Daniela Schlegel

Das Recht auf Löschen

Daten vernichten oder unwiederbringlich machen und das global?

Für alle Pflichten und Rechte in Bezug auf die Verarbeitung personenbezogener Daten gilt die rechtmäßige Verarbeitung als gemeinsame Grundlage und am Ende steht immer das Recht auf Löschen. Löschen? Was verbinden Sie als Leser*in mit dem Wort Löschen, wenn es um die Datenerstellung geht, also bspw. um Schreiben oder Zeichnen? Der Beitrag setzt sich mit den Fragen einer datenschutzkonformen Löschung auseinander und zeigt auf, was dies eigentlich in der Praxis bedeutet. Es soll aufgezeigt werden, dass Löschen im Zusammenhang mit Daten gegenwärtig eine eher irreführende Wortwahl und das Thema Löschen deshalb für Viele so unbehaglich ist.

1 Wortvorschläge und ihre (Aus-)Wirkungen

Die Autorin verbindet mit „Löschen" ihre eigene Schulzeit. Beim Schreiben mit einem Tintenfüller wurden die ursprünglichen Daten mit einem Tintenkiller tatsächlich gelöscht, quasi unsichtbar gemacht. Dies war allerdings nur ab den höheren Klassenstufen erlaubt.

In den unteren Klassenstufen war und ist es auch heute noch so, dass die Kinder die ursprünglichen Daten durchstreichen und die Korrektur dahinter schreiben. Das Durchgestrichene ist also weiterhin lesbar und bleibt Teil der Schreibschrift. Will man das Durchgestrichene unkenntlich bzw. unleserlich machen (vs. sicheres Löschen), geschieht das durch ein wiederholendes Durchstreichen (mehrfaches *Überschreiben*), bis der Text nicht mehr lesbar ist.

Doch was ist eigentlich das konkrete Ziel?

Daten sollen nachhaltig vernichtet werden. Daten sollen so unkenntlich gemacht werden, dass sie auch mit den gegenwärtigen, technischen Möglichkeiten für Experten nicht wieder auslesbar sind.

1.1 Angewandte Methode statt Löschen?

Wie in den unteren Schulklassen bleiben die nicht mehr gewollten Daten beim „Klicken" auf den Button „Löschen" erhalten und können auch von Fachkundigen wiederhergestellt und gelesen werden. In der digitalen Ökonomie werden die Daten, die nicht mehr benötigt werden, lediglich vom System zur Nutzung (wieder) freigegeben.

Die Freigabe erfolgt über die suggerierten Funktionen Löschen und Formatieren. Dabei wird einzig ein neuer Index auf dem Datenträger angelegt, also eine Art neues Inhaltsverzeichnis. Mit dem neuen Inhaltsverzeichnis fehlen die ursprünglichen Verweise auf die Bereiche, in denen die noch bestehenden Daten liegen und das System wird diese Bereiche neu beschreiben und damit die ursprünglichen Daten nach und nach *überschreiben*. Das *Überschreiben*[1] findet also nicht sofort, nicht für den gesamten Bereich und möglicherweise auch nie statt.

Als ein Bild skizziert, kann sich dies beispielsweise wie ein Manuskript (ca. 2.000 Seiten) für einen Film vorgestellt werden. Dabei ist es völlig irrelevant, ob es sich in Papierform oder als Worddatei vorgestellt wird. Der Drehbuchautor möchte eine seiner Rollen ändern (Text) und damit auch die Handlung (Inhaltsverzeichnis/Kapitel) umschreiben. Er *ändert* dafür zuerst die Seiten mit dem Inhaltsverzeichnis (vs. Löschen & Formatieren). Da nun der Verweis auf die ursprünglichen Kapitel fehlt, sucht er jetzt mühsam nach den Stellen im Manuskript, in denen die Rolle spielte (analog zur Datenwiederherstellung und Forensik). Im gesamten Text *streicht* er die gefundenen Textpassagen (*Datenfreigabe*) der ursprünglichen Rolle durch und schreibt nach dem neu-

