FSDZ RECHTSANWÄLTE & NOTARIAT AG
ZUGERSTRASSE 76b
CH-6340 BAAR
Tel. ++ 41 41 727 60 80
Fax.++ 41 41 727 60 85
faessler@fsdz.ch

ERSTGEDANKEN ZU EINEM DATENLÖSCHUNGSKONZEPT

2.9.2019

Lukas Fässler, Rechtsanwalt & Informatikexperte

http://www.fsdz.ch/team/faessler-lukas

/Volumes/DISKs-Public-1/06 FACHTEXTE/Publikation Entwurf Datenlöschungskonzept -V-3-00- 30-08-2019.docx

Ausgehend von Art. 17 Abs. 1 DSGVO besteht seit dem 25.5.2018 die Pflicht zur Datenlöschung, wenn etwa die Speicherung aus fachlichen Gründen nicht mehr notwendig ist. Deshalb sollten Unternehmen möglichst zeitnahe damit beginnen, sich mit dem Thema «richtiges Löschen» von sensiblen Daten zu befassen, zumal die DSGVO entsprechende Konzepte verlangt.

Vor diesem Hintergrund haben wir Ihnen in dieser Publikation einige, nicht abschliessende Überlegungen zur Erarbeitung eines Löschungskonzeptes für die in einer Applikation verwalteten personenbezogenen Daten zusammengestellt.

1. «Weg mit den Daten – aber richtig!»

Quelle: https://www.cio.de/a/weg-mit-den-daten-aber-richtig,3576419

a) Erster Schritt: Datenbestände und Speichersysteme erfassen

- Ermitteln, wo welche Informationen gespeichert sind (SSDs und Festplatten, auf Mobilsystemen, Magnetbändern, Sticks oder DVDs, Network-Attached-Storage-Server [NAS], Drucker und Multifunktionssysteme [Druckdaten]).
- Klärung, ob nur die personenbezogenen Daten zu löschen sind oder alle Daten, auch solche, die nicht direkt personenbezogen sind. Es ist eher zu empfehlen, von einer vollständigen Löschung aller Daten auszugehen. Dies ist einerseits technisch einfacher (keine Extraktion von einzelnen Datenbeständen), aber auch datenschutzrechtlich weniger bedenklich, da allenfalls die Summe nicht gelöschter, nicht personendatenrelevanter

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Partnerkanzleien:

Böhni Rechtsanwälte GmbH
Roman Böhni
MLaw Rechtsanwalt,
BSc Wirtschaftsinformatik
Tel.: ++41 41 541 79 60
roman.boehni@boehnilaw.ch
www.boehnilaw.ch

de la cruz beranek Rechtsanwälte AG
Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin
delacruz@delacruzberanek.com

Nicole Beranek Zanon
Rechtsanwältin und Notarin[1,2]
beranek@delacruzberanek.com

Industriestrasse 7
CH-6300 Zug
Tel.: ++41 41 710 28 50
Fax: ++41 41 710 90 76
www.delacruzberanek.com
UID: CHE-389.928.945 MWST

Lichtsteiner Rechtsanwälte und Notare
Urs Lichtsteiner
lic. iur. Rechtsanwalt[1,2], MSc (Stanford)
lichtsteiner@lilaw.ch

Baarerstrasse 10, Postfach 7517
CH-6302 Zug
Tel.: +41 41 726 90 00
Fax: +41 41 726 90 05
www.lilaw.ch
info@lilaw.ch
UID: CHE-404.805.335 MWST

Anwaltskanzlei Dr. Weltert
Hans M. Weltert
Dr. iur. Rechtsanwalt[1,4]
hans.weltert@raweltert.ch

Matthias Heim
lic.iur. Rechtsanwalt[1,4]
matthias.heim@raweltert.ch

Michael Heim
lic.iur. Rechtsanwalt[1,4]
michael.heim@raweltert.ch

Bahnhofstrasse 10
CH-5001 Aarau
Tel.: +41 62 832 77 33
Fax: +41 62 832 77 34
www.raweltert.ch
info@raweltert.ch
UID: CHE-100.877.506 MWST

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug
[3] Eingetragen im Anwaltsregister des Kantons Zürich
[4] Eingetragen im Anwaltsregister des Kantons Aargau

Informationen wiederum einen Rückschluss auf eine Einzelperson zulassen könnten.
- Sicherstellen, dass **gesetzliche Aufbewahrungsfristen** eingehalten werden. Klärung, welche gesetzlichen Grundlagen einen Einfluss auf die zu löschenden Daten haben (Bundesgesetze, Kantonale Gesetze oder Verordnungen).

b) Zweiter Schritt: Die richtige Methode für Löschen von Daten finden
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt in seinen IT-Grundschutz-**Kompendium**[1] einen Fragenkatalog bereit, mit dessen Hilfe Unternehmen eine Anforderungsanalyse (CON.6.A1 ff.) durchführen können (abrufbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_6_Löschen_und_Vernichten.html)**= IT-Grundschutz-Katalog 2016, Ziffer M.2.167, S. 1818 ff.** (Letzterer abrufbar unter https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf, zuletzt besucht am 30.8.2019).

