dsb
datenschutzbeauftragte
des kantons zürich

Merkblatt

Vernichten elektronischer Daten

Das Gesetz über die Information und den Datenschutz (IDG, LS 170.4) verlangt die Löschung respektive die Vernichtung der Informationen, die nicht durch das zuständige Archiv archiviert werden.

Dieses Merkblatt richtet sich an öffentliche Organe. Es enthält Ausführungen zum Vernichten elektronisch bearbeiteter Daten, insbesondere über:

- Auslösende Faktoren für eine Datenvernichtung
- Vernichtungsmethoden
- Risikoreduzierende Massnahmen
- Zu berücksichtigende Speicherorte

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch

Inhalt

1 Einleitung 3
1.1 Begriff ... 3
1.2 Gesetzliche Grundlagen ... 3
1.3 Prozess und Dokumentation ... 3

2 Auslösende Faktoren für eine Datenvernichtung 3
2.1 Ablauf der Aufbewahrungsfrist ... 3
2.2 Feststellen widerrechtlicher Bearbeitung ... 3
2.3 Ersuchen der Betroffenen CON.6 Löschen ... 4

3 Vernichtungsmethoden 4
3.1 Physische Vernichtung ... 4
3.2 Magnetische Löschung ... 4
3.3 Technisches Überschreiben (Wipen) ... 4
3.4 Löschen nicht flüchtiger elektronischer Speichermedien (Solid State Disks) ... 4
3.5 Logische Löschung ... 4

4 Risikoreduzierende Massnahmen 5
4.1 Anonymisieren ... 5
4.2 Schlüssel vernichten ... 5
4.3 Zugriff sperren ... 5
4.4 Pseudonymisieren ... 5
4.5 Referenzen löschen ... 5

5 Berücksichtigung des Speicherorts und der Art der Daten 6
5.1 Daten in Fachanwendungen ... 6
5.2 Daten auf Serverlaufwerken ... 6
5.3 Sicherungskopien von Daten ... 6
5.4 Protokollierungsdaten ... 6
5.5 Daten in der Cloud ... 7
5.6 Daten auf mobilen Datenbearbeitungsgeräten ... 7
5.7 Daten auf mobilen Datenträgern ... 7
5.8 Daten auf Write-Once-Read-Many-Speichern (WORMS) ... 7
5.9 Daten auf ausgesonderten Geräten ... 7
5.10 Daten auf privaten Geräten ... 7

6 Weiterführende Informationen 8

1 Einleitung

1.1 Begriff

Mit dem Begriff der Vernichtung ist im Regelfall die physische Vernichtung oder die nachhaltige Löschung der Information gemeint. Während die physische Vernichtung die Zerstörung des Mediums beinhaltet (Datenträger, Papier), ist unter dem Begriff Löschung die Unkenntlichmachung gespeicherter Daten zu verstehen (der Datenträger bleibt dabei erhalten).

Kann nicht sofort gelöscht respektive vernichtet werden, sind bis zum Zeitpunkt des Vernichtens risikoreduzierende Massnahmen zu implementieren.

1.2 Gesetzliche Grundlagen

- § 5 Abs. 3 und § 11 Abs. 2 IDG, LS 170.4
- Fachspezifische Grundlagen wie § 18 b Patientinnen- und Patientengesetz, LS 813.13

1.3 Prozess und Dokumentation

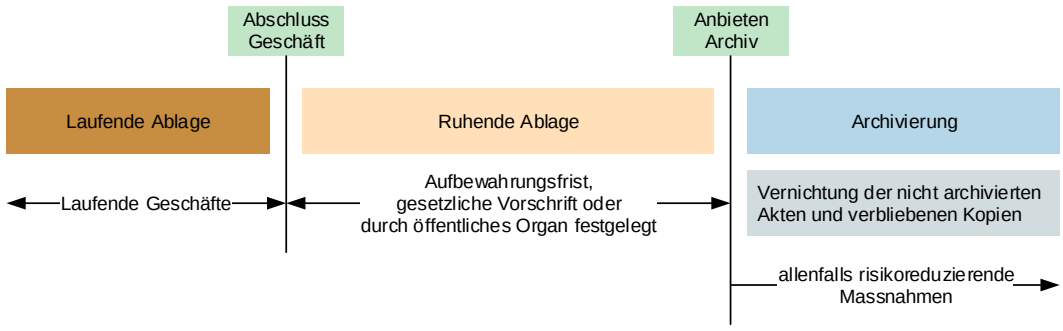
Der Prozess, die Verantwortlichkeiten und der Ablauf für die Vernichtung von Daten sind festzulegen, zu dokumentieren und regelmässig zu überprüfen.