Daniela Schlegel

Netzwerkspezialistin, zertifizierte Informationssicherheitsbeauftragte (ISO) und Datenschützerin (DSB); Inhaberin von konzoom.de und dsdsb.expert; betreut vor allem Kunden und Projekte rund um die Themen IT-Netzwerksicherheit, ISMS und Datenschutz mit dem Fokus auf sicherheitsrelevante Infrastrukturen (KRITIS) und deren Nutzen für die Gesellschaft.
E-Mail: mitteilung@dsdsb.expert

1 Hier ist das einfach Überschreiben gemeint.

en Inhaltsverzeichnis neue Kapitel und Anweisungen für das gesamte Drehbuch.

Es liegt also ein Manuskript vor, das ein neues Inhaltsverzeichnis, neue Kapitel (Verweise) und neuen wie auch durchgestrichenen Text aufweist. Die angewendeten Methoden[2] dafür sind (Ver) Änderung/Anpassung, Datenfreigabe/Freigabe und Erstellen/Anfertigen/Erzeugen/Generieren.

Grundsätzlich verbinden wir mit dem Begriff Löschen, etwas Vorhandenes zu entfernen bzw. zu beseitigen. Der Begriff Löschen kommt ursprünglich aus der Schifffahrt und wurde im Zusammenhang mit der Entladung von Schiffen verwendet.[3] Wenn auch in einem ganz anderen Zusammenhang, so steht auch hier der Begriff Löschen im engeren Wortsinn für etwas Vorhandenes (vom Ort) entfernen.[4] In diesem Fall, in diesem Kontext bedeutet dies, aus einem gefüllten Raum einen leeren Raum machen.

Doch zurück zu Bits & Bytes. Nach der hier vertretenen Auffassung ist das Prinzip des Löschens oder Entfernens für die digitale Ökonomie jedoch gegenwärtig nicht mitgedacht. Der Mensch neigt ohnehin eher zur Bewahrung und Weitergabe von Wissen und Informationen, was personenbezogene Daten unweigerlich einbezieht und letztlich auch der Grundgedanke und Treiber für die Entstehung und den Siegeszug des Internets ist, wie wir es heute kennen. Am Anfang stand Sammeln und Teilen. Gegenwärtig kommt „Löschen" und Vergessenwerden hinzu.

2.2 Was sagt das BSI dazu?

Das BSI bestätigt uns Verbraucher*innen, dass „Normales Löschen nichts bringt".[5] Es spricht dabei aber vom „endgültigen Löschen" auf Festplatten und Smartphones in der Überschrift. Die vielen Facetten des Löschens auf der Webseite des BSI sind dabei dem ersten Eindruck nach wenig zweckdienlich, mangelt es doch an der notwendigen Aufklärung zum Vorgehen.

2.2.1 Normales Löschen

Das BSI beschreibt den Vorgang des normalen Löschens anhand von Windows und dem Papierkorb und klärt auf: „Normales" Löschen bringt nichts.[6] Dabei den Gedanken zugrunde legend, dass aus dem Papierkorb die Daten jederzeit wiederhergestellt und damit einer neuen bzw. der alten Nutzung zugeführt werden können.

2.2.2 Richtiges Löschen

Das BSI stellt dem Kapitel zum richtigen Löschen voran, dass dies nur für die Daten möglich ist, auf die das Programm zum *Überschreiben* Zugriff hat und schließt weitere Daten aus, die in defekten Speicherbereichen von Anwendungsprogrammen abgelegt sind. Weiterhin beschreibt das BSI in diesem Kapitel: „Dabei werden die Daten einmal oder mehrfach mit vorgegebenen Zeichen oder Zufallszahlen überschrieben, was in den meisten Fällen ausreichend ist."[7] Basierend auf der Aussage des BSI stellt sich demzufolge die berechtigte Frage: Ist einmal Überschreiben richtiges Löschen?