Zu berücksichtigen ist beispielsweise:

- Ob die SSD's, Festplatten oder Magnetbänder nach dem Löschen weiterhin benutzt werden sollen oder nicht. Wenn nicht, können sie geschreddert werden.
- Welche Datenträger und Datentypen vorhanden sind, etwa Word- und Excel-Dateien, Einträge in Datenbanken, Adressinformationen etc.
- Ob zertifizierte Tools für das sichere Löschen vorhanden sind und Mitarbeiter diese bedienen können.
- Welchen Schutzbedarf die gespeicherten Daten haben und ob sich diese Informationen mit den vorhandenen Werkzeugen gesetzeskonform vernichten lassen.

«Delete» ist keine Lösung
Das BSI empfiehlt, ein "Leasing" durchzuführen. Dabei werden Daten auf einem Datenträger durch ein mehrmaliges Überschreiben mit Zufallszahlen (Nullen und Einsen) unlesbar gemacht.
Das erfolgt mit kommerziellen Tools wie zum Beispiel «Blancco» (https://www.blancco.com/de/), das in Versionen für Server, PCs, mobile Endgeräte und Speicher-Systeme zur Verfügung steht. Zudem gibt es kostenlose Software, beispielsweise DBAN (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/DBAN/dban_node.html) und Parted Magic (https://partedmagic.com) und natürlich weitere.

Drei bis sieben Mal «erasen»
Laut BSI reichen bei normalen Geschäftsdaten drei Erasing-Vorgänge aus, bei vertraulichen Informationen ist ein siebenmaliges Überschreiben angesagt. Das gilt beispielsweise für Verschluss-Sachen von Behörden, medizinische Daten sowie Entwicklungsunterlagen von Unternehmen. Nach Einschätzung des BSI ist es in jedem Fall besser, den kompletten Datenträger zu löschen.

SSD's erfordern eine Sonderbehandlung
Um eine SSD sicher zu löschen, kann paradoxerweise ein Befehl verwendet werden, der eigentlich für Festplatten vorgesehen ist: „ATA Secure Erase". Er eignet sich für Solid State Drives, die über den

[1] Seit 2018 gibt es das IT-Grundschutz-Kompendium als Nachfolgewerk der IT-Grundschutz-Kataloge.

SATA-Bus an einen Rechner angebunden sind. Ausserdem liefern Anbieter von SSD‘s wie Samsung, Western Digital, Intel oder Micron ihre Flash-Speicher mit Tools aus, mit denen der Nutzer ein "Erasing" durchführen kann.

Gewalt anwenden
Wenn Datenträger wie SSD‘s, Festplatten, Speicherkarten oder DVDs nicht mehr weiterverwendet werden, bietet sich das Schreddern der Datenträger durch spezielle Systeme an. Eines davon ist der Degausser. Dabei werden magnetische Datenspeicher starken magnetischen Feldern ausgesetzt, wodurch die Datenträger unwiederbringlich vernichtet werden. Solche Systeme sind allerdings mit rund EUR 5'000.00 sehr teuer.

Schreddern
(Quelle: https://www.aktenvernichterdirekt.de/Din-Sicherheitsstufen?id=1&cat=Din-Sicherheitsstufen)

- Für das Schreddern sieht die DIN 66399 **drei Schutzklassen** vor:

  Schutzklasse 1:
  steht für die normale Sicherheit, welche für interne Daten erforderlich ist, bei denen ein Unternehmen zu Schaden kommen könnte, wenn es an die Öffentlichkeit kommen würde, oder die Gefahr von Identitätsraub besteht.

  Schutzklasse 2:
  steht für die höhere Sicherheit für vertrauliche Daten, bei denen es zu negativen Auswirkungen für ein Unternehmen oder zur Verletzung gesetzlicher Bestimmungen kommen kann, wenn diese an die Öffentlichkeit gelangen.

  Schutzklasse 3:
  steht für die höchste Sicherheit, welche für besonders vertrauliche oder geheime Daten, bei denen es zu schwersten Schäden in einem Unternehmen oder Regierungseinrichtung kommen kann, wenn diese an die Öffentlichkeit gelangen.

