Baustein 60 „Löschen und Vernichten“

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

Hinweis: Dieser Baustein wurde von den Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein und der Evangelischen Kirche Deutschlands zur Erprobung der SDM-Methode erarbeitet und veröffentlicht. Dieser Baustein ist keine Publikation der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

1. Bezug zu Gewährleistungszielen

Datensparsamkeit, Vertraulichkeit, Intervenierbarkeit, Nichtverkettung

2. Beschreibung

Im allgemeinen Sprachgebrauch beschreibt der Begriff „Löschen“ das Unzugänglichmachen von Daten und umfasst damit prinzipiell sowohl reversible wie auch irreversible Prozesse. Im juristischen Sinne ist Löschen das dauerhafte Unkenntlichmachen von gespeicherten personenbezogenen Daten mittels geeigneter Prozesse, die vom irreversiblen Unzugänglichmachen einzelner Daten bis zur physikalischen Zerstörung des gesamten Datenträgers (Vernichten) reichen. Dieser Baustein beschreibt die datenschutzrechtlichen Anforderungen im juristischen Sinne.

Der Vorgang des Löschens muss auf irreversible Weise bewirken, dass aus den gelöschten Daten selbst mit verhältnismäßig hohem Aufwand keine Informationen über bestimmte oder bestimmbare Personen mehr gewonnen werden können. Der Informationsgehalt gelöschter Daten darf somit nicht oder nur mit unverhältnismäßig hohem Aufwand reproduzierbar sein. Datenschutzrechtlich ist eine Löschung eines Datums erst dann vollzogen, wenn auch keine Kopie dieses Datums mehr bei dem Verantwortlichen oder einem möglichen Auftragsverarbeiter gespeichert ist.

Das Löschen dient der Umsetzung mehrerer Gewährleistungsziele. Dass das Löschen von Daten die Gewährleistungsziele Datensparsamkeit und Vertraulichkeit unterstützt, ist selbstverständlich. Gelöschte Daten stehen zudem auch nicht mehr für mögliche personenbezogene Verkettungen zur Verfügung (Nichtverkettung). Das Löschen dient auch der Gewährleistung der Intervenierbarkeit, weil Betroffenen 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 sind auf Verlangen der betroffenen Person und/oder unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig durch den Verantwortlichen unverzüglich zu löschen. Dies ist typischerweise dann der Fall, wenn die Notwendigkeit der Verarbeitung zur Zweckerreichung entfallen ist, eine Einwilligung widerrufen wurde, die betroffene Person in bestimmten Fällen Widerspruch gegen die Verarbeitung eingelegt hat und 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.

Soll lediglich der Personenbezug von gespeicherten Daten entfernt werden, so ist dies kein Löschen im Sinne dieses Bausteins.

Wenn es gesetzlich vorgegebene maximale Speicherfristen gibt, haben Verantwortliche und Auftragsverarbeiter die Daten nach Ablauf der Fristen unaufgefordert zu löschen. Andernfalls sind solche Fristen soweit möglich festzulegen und umzusetzen. Mit der Verpflichtung zur Löschung korrespondiert ein Anspruch des Betroffenen auf Löschung seiner Daten, sofern nicht wegen einer besonderen Art der Speicherung an die Stelle der Löschung eine „Einschränkung der Verarbeitung“ tritt (Art. 18 DS-GVO).

Das „Recht auf Vergessenwerden“ gem. 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, einer breiten Öffentlichkeit zugänglich sind.

Der Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat und der gemäß Art. 17 Abs. 1 DS-GVO zu deren Löschung verpflichtet ist, hat unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten an gemessene Maßnahmen, auch technischer Art, zu treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten (gleichfalls) verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links 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 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. Beispielsweise können in Protokolldaten 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.

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

In Abhängigkeit vom Schutzbedarf der zu löschenden Daten, der Menge der zu löschenden Daten und der Art der Datenträger kommen daher verschiedene Methoden in Betracht:

- 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),
- 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,
- physikalische Zerstörung (Vernichtung) des Datenträgers (bspw. Papier, Festplatten, SSD-Speicher) durch mechanisches Zerkleinern (Schreddern), Einschmelzen oder Verbrennen.

Um einer Löschverpflichtung im o. g. juristischen Sinne zu entsprechen, reichen beispielsweise folgende Maßnahmen nicht aus:

- Austragen aus elektronischen Verzeichnissen bzw. Tabellen bspw. durch Löschbefehle von Betriebssystemen (z. B. Kommandos wie Delete, Erase),
- Formatieren von Datenträgern,
- Freigabe von Datenträgern (z. B. eines USB-Sticks) zur Wiederverwendung durch Organisationsanweisung,
- Löschen des Entschlüsselungsschlüssels von verschlüsselt gespeicherten Daten; dies kann (in Abhängigkeit vom Kryptokonzept) allenfalls eine Maßnahme darstellen, um eine kurze Zeitspanne bis zur Löschung der Daten selbst oder bis zur physikalischen Vernichtung des Datenträgers zu überbrücken,
- Aussprechen eines Verbots der Kenntnisnahme und Nutzung der Daten an Mitarbeiter/-innen der verantwortlichen Stelle,
- 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 (M60.01) mit beherrschbarem Aufwand möglich ist, ohne die Integrität des verbleibenden Datenbestandes und ohne besondere Zweckbindungsregelungen (bspw. von Protokolldaten, die der Datenschutzkontrolle dienen) zu beeinträchtigen (M60.02). Die Granularität, in der Daten gespeichert werden und vor allem löschbar sind, hängt maßgeblich vom Schutzbedarf, vom Zweck der Erhebung und von der weiteren Verwendung der Daten ab. Je höher der Schutzbedarf der Daten ist, desto präziser müssen Daten löschbar sein. Das schließt jedoch nicht aus, dass etwa besonders hoher Schutzbedarf auch ein