2.2.3 Endgültiges Löschen

Eine Definition oder Erläuterung zum endgültigen Löschen bleibt das BSI dem Verbraucher gegenüber auf seiner Webseite leider schuldig. Stattdessen erfolgt eine Darstellung mit der Überschrift: „Wenige Schritte zum sicheren Löschen von Daten".[8] Es folgen Ausführungen zu „Daten verschlüsseln", „Daten überschreiben" und das Thema Werkseinstellung", wohlgemerkt für Verbraucher.

Für eine sogenannte Shredder-App folgt hingegen keine Empfehlung, dafür aber wieder direkt die Ungewissheit, inwieweit diese Apps tatsächlich auf den verschiedenen Plattformen ausreichend evaluiert wurden.

2.2.4 Zwischenbilanz

Auch das BSI bietet gegenwärtig keine eindeutige Definition der Begrifflichkeiten für Verbraucher in Bezug auf das Löschen von Daten auf ihren Endgeräten. Leider steht das in einem Widerspruch zu allen einschlägigen Vorgaben für die Wirtschaft in Bezug auf Awareness- und Sensibilisierungsmaßnahmen.

Das verwundert deshalb, weil der BSI-Grundschutz, CON.6 Löschen und Vernichten,[9] hierzu sehr deutlich wird. Allerdings richtet sich der BSI-Grundschutz an die Wirtschaft, nicht an die Endverbraucher.

3 Sichere Methode: Mehrmaliges Überschreiben mit unterschiedlichen Bitmustern

Fast schon generalisierend gilt für die „sichere Datenlöschung" das Motto: Je häufiger, desto besser. Allerdings sind die Speichertechnologien und die genutzten Bitmuster entscheidend, nicht nur die Anzahl der Schreibvorgänge. Je höher die Aufzeichnungsdichte ist, umso geringer ist die Anzahl der Wiederholungen des *Überschreibens*.

Es gibt sehr unterschiedliche Methode des *mehrmaligen Überschreibens mit unterschiedlichen Bitmustern („Lösch"-Algorithmen*). Bei einer Recherche im Internet ist es leider nicht gelungen, aktuelle Zusammenfassungen zu diesem Thema zu finden oder die Quellen der Artikel zu verifizieren. Um dennoch aufzuzeigen, dass es sehr wohl „Standards" zu diesem Thema gibt, sol-

2 Art und Weise eines Vorgehens (Duden Stand 23.6.2023 https://www.duden.de/rechtschreibung/Methode).

3 https://archive.org/details/etymologischesw05kluggoog/page/208/mode/2up?view=theater (Stand 5.7.2023).

4 https://www.gesetze-im-internet.de/hgb/ (Stand 22.6.2023).

5 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html (Stand 23.6.2023).

6 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html (Stand 26.6.2023).

7 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html (Stand 26.6.2023).

8 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html (Stand 26.6.2023).

9 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2021.pdf?__blob=publicationFile&v=2 (Stand 27.6.2023).

len hier stellvertretend die Algorithmen und Empfehlungen der Hersteller Acronis[10] und Kaspersky[11]aufgeführt werden:

- *American: U.S. Standard, DoD 5220.22-M[12];*
- *American: NAVSO P-5239-26[13];*
- *German: VSITR[14];*
- *Russian: GOST P50739-95[15]*
- *Peter Gutmann algorithm – data on hard disk is destroyed with 35 passes;[16]*
- *Bruce Schneier algorithm – data is destroyed with 7 passes."*

Die Tatsache, dass es zu diesem Thema kaum öffentliches Material zu geben scheint, ist bezeichnend und ein Indiz dafür, warum das Thema „Löschen" so schwer zu bearbeiten ist.

Nichtsdestotrotz ist das mehrfache Überschreiben mit unterschiedlichen Bitmustern gegenwärtig das Maß der Dinge.

