegt und nach den Vorgaben der DS-GVO in das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO aufgenommen werden (M60.P02). Ausgangspunkt für die Festlegungen sind, soweit einschlägig vorhanden, die gesetzlich vorgegebenen Speicherfristen. Aufgrund und im Rahmen ihrer aus der DS-GVO ergebenden Verpflichtungen sollen der Verantwortliche und der Auftragsverarbeiter in einem Löschkonzept festlegen, wie sie die datenschutzrechtlichen Pflichten zur Löschung personenbezogener Daten erfüllen wollen (M60.P03). Hilfreich

hierfür ist die technischen Norm DIN 66398 („Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“). Sie empfiehlt unter anderem, in einem Löschkonzept die Löschregeln mit den Löschfristen sowie den Startzeitpunkten, ab denen die Frist zu laufen beginnt, festzuschreiben.

Darüber hinaus MUSS ein Berechtigungs- und Rollenkonzept erstellt werden, auf dessen Basis ein in einem Löschkonzept beschriebener organisatorischer Prozess steuert, welche Personen des Verantwortlichen oder des Auftragsverarbeiters für die Prüfung, Anordnung und Durchführung von Löschungen zuständig sind. Dies kann von besonderer Bedeutung sein, wenn sich das Löschen personenbezogener Daten auch auf einen bestimmten Personenkreis bzw. bestimmte Rollen innerhalb des Verantwortlichen oder des Auftragsverarbeiters bezieht.

Das Löschen und Vernichten von Datenträgern erfordert Prozesse, die abhängig sind von der Art der zu vernichtenden Datenträger und vom Risiko, das aus der Verarbeitung der zu löschenden Daten resultiert. Die Auswahl geeigneter Löschmechanismen sowie das Löschen selbst sind Teil des Datenschutzmanagement-Prozesses und sollten verarbeitungsübergreifend auf Organisationsebene geplant und gesteuert werden. Weitere Hinweise zur Prozessgestaltung bei der Vernichtung enthält das Dokument DIN SPEC 66399-3.

Für das Löschen von Protokolldaten sind gesonderte Prozesse einzurichten (M60.P04).

Um die Löschpflichten für die Datenbestände bei Auftragsverarbeitern umsetzen zu können, sind vertragliche Regelungen und verbindliche Weisungen erforderlich (M60.P05). Unter bestimmten Voraussetzungen trifft die Pflicht zur Löschung auch die Auftragsverarbeiter direkt (siehe bspw. Art. 28 Abs. 10 DS-GVO).

Sofern das Löschen nach fest vorgegeben Regeln erfolgt (etwa Löschen von Daten bestimmter Zeitscheiben), MUSS geprüft werden, ob diese Prozesse automatisiert ablaufen können. In diesem Zusammenhang sind weitere Prozesse erforderlich, die jederzeit ein gezieltes Aussetzen und Unterbrechen automatisierter Löschprozesse ermöglichen (M60.P06).

Bei der Auswahl der konkreten Löschmaßnahme ist zudem zu berücksichtigen, aus welchem Grund die Löschung erfolgt (M60.P07). So können bspw. strengere Maßstäbe anzulegen sein, wenn ein Datenträger die Organisation verlässt, als wenn nach einem Verarbeitungsschritt temporäre Daten gelöscht werden müssen.

Um beim Wiedereinspielen von Daten aus Backups das Überschreiben bereits gelöschter Daten zu verhindern, MÜSSEN entsprechende Überwachungsprozesse eingerichtet werden (M60.P08).

Das Löschen verschlüsselter Daten erfordert spezielle Regeln und Prozesse zum Umgang mit diesen Daten und den dazugehörigen Verschlüsselungsschlüsseln (M60.P09, M60.P10).

Um das in der DS-GVO normierte Recht auf Vergessenwerden umzusetzen, muss durch entsprechende Prozesse auch nachvollziehbar sein, wann welche personenbezogenen Daten veröffentlicht wurden (M60.P11, M60.P12). Darüber hinaus müssen Strategien vorhanden

sein, die beschreiben, wie mögliche Datenempfänger über die an den Verantwortlichen gerichteten Anträge zur Löschung dieser Daten informiert werden (M60.P13).

