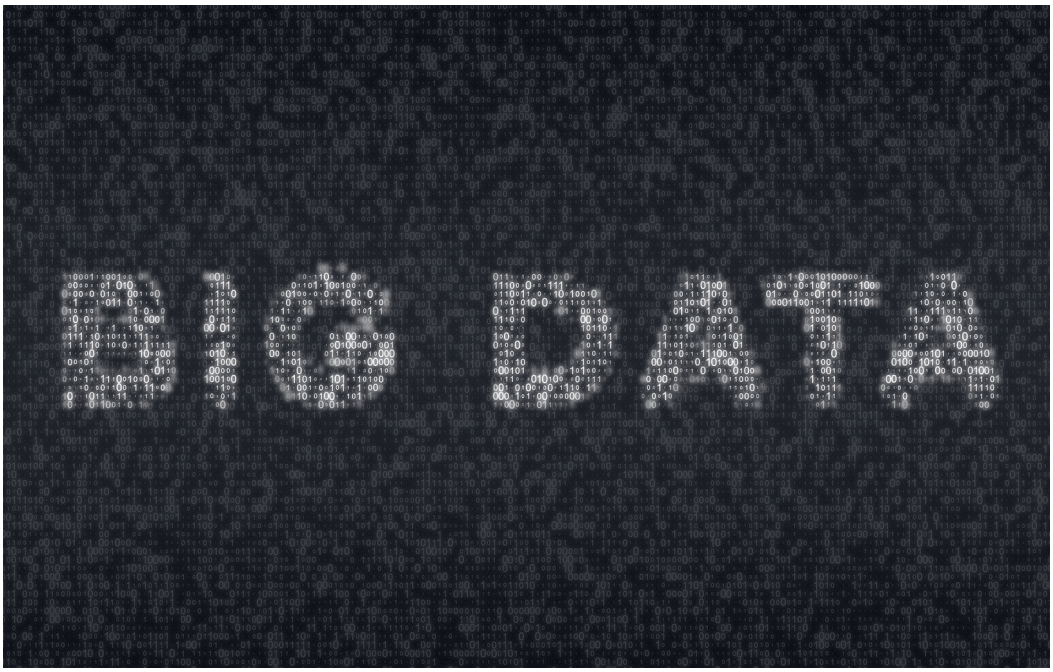

Bild: Pixabay

Die ISO/IEC 27555:2021 zeigt, dass Löschung kein Nebenschauplatz der Informationssicherheit ist.

ISO 27555:2021: Löschung personenbezogener Daten

Weitgehend unbekannt wurde bereits im Oktober 2021 eine ISO-Norm mit dem Titel «Leitlinien für die Löschung personenbezogener Daten» veröffentlicht. Die ISO/IEC 27555:2021 bietet Organisationen einen strukturierten Rahmen, um personenbezogene Informationen (PII) nicht nur sicher zu speichern, sondern sie zum richtigen Zeitpunkt auch zu löschen.

Die Speicherung personenbezogener Daten über ihre eigentliche Zweckbindung hinaus ist nicht nur datenschutzrechtlich problematisch. Sie öffnet auch die Tür für Missbrauch, Datenschutzverletzungen und forensische Rückgewinnung. Jede nicht gelöschte Information verlängert unnötig das Risiko. Und mit jedem Backup, jedem Archiv und jeder vergessenen Datei potenziert sich die Angriffsfläche.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

PII-Cluster

Die Norm selbst hat den gewohnten Aufbau. Kapitel 1 zeigt kurz den Umfang der Norm, das Kapitel 2 stellt Verweise zu anderen Normen her (hier nur zur ISO 29100, dem Privacy Framework), das Kapitel 3 definiert zehn neue Begriffe und im Kapitel 4 werden sieben abgekürzte Begriffe erläutert. Ein Begriff soll an dieser Stelle kurz beschrieben werden, und zwar «PII-Cluster». Dabei handelt es sich um personenbezogene Daten, die für einen einheitlichen funktionalen Zweck verarbeitet werden. Wichtig dabei ist, dass PII-Cluster (PII = Personally Identifiable Information, also personenbezogene Daten, die zur Identifizierung einer bestimmten Person verwendet werden können) unabhängig von der technischen Darstellung der Datenobjekte beschrieben werden. PII-Cluster umfassen dabei auch Informationen, die nicht elektronisch gespeichert sind.

Kapitel 5.2 (Titel Einschränkungen) der Norm stellt fest: Wer Daten länger als notwendig aufbewahrt, verletzt Prinzipien wie Datenminimierung und Zweckbindung. Sobald gesetzliche oder vertragliche Aufbewahrungspflichten erfüllt sind, muss gelöscht werden – vollständig, überprüfbar und ohne technische Hintertüren.

Ein Beispiel: Buchhaltungsdaten müssen in vielen Ländern zehn Jahre aufbewahrt werden. Danach muss die kontrollierte und nachweisbare Löschung erfolgen.