summarisches Löschen aller auf eine Person bezogener Daten erfordern kann, das ein feingranulares Differenzieren entbehrlich macht.

Systeme

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 (M60.03, M60.04, M60.05) wird hier nicht näher eingegangen. Hierzu wird auf die entsprechenden Maßnahmen des BSI-Grundschutzkompendiums 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 BSI-Grundschutzkompendium 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 (M60.06). Dazu gehört auch, dass die unbefugte Löschung verhindert wird oder zumindest die Tatsache der Löschung nachträglich nachweisbar ist (M60.07). Soweit das Löschen selbst wieder protokolliert wird, dürfen in diesen Protokollen keine Daten enthalten sein, für die eine Löschverpflichtung besteht (M60.08).

Um gesetzlich vorgegebene Löschfristen automatisiert überwachen zu können, sind technische Systeme geeignet, die entsprechende Zeitstempelsysteme beinhalten oder nutzen können (M60.09). 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 (M60.10).

Sofern Löschungen nach bestimmten systematischen Vorgaben erfolgen, sollten die technischen Systeme den Vorgang des Löschens automatisiert durchführen können (M60.11).

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 wesentlich aufwändiger als das Löschen im aktiven Datenbestand ist, kann diese Löschung im Zuge des Überschreibens oder der Vernichtung der Sicherungsdatenträger als Ganzem erfolgen, wobei der Zeitpunkt und die Frequenz dieses Vorgangs maßgeblich vom Schutzbedarf der betreffenden Daten abhängig gemacht werden muss (siehe dazu Abschnitt hoher Schutzbedarf). 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 (M60.12). Regelhaft sollten die Löschung der Daten in den Backup-Dateien spätestens ein Jahr nach der Löschung im Produktivdatenbestand erfolgen. Dem Prinzip der Datenminimierung folgend sollten jedoch immer kürzere Fristen angestrebt werden.

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

Prozesse

Eine wesentliche Voraussetzung für die ordnungsgemäße Funktion von Löschprozessen ist die Festlegung von Löschfristen (M60.13). Diese sind schriftlich festzulegen und nach den Vorgaben der DS-GVO in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmen (M60.14). 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 (M60.15). Hilfreich hierfür ist die 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 ist ein Rollen- und Rechtekonzept erforderlich, 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 (siehe Baustein „Rollen und Berechtigungen“). 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 durch Vernichten von Datenträgern erfordert Prozesse, die abhängig von der Art der zu vernichtenden Datenträger und vom Schutzbedarf der zu löschenden Daten sind. Die gesamte Anwendung des SDM ist als organisatorischer Prozess zu verstehen, der im Fall des Löschens die Auswahl geeigneter Vernichtungsmechanismen steuert. Weitere Hinweise zur Prozessgestaltung bei der Vernichtung enthält das Dokument DIN SPEC 66399-3.

Für das Löschen von Protokolldaten sind gesonderte Prozesse einzurichten (M60.16).

Um die Löschpflichten für die Datenbestände bei Auftragsverarbeitern umsetzen zu können, sind vertragliche Regelungen und verbindliche Weisungen erforderlich (M60.17). 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), ist zu prüfen, ob diese Prozesse automatisiert ablaufen können. In diesem Zusammenhang sind weitere Prozesse erforderlich, die jederzeit ein gezieltes Aussetzen und Unterbrechen automatisierter Löschprozesse ermöglichen (M60.18).

Bei der Auswahl der konkreten Löschmaßnahme ist zudem zu berücksichtigen, aus welchem Grund die Löschung erfolgt (M60.19). So können beispielsweise 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, sind entsprechende Überwachungsprozesse erforderlich (M60.20).

Das Löschen verschlüsselter Daten erfordert spezielle Regeln und Prozesse zum Umgang mit diesen Daten und den dazugehörigen Verschlüsselungsschlüsseln (M60.21, M60.22); siehe dazu auch Baustein Kryptographie.

Um das in der DS-GVO normierte Recht auf Vergessenwerden umzusetzen, muss durch entsprechende Prozesse auch nachvollziehbar sein, wann welche personenbezogenen Daten veröffentlicht wurden (M60.23, M60.24). Darüber hinaus müssen Strategien vorhanden sein, die beschreiben, wie mögliche Datenempfänger über die an den Verantwortlichen gerichteten Anträge zur Löschung dieser Daten informiert werden (M60.25).