Durch geeignete Prozesse muss weiterhin sichergestellt werden, dass eine Löschung alle Kopien erfasst, also bspw. auch auf mobilen Geräten vorgehaltene Offline-Kopien oder Kopien in Cloud-Strukturen (M60.P14).

3. Differenzierung bei hohem Schutzbedarf

Die technischen und organisatorischen Maßnahmen zum Löschen müssen dem Schutzbedarf der betroffenen natürlichen Personen und somit dem Risiko, das aus der Verarbeitung der Daten resultiert, angemessen sein. Um diese Forderung praktisch umsetzen zu können, sind Risiken zu klassifizieren. Diese grundsätzliche Forderung berücksichtigt bspw. die Norm DIN 66399 („Vernichten von Datenträgern“), indem sie jedem Verantwortlichen und jedem Auftragsverarbeiter empfiehlt, alle im Geschäftsverkehr vorkommenden oder anfallenden Informationen (Daten) bzw. die sie speichernden Datenträger zunächst hinsichtlich des Schutzbedarfs in drei Schutzklassen zu klassifizieren. Sieben Sicherheitsstufen beschreiben zudem Anforderungen an die Wirksamkeit der Vernichtung, d. h. die Höhe des Aufwands für Angreifer, vernichtete Datenträger bzw. darauf gespeicherte Daten wiederherzustellen und Information zur Kenntnis nehmen zu können. Die Norm sieht vor, Datenträger bestimmter Schutzklassen nur nach bestimmten Sicherheitsstufen zu vernichten. Die Norm kann helfen, dem o. g. Prinzip der Angemessenheit Rechnung zu tragen. Für das Löschen von Daten, deren Verarbeitung zu einem sehr hohen Schutzbedarf führt, sind in der Regel Maßnahmen ab der Sicherheitsstufe 4 relevant.

Auch für elektronisch gespeicherte Daten hängt die Auswahl von Löschmaßnahmen vom Risiko ab, das durch die Verarbeitung der betreffenden Daten entsteht. Löschen elektronisch gespeicherter Daten kann durch das gezielte Überschreiben einzelner Datenfelder bzw. größerer zu löschender Speicherbereiche oder durch ein Überschreiben des gesamten Datenträgers mit Hilfe spezieller Löschprogramme bewirkt werden. Hoher Schutzbedarf stellt jedoch besondere Anforderungen an solche Löschprogramme. Unter bestimmten Voraussetzungen kann es angebracht sein, die Integrität von Löschtools durch gesonderte Maßnahmen sicherzustellen (bspw. Signaturverfahren). Der gesamte Einsatz von Löschprogrammen im Bereich des hohen Schutzbedarfs erfordert einen standardisierten Prozess, der die einzelnen Löschschritte detailliert beschreibt und so zu vollständig standardisierten Abläufen führt. Dies beinhaltet auch eine lückenlose Dokumentation von Löschvorgängen. Die Dokumentation von Löschvorgängen darf jedoch keine Inhaltsdaten enthalten, die zu löschen sind (siehe M60.S06). Dies würde den Löschvorgang konterkarieren.

Sollen Daten gelöscht werden, deren Verarbeitung zu einem hohen Risiko führt, sind auch besondere Anforderungen an die Löschung von deren Sicherungskopien zu stellen. Das Löschen kann bei hohem Schutzbedarf ein „außerplanmäßiges Aufräumen“ von Backups erfordern. Die Integrität der Backups darf hierdurch jedoch nicht gefährdet werden. Das Erstellen eines neuen Backups und Löschen des alten Backups scheidet in der Regel aus, da damit bei zwischenzeitlich erfolgten fehlerhaften oder unbefugten Änderungen auch hier der korrekte Stand aus dem Backup entfernt wird. Kommt auch das selektive Löschen im

Backup nicht in Betracht, kann beispielsweise ein Prozess implementiert werden, mit dem Datenbestände in ein zu diesem Zweck vorgehaltenes System eingespielt, teilweise gelöscht und die verbleibenden Daten erneut gesichert werden. Je höher der Schutzbedarf ist umso höher ist die Frequenz dieser „Korrekturläufe“ zu wählen. Die konkrete Ausgestaltung dieses Prozesses hängt vom jeweiligen Einzelfall ab. Selbstverständlich MÜSSEN auch die ursprünglichen Backup-Medien irreversibel gelöscht werden.