2 Auslösende Faktoren für eine Datenvernichtung

2.1 Ablauf der Aufbewahrungsfrist

Öffentliche Organe dürfen Informationen solange aufbewahren, wie sie diese zur Erfüllung ihrer Aufgaben benötigen (laufende Ablage). Die maximal folgende Aufbewahrungsfrist (ruhende Ablage) wird von den öffentlichen Organen gemäss IDG selbst festgelegt, es sei denn, es existieren spezialgesetzliche Regelungen wie beispielsweise im Gesundheitsbereich.

§ 5 Abs. 3 IDG verpflichtet die öffentlichen Organe, Informationen nach Ablauf der Aufbewahrungsfrist dem zuständigen Archiv anzubieten. Informationen, die vom zuständigen Archiv nicht als archivwürdig befunden werden, sind zu vernichten. In der folgenden Grafik sind die einzelnen Schritte entsprechend dargestellt.



2.2 Feststellen widerrechtlicher Bearbeitung

Wurden Daten widerrechtlich erhoben, müssen diese unverzüglich vernichtet werden. Die Frist bis zur Vernichtung muss kurz sein, das heisst, sie darf nur wenige Tage betragen. In diesen Fällen ist in Bezug auf den Lösch- respektive Vernichtungsprozess ein höherer Aufwand zumutbar.

2.3 Ersuchen der Betroffenen

Von der Datenbearbeitung betroffene Personen können unter bestimmten gesetzlichen Voraussetzungen die Vernichtung ihrer Personendaten verlangen. Sind die rechtlichen Voraussetzungen erfüllt, beispielsweise weil die Widerrechtlichkeit festgestellt wurde, sind die betreffenden Daten zu vernichten.

3 Vernichtungsmethoden

3.1 Physische Vernichtung

Durch die physische Vernichtung des Datenträgers (zum Beispiel durch mechanisches Zerkleinern (Schreddern) oder Einschmelzen) werden die Daten vollumfänglich vernichtet. Bei der Weitergabe an Dritte ist durch entsprechende Massnahmen zu gewährleisten, dass die ausgetauschte Festplatte nicht weiterverwendet wird und Daten möglicherweise wieder rekonstruiert werden können. Dies gilt sowohl für die Entsorgung als auch bei einem Austausch oder bei einer Reparatur.

Weitere Informationen hierzu finden sich im BSI IT-Grundschutz-Kompendium CON.6 Löschen und Vernichten oder in der DIN-Norm 66399: Büro- und Datentechnik – Vernichten von Datenträgern

3.2 Magnetische Löschung

Spezielle Löschgeräte ermöglichen durch eine spezifische Magnetisierung das Löschen der Informationen ganzer Festplatten, so dass die Reproduktion von Daten unmöglich oder weitgehend erschwert wird. Solche Löschgeräte können selbst bei defekten Festplatten noch wirksam eingesetzt werden, funktionieren hingegen bei optischen oder nicht flüchtigen Speichermedien (beispielsweise Solid State Disks) nicht.

3.3 Technisches Überschreiben (Wipen)

Einzelne Dateien oder auch ganze wiederbeschreibbare Speichermedien können durch mehrmaliges Überschreiben mit zufälligen Zeichenfolgen (Wipen) nachhaltig gelöscht werden. Die Daten sind mehrmalig zu überschreiben, da beim einmaligen Überschreiben noch eine magnetische Restladung auf dem Datenträger gemessen werden kann, die für eine Rekonstruktion der ursprünglichen Daten ausreicht.

3.4 Löschen nicht flüchtiger elektronischer Speichermedien (NVM)

In moderne Systeme sind oft nicht flüchtige elektronische Speichermedien (NVM) verbaut. Diese heissen je nach Bauform anders – beispielsweise «Solid State Disk» (SSD) oder «NVM Express» (NVMe). Bedingt durch den Aufbau solcher Speichermedien können die gespeicherten Daten nicht durch mehrmaliges Überschreiben (Wipen) oder Magnetisierung gelöscht werden. Solche Speichermedien müssen über spezielle Löschbefehle (zum Beispiel mit dem ATA-Befehl «Enhanced Security Erase») sicher gelöscht werden. Unterstützt ein Speichermedium keinen solchen Löschbefehl, so sind die Daten vorgängig zu verschlüsseln und das Speichermedium bei der Aussonderung physisch zu vernichten (Schreddern).

3.5 Logische Löschung

Unter der logischen Löschung ist die Vernichtung des Zugriffsschlüssels (Index) auf die Daten zu verstehen. Das ist beispielsweise bei der Löschung mittels Delete-Taste oder Papierkorb der Fall. Dabei wird nur die Indexdatei der Datei entfernt. Durch Wiederherstellen der Indexdatei kann wieder auf die Datei zugegriffen werden.