4 Plan B: Unwiederbringlichkeit

Zusätzlich zur sicheren Methode des mehrfachen Überschreibens (mit unterschiedlichen Bitmustern) gibt es physische Lösungsmethoden:

1. Entmagnetisierung digitaler Datenträger
2. Physische Zerstörung des Datenträgers

Bei diesen beiden Methoden der *Datenträgervernichtung* entsteht unweigerlich ein fester Bezug zu einem Datenträger mit dem uns bekannten Ablageort. Für einen Endnutzer bezieht sich das auf seinen persönlichen und die gemeinsamen Ordner auf dem Endgerät, auf dem gemeinsamen Laufwerk oder dem USB-Stick.

Das spürbare Unbehagen für die Erhebung der digitalen Datenpools, Verarbeitungswege und Löschkonzepte für den digitalen Wirtschaftsraum zeigt, speziell mit Blick auf XaaS-Modelle und Cloud, ist absolut begründet.

Zudem ist die physische Zerstörung von digitalen Datenträgern kaum nachhaltig (und wirtschaftlich). Man stelle sich vor, Amazon, Microsoft oder Google zerstören mit jedem Recht auf Löschung und Vergessenwerden vor Ort physische Platten. Dessen ungeachtet, dass damit die Daten auf anderen Datenträgern nicht gelöscht würden.

Dabei sind „bekannte Ablageorte" die visuell, eigenen und gemeinsam genutzten, analogen und digitalen Ablage- und Ordnerstrukturen. „Unbekannte Ablageorte" sind demgegenüber die analogen und digitalen Ablage- und Ordnerstrukturen außerhalb unserer Wahrnehmung,[17] systembedingt (bspw. Betriebssysteme, Anwendungen, Funktionen), Internetinfrastrukturen (bspw. Zwischenspeicher, Backup- und Wiederherstellungssysteme, XaaS-Modelle oder Hosting-, Service-, Application-, Cloud-Provider), Softwarecode und IT-Diagnose-Daten, Übermittlung an Dritte/Drittländer).

Der Klick auf den Button „Löschen" bewirkt daher zunächst einmal nur, dass auf dem Einzelsystem[18] der Sektor und der Speicherplatz für genau diesen einen Datensatz (bspw. die eine Datei Manuskript mit 100MB) im System zur Wiederbeschreibung freigegeben wird.

Unberührt von diesem Vorgang bzw. von dieser Datenplatzfreigabe sind alle weiteren Kopien,[19] Einzelsysteme und das Internet. Systembedingt legt die digitale Ökonomie eine Vielzahl von Kopien an. Ganz vorne dran der Cache[20] und Schattenkopien für einen ausfallfreien Datenzugriff und -transport. Beide sind notwendig für ein wesentliches Schutzziel der Informationssicherheit: die Verfügbarkeit.

5 Keine Frage von analog oder digital!

Auch analoge Datenträger wie Papier wurden und werden durch die Vervielfältigung und Weitergabe an Orten abgelegt und aufbewahrt, die dem einzelnen Endnutzer oder Fachbereich unbekannt sind. Es ist wichtig zu verstehen, dass dies kein Phänomen oder nur eine Aufgabe der digitalen Ökonomie ist. Und nein, die Herausforderung zur umfangreichen Vernichtung (physisch, analog) oder „Löschung" (digital) besteht nicht erst durch die EU DSGVO.

Was können wir also tun, um den beiden Rechten „Löschen" und „Vergessenwerden" genauso offen und ohne Emotion zu begegnen, wie all den anderen Rechten? Folgender Lösungsansatz wäre denkbar.

5.1 Das Verarbeitungsverzeichnis

Ausgehend von dem Verarbeitungsverzeichnis nach EU DSGVO, besteht bereits ein Überblick zur Datenverarbeitung und Datenablage für die (einzelnen) Bereiche. Meist wird dieser im jeweiligen Sachgebiet erstellt und spiegelt zunächst (nur) den bereichsinternen Kenntnisstand wieder.