Zahlreiche Beispiele für hohen Schutzbedarf sind im medizinischen Bereich zu finden. Bei Gesundheitsdaten handelt es sich in der Regel um Daten aus dem Katalog der besonderen Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO. Ärztliche Aufzeichnungen zu medizinischen Behandlungen (z. B. Anamnese, Aufnahme- und Aufklärungsbögen, Befunde, Medikation, Pflegeanordnungen, Arztbriefe, EKG, EEG, CTG, histologische Berichte, OP-Berichte) sind gemäß § 10 Abs. 3 MBO (Stand 2015) bzw. § 630f BGB für die Dauer von 10 Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Vergleichbar hohe Anforderungen können auch bei anderen Berufsgeheimnisträgern vorhanden sein, die der Schweigepflicht nach § 203 StGB unterliegen.

4. Referenzen

DSK: *Kurzpapier Nr. 11 (Recht auf Löschung / Recht auf Vergessenwerden)*
https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Kurzpapiere/Kurzpapier_Nr_11.pdf

BSI: *BSI-Grundschutzkompendium, Baustein CON.6: Löschen und Vernichten* (*https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_6_L%C3%B6schen_und_Vernichten.html*; Stand 1. Februar 2020), insbesondere
- *CON.6.A3 Löschen der Datenträger vor und nach dem Austausch,*
- *CON.6.A4 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern,*
- *CON.6.A5 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern,*
- *CON.6.A10 Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten und*
- *CON.6.A11 Vernichtung von Datenträgern durch externe Dienstleister.*

Daten auf Festplatten richtig löschen
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html (Stand 03/2020)

Technische Normen: *DIN 66399-1, DIN 66391-2 und DIN 66399-3*
DIN 66398

5. Zusammenfassung der Maßnahmen

Die einzelnen Maßnahmen können hinsichtlich des Anwendungsbereichs unterschieden werden nach Maßnahmen, welche primär auf einzelne Verarbeitungen angewandt werden

sollten (*kursive Darstellung*) und solche, welche primär die gesamte Organisation betreffen und damit im Rahmen des Datenschutzmanagements gebündelt und verwaltet werden sollten. Weiterhin sind alle Maßnahmen grob den PDCA-Phasen des Datenschutzmanagement-Prozesses (siehe SDM-Methode) zugordnet. Maßnahmen, die in früheren Versionen des Bausteins enthalten waren, aber in einer nachfolgenden Version ungültig wurden, werden weiterhin aufgeführt (~~durchgestrichene Darstellung~~). Damit bleibt die Nummer einer Maßnahme bei einer neuen Version erhalten. Die Spalte „Gültigkeit“ gibt an, seit welcher Version die Maßnahme in der enthaltenen Form gültig ist. Bei ungültigen Maßnahmen enthält diese Spalte die Versionsnummer des Bausteins, in der die Maßnahme letztmalig gefordert bzw. empfohlen wurde.

Ebene Daten

Nr.	Maßnahme	PDCA	Gültigkeit
M60.D01	*Datenstrukturen und Speicherarten, die das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten in einer vom Schutzbedarf abhängigen Granularität ermöglichen*	P, D	V1.0
M60.D02	*Strukturen von Daten und Datenmodellen dergestalt, dass das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten die Integrität der verbleibenden Daten nicht gefährdet*	P, D	V1.0