Zwischen Aufbewahrungsfrist und regelmässiger Löschungsfrist

Die Norm unterscheidet zwischen Aufbewahrungsfrist (5.4.1) und regelmässiger Löschungsfrist (5.4.2). Erstere regelt, wie lange Daten zweckmässig oder rechtlich benötigt werden. Letztere beginnt danach – und definiert den maximalen Zeitraum, innerhalb dessen die Löschung abgeschlossen sein muss. Die Löschung muss ein aktiver Teil des Datenlebenszyklus sein. Es reicht nicht, Daten unbefristet in Sicherungen oder Archiven zu «parken». Auch dort gelten dieselben Löschregeln wie im Primärsystem. Das Kapitel 5.5 schreibt dazu «Für in Archiven enthaltene PII sollten dieselben Löschungsregeln gelten wie für die jeweiligen PII-Cluster, und diese Regeln sollten in den betreffenden Archiven umgesetzt werden.»

Daten sollten nie einzeln verwaltet werden. Im Kapitel 6 wird deshalb auf das das Konzept der PII-Cluster eingegangen. So werden beispielsweise Rechnungen, Zahlungseingänge und Buchungssätze zum Cluster «Buchhaltungsdaten» zusammengefasst. Jeder Cluster erhält eine individuelle Löschregel mit definiertem Startpunkt und Frist. Damit wird die Löschung planbar und konsistent.

Dabei zeigen vier Beispiele, wie ein und dieselben Informationen (zum Beispiel Name und Adresse) in mehreren Clustern vorkommen können – mit jeweils eigenen Regeln.

Nicht jede PII braucht eine eigene Löschfrist. Kapitel 7.1 empfiehlt, mit einer begrenzten Anzahl von Standard-Löschfristen zu arbeiten. Idealerweise sind es zwischen fünf und zehn – eine Grössenordnung, die sich in der Praxis bewährt hat. Diese Standardfristen werden dann mit abstrakten Startpunkten (zum Beispiel «Vertragsende» oder «letzter Kontakt») kombiniert und zu Löschungsklassen zusammengefasst. Die beiden Unterkapitel 7.2 und 7.3 gehen vertiefter auf die regulären Löschungsfristen (zum

Beispiel Rechtsvorschriften) und Standard-Löschfristen (zum Beispiel drei Jahre nach Vertragsende).

Gerichtsverfahren oder Reklamationsfall

Natürlich gibt es Situationen, in denen Daten länger benötigt werden – etwa bei einem laufenden Gerichtsverfahren oder bei einem nachträglichen Reklamationsfall. Kapitel 7.4 erläutert solche besonderen Situationen und zeigt, wie Ausnahmen kontrolliert gehandhabt werden können.

Wichtig ist dabei: Jede Ausnahme muss dokumentiert, befristet und technisch abgesichert sein. Und sie darf nicht als Regelersatz missbraucht werden. Die Norm nennt als Beispiel eine verlängerte Aufbewahrung wegen fehlerhafter Verarbeitung – mit klar definiertem Zeitrahmen für Analyse und Korrektur.

Ein besonders kritischer Punkt: Sicherungskopien. Sie werden oft als juristischer oder technischer Puffer missverstanden – tatsächlich aber müssen auch sie gelöscht oder überschrieben werden, wenn die Fristen des enthaltenen PII-Clusters erreicht sind.

Kapitel 5.5 und 7.4.5 stellen klar: Backups sind Wiederherstellungsinstrumente, keine Datenfriedhöfe. Daher sollte der Löschzeitraum der Sicherungskopien auf den kürzesten Löschzeitraum und die Sensibilität der enthaltenen PII abgestimmt werden.

Löschregeln sollen nicht an spezifische Technologien gebunden sein. Ob ein Dokument auf Papier, als PDF auf einem USB-Stick oder in einer Datenbank gespeichert ist – die Löschpflicht bleibt dieselbe. Kapitel 5.8 fordert deshalb eine technologieunabhängige Dokumentation der Löschvorgaben. Diese Dokumentation muss auch die Unterscheidung zwischen Löschung in Live-Systemen, Archiven und Backups berücksichtigen.

Kapitel 6.3 ergänzt diesen Punkt: Jede Entscheidung über Cluster, Fristen und Startpunkte muss nachvollziehbar dokumentiert sein – idealerweise in einem Katalog der Löschregeln. Dieser dient als Nachweis für Prüfungen, Audits und interne Kontrollen.

Das Kapitel 8 unterstützt bei der Definition von Löschungsklassen. Der Ausgangspunkt bezieht sich auf eine Bedingung, die im Lebenszyklus von PII auftritt. Die spezifischen Bedingungen können durch Bezugnahme auf den Zeitpunkt, zu dem die PII erhoben wurden, oder auf eine spezifische Bedingung während des Lebenszyklus der PII bestimmt werden. Eine Matrix kann helfen, die verschiedenen Informationen grafisch festzuhalten. Viele Systeme erlauben keine vollständige oder differenzierte Löschung. ISO/IEC 27555 fordert deshalb in Kapitel 9, dass Löschbarkeit bereits bei der Auswahl, Entwicklung und Beschaffung von IT-Systemen berücksichtigt werden muss. Ein System, das Daten nur versteckt, ist nicht normkonform. Löschung muss technisch möglich und administrativ durchführbar sein – auch in manuellen Prozessen.

Fazit

Die ISO/IEC 27555:2021 zeigt, dass Löschung kein Nebenschauplatz der Informationssicherheit ist. Sie ist integraler Bestandteil eines verantwortungsvollen Umgangs mit personenbezogenen Daten. Wer löscht, verringert Risiken, minimiert Haftung und zeigt Respekt gegenüber den Rechten der betroffenen Personen.

Löschen heisst nicht vergessen – sondern wissen, wann etwas nicht mehr gebraucht wird.