Die Kunst besteht dann darin, die Verarbeitungsverzeichnisse an den einzelnen Schnittstellen miteinander zu verknüpfen. Der Gesamtüberblick entsteht aber nur, wenn ein Geschäftsprozess Ende-zu-Ende und unter den Gesichtspunkten des Daten-Lebenszyklus betrachtet wird.

5.2 Betrachtung primärer Geschäftsprozesse

Was die EU DSGVO für den Datenschutz ist, ist die ISO/IEC 27000-Serie für die Informationssicherheit und für den Aufbau eines ISMS.[21] Das ISMS ist prozessorientiert und ausgehend von der Unternehmensführung (Top-Down). Alle primären Geschäftsprozesse[22] werden bis auf das einzelne Asset hinunter betrachtet und der Schutzbedarf des primären Geschäftsprozesses

10 https://kb.acronis.com/de/node/8752 (last update: 24-08-2010) (Stand 6.7.2023).

11 https://support.kaspersky.com/KTS/2021/de-DE/84522.htm (Stand 24.7.2023).

12 https://www.dami.army.pentagon.mil/site/IndustSec/docs/DoD%20522022-m.pdf (Stand 24.7.23).

13 https://irp.fas.org/doddir/navy/5239_26.htm (Stand 24.7.23)

14 https://delit.ag/blog/datenloesch-algorithmus-bsi-vsitr (update 22. Januar 2021) (Stand 6.7.2023).

15 https://support.kaspersky.com/KTS/2021/de-DE/84522.htm (Stand 24.7.23)

16 https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (Stand 24.7.2023).

17 Dazu zählen auch die eigenen Endgeräte (unbekannter Datenabfluss oder durch Synchronisation).

18 PC, mobile Endgeräte, Speichermedien (bspw. USB).

19 Vervielfältigung des ersten digitalen Datensatzes.

20 Cache (Kurzform) bezeichnet ein chipbasiertes Element in den Endgeräten, dass das Abrufen von Daten aus dem internen Speicher des Einzelsystems effizienter macht. Ein Browser-Cache ist ein Zwischenspeicher zum effizienteren Laden von Daten aus dem Internet.

21 Information Security Management System.

22 Primäre Geschäftsprozesse sind direkt für die Wertschöpfung des Unternehmens verantwortlich.

wird auf die gesamte Verarbeitungskette und damit bis auf die Ebene der einzelnen Assets vererbt.

Wir wissen, Daten sind ein Asset.

Datensicherung, Wiederherstellung (System und Daten) und Notfallpläne sind sekundäre Geschäftsprozesse[23] und (eben) keine „Hauptprozesse der IT-Abteilung". Allein diese drei sekundären Geschäftsprozesse bilden die technische Grundlage für eine Vielzahl von primären Geschäftsprozessen (bspw. für das Betriebskontinuitätsmanagement (BKM; englisch business continuity management (BCM) und Krisen- und Notfall-Management)![24]

Auch der BSI-Grundschutz (CON.6.A1) regelt, dass die

> *„Fachverantwortlichen für jedes Fachverfahren bzw. Geschäftsprozess regeln, welche Informationen unter welchen Voraussetzungen gelöscht und entsorgt werden müssen."*[25]

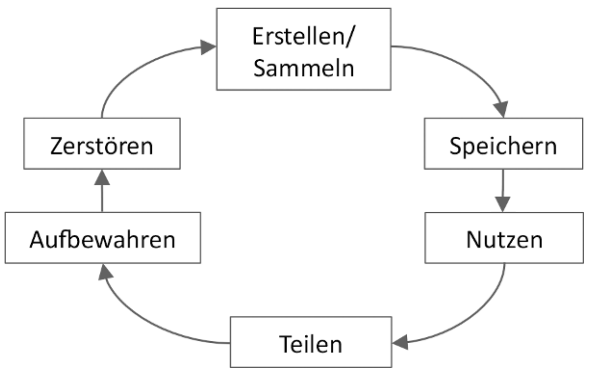
5.3 Berücksichtigung des Lebenszyklus von Daten

Im Asset-Management (u. a. ISO27k, BSI-GS) gelten Daten (auch) als Asset[26] und damit gilt für Daten, wie für alle anderen Asset-Klassen auch, ein Lebenszyklus. Während dieses Lebenszyklus haben die Daten immer wieder einen anderen Status. Man unterscheidet hier in data at work, data in transfer und data at rest (Daten im Zugriff, Daten während des Transports, Daten gespeichert oder archiviert).