Durch geeignete Prozesse muss weiterhin sichergestellt werden, dass eine Löschung alle Kopien erfasst, also beispielsweise auch auf mobilen Geräten vorgehaltene Offline-Kopien oder Kopien in Cloud-Strukturen (M60.26).

3. Differenzierung bei hohem Schutzbedarf

Die technischen und organisatorischen Maßnahmen zum Löschen müssen der Risikostufe und somit dem Schutzbedarf der Daten angemessen sein. 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 mit sehr hohem Schutzbedarf sind in der Regel Maßnahmen ab der Sicherheitsstufe 5 relevant.

Auch für elektronisch gespeicherte Daten hängt die Auswahl von Löschmaßnahmen vom Schutzbedarf der betreffenden Daten ab. 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 Löschprozessen. Die Dokumentation von Löschprozessen darf jedoch keine Inhaltsdaten enthalten, die zu löschen sind (siehe M60.08). Dies würde den Löschprozess konterkarieren.

Sollen Daten mit hohem Schutzbedarf gelöscht werden, sind auch besondere Anforderungen an die Löschung von deren Sicherungskopien zu stellen. Während die Löschung normal schutzbedürftiger Daten in der Regel erst beim (in der Regel anlassbezogenen) Einspielen des Sicherungsdatenbestandes umgesetzt werden braucht (siehe M60.12), kann das Löschen hoch schutzbedürftiger Daten 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 sind auch die ursprünglichen Backup-Medien irreversibel zu löschen.

Zahlreiche Beispiele für besonders schutzbedürftige Daten sind im medizinischen Bereich zu finden. Bei Gesundheitsdaten handelt es sich in der Regel um Daten aus dem Katalog der besonderen Kategorien personenbezogener Daten gem. 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: *M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung*
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04032.html

M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02167.html

M 4.234 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04234.html

M 2.434 Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02434.html

M 2.436 Vernichtung von Datenträgern durch externe Dienstleister
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02436.html

Daten auf Festplatten richtig löschen
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html
(Stand 03/2017)

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

5. Zusammenfassung der Maßnahmen

Ebene Daten

M60.01 Datenstrukturen und Speicherarten, die das Löschen der Inhalte einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten in einer vom Schutzbedarf abhängigen Granularität ermöglichen

M60.02 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

Ebene Systeme

M60.03 Überschreiben von Daten, Datenfeldern, Datenattributen oder kompletten Datenträgern mit speziellen Löschprogrammen (Wipe-Tools)

M60.04 Schreddern zur Vernichtung von Datenträgern jeder Art

M60.05 Einschmelzen oder Verbrennen von Datenträgern jeder Art

M60.06 Integritätssicherung beim Löschen

M60.07 Protokollierung von Löschungen
M60.08 Datensparsame Ausgestaltung der Protokollierung von Löschungen
M60.09 Automatisierte Überwachung von Löschfristen unter Nutzung von Zeitstempelsystemen oder Auswertungen entsprechender Löschattribute
M60.10 Möglichkeiten der Zuordnung zwischen Daten und dem zeitlichen Anknüpfungspunkt für die Löschverpflichtung
M60.11 Technische Systeme zur automatisierten, zeitgesteuerten Löschung unter Nutzung von Zeitstempelsystemen oder durch Auswertungen anderer Zuordnungssysteme oder entsprechende Löschattribute
M60.12 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

Ebene Prozesse

M60.13 Festlegung von Löschfristen
M60.14 Dokumentation von Löschfristen (ggf. im Verzeichnis von Verarbeitungstätigkeiten)
M60.15 Löschkonzept
M60.16 Regelungen mit besonderen Löschvorgaben für Protokolldaten unter Berücksichtigung der speziellen Aufbewahrungs- und Zweckbindungsvorgaben
M60.17 Regelungen zum Löschen von Daten, die im Rahmen der Datenverarbeitung im Auftrag bei Auftragnehmern gespeichert sind
M60.18 Prozess zur zeitgesteuerten, automatisierten Löschung von Daten
M60.19 Einbeziehung des Löschgrundes in die Auswahl eines Löschprozesses
M60.20 Prozess zur Überwachung der Rücksicherung hinsichtlich möglicher Löschpflichten
M60.21 Regelungen zum Umgang mit Verschlüsselungsschlüsseln von zu löschenden (verschlüsselten) Daten
M60.22 Regeln zum Löschen von Verschlüsselungsschlüsseln
M60.23 Regelungen zur Dokumentation von Veröffentlichung von Daten
M60.24 Prozess zur Protokollierung der Übermittlung personenbezogener Daten
M60.25 Prozess zur Information möglicher Datenempfänger über die Pflicht zur Löschung dieser Daten
M60.26 Dokumentation der Anzahl und des Speicherortes von Kopien

6. Anmerkung zur Nutzung dieses Bausteins

„Datenschutzaufsichtsaufsichtsbehörden der Bundesländer Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein sowie der Evangelischen Kirche Deutschlands. Datenlizenz Deutschland – Namensnennung – Version 2.0 (www.govdata.de/dl-de/by-2-0).“