Ebene Systeme

M60.S01	*Überschreiben von Daten, Datenfeldern, Datenattributen oder kompletten Datenträgern mit speziellen Löschprogrammen (Wipe-Tools)*	P, D	V1.0
M60.S02	*Schreddern zur Vernichtung von Datenträgern jeder Art*	D	V1.0
M60.S03	*Einschmelzen oder Verbrennen von Datenträgern jeder Art*	D	V1.0
M60.S04	*Integritätssicherung beim Löschen*	P, D	V1.0
M60.S05	Protokollierung von Löschungen	P, D	V1.0
M60.S06	Datensparsame Ausgestaltung der Protokollierung von Löschungen	P, D	V1.0
M60.S07	Automatisierte Überwachung von Löschfristen unter Nutzung von Zeitstempelsystemen oder Auswertungen entsprechender Löschattribute	D	V1.0
M60.S08	*Möglichkeiten der Zuordnung zwischen Daten und dem zeitlichen Anknüpfungspunkt für die Löschverpflichtung*	P, D, C	V1.0
M60.S09	Technische Systeme zur automatisierten, zeitgesteuerten Löschung unter Nutzung von Zeitstempelsystemen oder durch Auswertungen anderer Zuordnungssysteme oder entsprechende Löschattribute	P, D	V1.0

M60.S10	Technische Systeme, die bei einer Rücksicherung von Datenbeständen aus Backups oder Datensicherungen sicherstellen, dass Daten, die im Original gelöscht wurden, nicht weiter genutzt oder verarbeitet werden	P, D	V1.0

Ebene Prozesse

M60.P01	Festlegung von Löschfristen	P, D	V1.0
M60.P02	Dokumentation von Löschfristen (ggf. im Verzeichnis von Verarbeitungstätigkeiten)	P	V1.0
M60.P03	Löschkonzept	P	V1.0
M60.P04	Regelungen mit besonderen Löschvorgaben für Protokolldaten unter Berücksichtigung der speziellen Aufbewahrungs- und Zweckbindungsvorgaben	P	V1.0
M60.P05	Regelungen zum Löschen von Daten, die im Rahmen der Datenverarbeitung im Auftrag bei Auftragnehmern gespeichert sind	P	V1.0
M60.P06	Prozess zur zeitgesteuerten, automatisierten Löschung von Daten	D	V1.0
M60.P07	*Einbeziehung des Löschgrundes in die Auswahl eines Löschprozesses*	P	V1.0
M60.P08	Prozess zur Überwachung der Rücksicherung hinsichtlich möglicher Löschpflichten	P, D, C	V1.0
M60.P09	Regelungen zum Umgang mit Verschlüsselungsschlüsseln von zu löschenden (verschlüsselten) Daten	P	V1.0
M60.P10	Regeln zum Löschen von Verschlüsselungsschlüsseln	P	V1.0
M60.P11	Regelungen zur Dokumentation von Veröffentlichung von Daten	P	V1.0
M60.P12	Prozess zur Protokollierung der Übermittlung personenbezogener Daten	P, D	V1.0
M60.P13	Prozess zur Information möglicher Datenempfänger über die Pflicht zur Löschung dieser Daten	P, D	V1.0
M60.P14	*Dokumentation der Anzahl und des Speicherortes von Kopien*	P, D	V1.0

6. Bezug zum Datenschutzmanagement

Dieser Baustein bezieht sich in weiten Teilen auf Anforderungen des Löschens und Vernichtens von Daten in der gesamten Organisation und bildet Löschpflichten des Verantwortlichen ab, welche auf ein einzelnes Verfahren aber auch die gesamte Organisation angewendet werden können. Wird der Baustein auf die die gesamte Organisation angewendet, sind die getroffenen Maßnahmen im Datenschutzmanagement der Organisation zu betrachten.

7. Anmerkung zur Nutzung dieses Bausteins

Dieser Baustein darf – ohne Rückfrage bei einer Aufsichtsbehörde – kommerziell und nicht kommerziell genutzt, insbesondere vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt oder auch mit eigenen Daten und Daten Anderer zusammengeführt und zu selbständigen neuen Datensätzen verbunden werden, wenn der folgende Quellenvermerk angebracht wird:

„Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Veränderungen, Bearbeitungen, neue Gestaltungen oder sonstige Abwandlungen der bereitgestellten Daten sind mit einem Veränderungshinweis im Quellenvermerk zu versehen. Datenlizenz Deutschland – Namensnennung – Baustein Löschen und Vernichten (www.govdata.de/dl-de/by-2-0).“