Für das Management eines Data-Lebenszyklus[27] müssen neben dem Status auch die zum Status zugehörigen Verarbeitungs- und Ablageorte berücksichtigt werden. Allein mit diesem Gedankenansatz weitet sich der Blick auf die Verarbeitungswege von Daten.

Der Lebenszyklus von jedem einzelnen Datum kann wie folgt dargestellt werden:

Abbildung 1 | Lebenszyklus von Daten



5.4 Denkbare Lösung

Von den primären Geschäftsprozessen ausgehend, müssen alle Assets, über die dieser Geschäftsprozess verarbeitet und gesichert wird, ermittelt werden. Hier entsteht bereits ein erster Lichtblick auf der Suche nach den Daten. Kennt man die Assets (Anwendungen, IT-Systeme, Beteiligte und damit auch Schnittstellen und mögliche Drittländer), dann erhält man für jeden Prozess den Überblick darüber, wo überall die Daten erstellt, verarbeitet, geteilt, gespeichert und vernichtet werden (vgl. Daten-Lebenszyklus). Der Ansatz des Top-Down, von der Unternehmensführung aus, über den primären Geschäftsprozess hin zu den einzelnen Assets, hilft dem Datenschutz, die zu schützenden Daten während des gesamten Daten-Lebenszyklus feststellbar zu machen. Es ist die sogenannte Vogelperspektive im Vergleich zu den Verarbeitungsverzeichnissen, die sich unternehmensintern gedanklich nur sehr schwer dem individuellen Arbeitsgebiet der einzelnen Abteilung entziehen kann.

In Unternehmen, in denen bereits ein ISMS etabliert ist, profitiert folglich der Datenschutz.

5.5 Sprachliche Konsequenz

Statt vom Löschen sollte von der Methodik gesprochen werden, die zur Anwendung kommt. Wenn Papier oder physische Geräte[28] vernichtet/zerstört, also Papier geschreddert wird, wenn physische Geräte zerstört oder entmagnetisiert, wenn auf physische Geräte Daten einmal oder mehrfach überschrieben werden, dann sollte dies auch so beschrieben und dokumentiert werden, um den Unterschied deutlich werden zu lassen.

Für jedes Beispiel und dessen Unterschiede in den Methodiken, entstehen so auch unterschiedliche Handlungsanweisungen und Prüfhandlungen.

Für das Ziel der *Unwiederbringlichkeit* kennen wir also die Methoden *mehrmals Überschreiben mit oder ohne unterschiedliche Bitmuster, die Vernichtung von Daten durch die Zerstörung ihrer digitalen Datenträger durch Entmagnetisierung oder physische Kräfte.*

Immer öfter wird darüber hinaus auch das Mittel der Verschlüsselung als eine Art „Ausweg" für den Datenschutz angeboten. In diesem Zusammenhang muss aber ausdrücklich darauf hingewiesen werden, dass die klassischen kryptographischen Methoden den Schutzzielen der Informationssicherheit dienen: Vertraulichkeit, Unverfälschtheit (bzw. Integrität) und Echtheit (bzw. Authentizität).[29] Die Verschlüsselung begünstigt selbstverständlich den Datenschutz gegenüber dem öffentlichen Raum (bspw. die Übertragung übers Internet), sie hat ihn aber nicht zum Ziel.