4 Risikoreduzierende Massnahmen

Der Vernichtung ist immer Vorrang zu geben. Können Daten in Ausnahmefällen nicht sofort vernichtet werden, sind risikoreduzierende Massnahmen zu prüfen. Dabei sind folgende Faktoren zu berücksichtigen:

- Risiko einer Persönlichkeitsverletzung gemäss Schutzbedarfsfeststellung Vertraulichkeit (zum Beispiel aufgrund der Art der Daten)
- Umfang der Personendaten / Anzahl Betroffene
- Aufwand der Vernichtung
- Wirksamkeit der risikoreduzierenden Massnahmen
- Dauer der maximalen Aufbewahrungsdauer

In den folgenden Kapiteln sind risikoreduzierende Massnahmen beschrieben.

4.1 Anonymisieren

Beim Anonymisieren wird der Personenbezug der Daten entfernt. Dadurch können die Daten nicht oder nur mit einem unverhältnismässig hohen Aufwand einer Person zugeordnet werden. Teilweise können die Daten nicht vollständig anonymisiert werden. Im Zeitalter von Big Data beziehungsweise der Verfügbarkeit umfassender zusätzlicher Informationen lässt sich der Personenbezug oft wiederherstellen (Deanonymisierung).

- Die Artikel-29-Datenschutzgruppe hat eine Stellungnahme zu den Anonymisierungstechniken mit anschaulichen Praxisbeispielen publiziert.

4.2 Schlüssel vernichten

Die Vernichtung aller vorhandenen Schlüssel zur Entschlüsselung der entsprechenden Daten ist eine vorübergehende Massnahme, bis der Datenträger physisch vernichtet wird. Das Restrisiko einer Datenwiederherstellung ist von der Stärke der Verschlüsselung (Algorithmus, Schlüssellänge etc.) abhängig.

4.3 Zugriff sperren

Der Zugriff wird auf wenige Personen beschränkt (zum Beispiel Systemadministrierende), protokolliert und die Zugriffsprotokolle kontrolliert.

4.4 Pseudonymisieren

Beim Pseudonymisieren werden die personenbezogenen Daten durch geheime Identifikatoren ersetzt. Dadurch kann der Personenbezug nur über den Pseudonymisierungsschlüssel wiederhergestellt werden.

4.5 Referenzen löschen

Mit der Löschung der Referenzen können die Personendaten über die Suchmechanismen nicht mehr gefunden werden. Sie sind aber noch im System vorhanden.

5 Berücksichtigung des Speicherorts und der Art der Daten

Beim Vernichten von Daten sind sowohl die Speicherorte als auch die Art der Daten zu berücksichtigen.

Bereits bei der Anschaffung von Systemen und Anwendungen ist die Vernichtung der Daten zu planen. Beispielsweise sind benutzerfreundliche Löschfunktionen (Privacy by Design) als auch Funktionen, die die Löschung unterstützen, explizit zu fordern.

5.1 Daten in Fachanwendungen

In den Fachanwendungen beziehungsweise in den dazugehörigen Datenbanken befinden sich vielfach umfangreiche, strukturierte Personendaten.

Die folgenden Funktionen unterstützen die datenschutzkonforme Vernichtung der Daten:
- Automatische Erinnerung nach Ablauf der Aufbewahrungsfrist
- Möglichkeit zur selektiven Löschung eines Datensatzes
- Automatische Protokollierung des Löschvorgangs
- Automatische Weitergabe von Löschaufträgen an externe Anwendungen
- Regelmässige Löschung des Transaktionsprotokolls

5.2 Daten auf Serverlaufwerken

In der Praxis ist der Grossteil der Personendaten auf Serverlaufwerken gespeichert, oft in Form von Microsoft-Office- und PDF-Dokumenten. Es liegt in der Verantwortung der Datenverantwortlichen, Daten auf Serverlaufwerken regelmässig zu vernichten. Dabei sind automatische Löschprozeduren der manuellen Überprüfung und Löschung vorzuziehen.

Um das Vernichten effizient zu gestalten, sollten die Löschfristen bereits in der Ablagestruktur berücksichtigt werden.

5.3 Sicherungskopien von Daten

Werden Daten gelöscht, müssen sie auch auf allfälligen Testsystemen und Sicherungskopien gelöscht werden. Das Konzept der Datensicherung hat sich an den Aufbewahrungsfristen zu orientieren.

In der Praxis gelingt es nicht immer, die Sicherungskopien zeitnah zu bereinigen. Bei einer Datenwiederherstellung können so gelöschte Daten auf ein System zurückgespielt werden. In diesem Fall ist durch einen entsprechenden Prozess sicherzustellen, dass unverzüglich ein erneutes Vernichten erfolgt. Zudem muss gewährleistet sein, dass die Sicherungskopien ausschliesslich zur Systemwiederherstellung verwendet werden.