6 Teamwork für den Datenschutz

Uns stehen eine Vielzahl an Modellen und Standards zur Verfügung, in denen das Ziel dasselbe ist, nur eben mit unterschiedlichen und die für sie jeweils fachspezifischen Umsetzungsvarianten.

23 Sekundäre Geschäftsprozesse sind nicht für die Wertschöpfung des Unternehmens verantwortlich, sind aber trotzdem notwendig und unterstützen den/die primären Geschäftsprozess(e), da sie den primären Geschäftsprozess erst möglich machen.

24 https://de.wikipedia.org/wiki/Betriebliches_Kontinuit%C3%A4tsmanagement (Stand 19.7.2023).

25 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2021.pdf?__blob=publicationFile&v=2 (Stand 27.6.2023).

26 Asset bezeichnet Vermögenswerte (Wirtschaftsgüter) eines Unternehmens.

27 https://cissprep.net/asset-lifecycle/Stand (Stand 22.6.2023).

28 Bspw. Festplatten, Rechner, Smartphones.

29 Engl. CIA: Confidentiality, Integrity, Authenticity.

Wichtig ist es daher, sich innerhalb des Teams der eigenen Befugnisse zu vergewissern und diese auch gegenüber Anderen klar zu kommunizieren.

Im Datenschutz liegt der Fokus auf personenbezogenen Daten und ihrer rechtmäßigen Verarbeitung in jedem Status. In der Informationssicherheit liegt der Fokus auf Richtlinien (IS-Framework) und Methoden (TOM) zum Schutz von sensiblen Daten im Allgemeinen und nach einem risikobasierten Ansatz. In der Netzwerksicherheit liegt der Fokus auf den technischen Standards, z. B. eine konkrete und als gegenwärtig sicher geltende Verschlüsselungsmethode. Die Aufgaben des Datenschutzes und der Netzwerksicherheit sind jeweils Teildisziplinen der (allgemeinen) Informationssicherheit. Das bedeutet, sie sind mitgedacht und in der Befugnis zur Umsetzung an die Fachbereiche adressiert.

Das ideale Team in diesem Zusammenhang besteht folglich aus den Verantwortlichen der Abteilungen Geschäftsführung, Compliance, Unternehmens- oder Konzernsicherheit, Datenschutz, Risko- und Abweichungsmanagement und den Verantwortlichen des jeweiligen, operativen Fachbereichs. Es sollte einen internen Prozess für das Abweichungs- und Risikomanagement geben (Datenschutz-Folgeabschätzung → Risikomanagement), in denen alle Bereiche vertreten sind. Teamwork eben!

Im Übrigen gelten die genannten Funktionsbereiche auch für KMUs. Es gibt vielleicht keine separate Abteilung und nur einen Mitarbeitenden plus Vertretung, dennoch sind die Pflichten zur Regeltreue/Regelkonformität (Compliance) einzuhalten und Zuständige zu definieren.

7 Zusammenfassung

- Das Wort Löschen sollte in der digitalen Ökonomie vermieden werden.
- Stattdessen sollten die angewandten Methoden für die Vernichtung und Unwiederbringlichkeit von Daten (digital und analog) verwendet werden.
- Der Daten-Lebenszyklus und hier speziell der Status des Endes eines Datums, also wenn die Daten nicht mehr aktuell sind oder nicht gespeichert werden dürfen, ist zu beachten.
- Von dem Ansatz des ISMS (Vogelperspektive) und dem Asset-Management aus, kann der Datenschutz profitieren, um einen weitreichenderen Überblick über die Datenverarbeitung und die Datenablage zu bekommen. An dieser Stelle sind unbedingt Offline-Backups, isolierte Sicherungen und die Synchronisation mit Internetdiensten zu berücksichtigen.

8 Fazit

Insgesamt gilt demzufolge, dass die Methoden *Überschreiben* und *Freigabe* von Daten und Speicher für das gesamte Netz/Internet gelten. Dieser Prozess dauert jedoch oder passiert vielleicht nie und beides entzieht sich unserer Kontrolle!