5.4 Protokollierungsdaten

Die Protokollierung ist für die Nachvollziehbarkeit und Fehlersuche zentral. Werden Protokollierungsdaten mit Personenbezug nicht mehr benötigt, müssen sie umgehend gelöscht werden.

Es lassen sich zwei Typen von Protokollierungsdaten unterscheiden:
- Protokollierung der Datenbearbeitung zur direkten Aufgabenerfüllung
- Protokollierung zu anderen Zwecken (zum Beispiel Login-Vorgänge, lesende Datenzugriffe, Internetzugriffe)

Die Aufbewahrungsdauer richtet sich nach der Erforderlichkeit. Folgende Angaben gelten als Richtwerte:
- Protokollierung der Datenbearbeitung zur direkten Aufgabenerfüllung: Analog der bearbeiteten Daten
- Protokollierung zu anderen Zwecken: Maximal ein Jahr (je nach Verwendungszweck)

5.5 Daten in der Cloud

Cloud-Ablagedienste werden unter anderem dazu verwendet, um von extern auf die Daten zuzugreifen. Die Kontrollmöglichkeiten bei solchen Daten sind eingeschränkt. Deshalb ist es umso wichtiger, dass sie sobald als möglich gelöscht werden.

Vor der Nutzung eines Cloud-Dienstes sind unter anderem auch die vertraglichen Bestimmungen zur Löschung zu prüfen. Kann der Cloud-Dienst das vollständige Vernichten nicht garantieren, kann er für das Bearbeiten von Personendaten nicht genutzt werden.

5.6 Daten auf mobilen Datenbearbeitungsgeräten

Mobile Datenbearbeitungsgeräte (zum Beispiel Notebooks, Smartphones) erstellen teilweise automatisch Kopien (zum Beispiel E-Mails). So kann mit den Daten ohne Netzwerkverbindung gearbeitet werden. Deshalb sind auch diese Geräte ins Vernichtungskonzept einzubeziehen, beispielsweise durch automatisierte Löschschnittstellen, Weisung für die Benutzung oder ein Mobile Device Management (MDM).

5.7 Daten auf mobilen Datenträgern

Mobile Datenträger (zum Beispiel USB-Sticks) werden häufig verwendet, um Daten von einem IT-System in ein anderes zu übertragen. Die dabei anfallenden Datenkopien sind nach Gebrauch zu löschen. Die Nutzung der mobilen Datenträger ist ganzheitlich zu regeln, inklusive der Umsetzung der Vernichtungsanforderungen.

5.8 Daten auf Write-Once-Read-Many-Speichern (WORMS)

Write-Once-Read-Many-Speicher werden verwendet, um Daten unveränderbar abzuspeichern. Auf diesen Medien ist eine selektive Datenlöschung nicht möglich. Falls Daten gelöscht werden sollen, muss der ganze Datenträger vernichtet werden. Deshalb sollten nur Daten mit ähnlichen Aufbewahrungsfristen auf demselben Datenträger gespeichert werden.

5.9 Daten auf ausgesonderten Geräten

Bei der Aussonderung von Geräten dürfen keine Daten unrechtmässig eingesehen werden. Dies bedeutet, dass die dazugehörigen Datenträger fachgerecht vernichtet werden müssen.

5.10 Daten auf privaten Geräten

Auf privaten Geräten ist die Datenspeicherung zu unterbinden. Dies kann beispielsweise durch die Verwendung von Remote-Desktop-Programmen wie Citrix oder RDP umgesetzt werden. Dabei verbleiben sämtliche Daten im Büro und nur der Inhalt des Bildschirms wird übertragen. Ist dies nicht oder nur bedingt möglich, sind Datenkopien auf privaten Geräten beim Vernichten ebenfalls zu berücksichtigten. Die Datenvernichtung auf privaten Geräten ist vorgängig zu regeln, beispielsweise im Rahmen von Bring-Your-Own-Device-Reglementen.

6 Weiterführende Informationen

Datenschutzbeauftragte des Kantons Zürich
- Merkblatt Informationsverwaltung

Staatsarchiv Kanton Zürich
- Informationsverwaltung – elektronisch und physisch

Bundesamt für Sicherheit in der Informationstechnik (BSI), Deutschland
- Baustein CON.6 Löschen und Vernichten
- Daten auf Festplatten richtig löschen
- Leitlinie zur Entwicklung eines Löschkonzepts

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Deutschland
- Orientierungshilfe Krankenhausinformationssysteme
- Orientierungshilfe «Protokollierung»
- Orientierungshilfe sicheres Löschen magnetischer Datenträger

Weitere Hinweise
- ISO/IEC 29101: Information technology - Security techniques - Privacy architecture framework

V 2.5 / Oktober 2024