  Des Weiteren gibt es **sechs Unterkategorien**:

  P Papierprodukte
  F Informationen in verkleinerter Form wie Filme, Mikrofiche usw.
  O Optische Datenträger wie CD’s, DVD’s und Blu-ray usw.
  T Magnetische Datenträger wie Disketten, Ausweise, magnetische Bänder und Kassetten usw.
  H Festplatten mit magnetischen Datenträgern, Laptops und externe Festplatten
  E Elektronische Datenträger wie Memorysticks, Laufwerke und Mobiltelefone

  Hinzu kommen **sieben Sicherheitsstufen**: Die Stufe 1 gilt für allgemeine Daten, etwa Broschüren und Kataloge. Die höchste Stufe 7 ist für streng geheime Informationen vorgesehen.

Beispielsweise für die Unterkategorie **P**:

P-1 12 mm Streifen oder max. Partikelgrösse von 2.000 mm²
P-2 6 mm Streifen oder max. Partikelgrösse von 800 mm²
P-3 2 mm Streifen oder max. Partikelgrösse von 320 mm²
P-4 Partikelschnitt von max. 160 mm² mit einer Streifenbreite von max. 6 mm = 6x25 mm
P-5 Partikelschnitt von max. 30 mm² mit einer Streifenbreite von max. 2 mm = 2x15 mm
P-6 Partikelschnitt von max. 10 mm² mit einer Streifenbreite von max. 1 mm = 1x10 mm
P-7 Partikelschnitt von max. max. 5 mm² mit einer Streifenbreite von max. 1mm = 1x5 mm

2. Fragenkatalog des IT-Grundschutz-Katalogs 2016:

Welche Verfahren geeignet sind, um die in einer Institution vorkommenden Daten oder Datenträger zu löschen oder zu vernichten, hängt von der Art der Datenspeicherung, der Datenträger und vom Grad der Schutzbedürftigkeit der Informationen ab. Auch ist zu berücksichtigen, für welche weitere Verwendung der Datenträger vorgesehen ist. Daher sollte eine **Anforderungsanalyse** vor der Auswahl durchgeführt werden, um geeignete Verfahren zu finden.

Hierbei sollten unter anderem **folgende Fragen** beantwortet werden:

- Welche Datentypen (auf welchen Betriebssystemen und in welchen Anwendungen) und welche Datenträgertypen (z. B. optisch oder magnetisch) mit welchen Datenvolumen (z. B. Megabyte, Gigabyte, Terabyte) sollen sicher gelöscht werden?
- Wie hoch ist der Schutzbedarf der auf den Datenträgern gespeicherten Daten?
- Wie gross ist Datenträger selbst? Wird das Ergebnis der Vernichtung dem Schutzbedarf gerecht?
- Wurden bzw. werden die Datenträger in einem geschützten Bereich verwendet?
- Sind bereits Werkzeuge zum Löschen und Vernichten von Informationen vorhanden? Sind diese geeignet für den identifizierten Schutzbedarf und die vorhandenen Datenträger-Arten?
- Welche Arten von Lösch- und Vernichtungsverfahren existieren für den identifizierten Schutzbedarf und die vorhandenen Datenträger-Arten? Wie hoch ist der Schulungsaufwand, um diese zuverlässig zu benutzen?
- Wie gross ist die voraussichtliche Menge von Datenträgern eines Typs, der gelöscht bzw. vernichtet werden soll?

Diese Fragen sind möglichst mit allen involvierten Dateneigentümern einheitlich und verbindlich zu klären. Sie stellen den Ausgangspunkt für das technische und organisatorische Lösungskonzept dar, welches – im Falle der Auslagerung von Betriebsservices an Dritte – in den Datenverarbeitungsvertrag neu aufzunehmen ist.

Es muss **nachvollziehbar dokumentiert** werden, welche Verfahren zum Löschen und Vernichten für die verschiedenen Datenarten und den jeweiligen Schutzbedarf ausgewählt wurden und wie diese anzuwenden sind.

Die Mitarbeiter müssen in die ausgewählten Verfahren zum Löschen und Vernichten von Informationen eingewiesen werden, vor allem, wenn sie die entsprechenden Werkzeuge selber benutzen sollen (Schulungskonzept).

Prüffragen:

- Wurden für die verschiedenen Datenarten und den jeweiligen Schutzbedarf angemessene Verfahren zum Löschen oder Vernichten festgelegt?
- Wurden die Mitarbeiter in die Verfahren zum Löschen und Vernichten von Informationen eingewiesen, vor allem in den Gebrauch der vorhandenen Werkzeuge und Geräte?
- Stehen für die verschiedenen Arten von Datenträgern geeignete Geräte und Werkzeuge zum zuverlässigen Löschen oder Vernichten der gespeicherten Informationen zur Verfügung?
- Wird das Ergebnis der Vernichtung regelmässig kontrolliert?
- Wird das für einen Datenträger gewählte Vernichtungsverfahren dem Stand der Technik (z. B. Grösse des Datenträgers) gerecht?

3. Anonymisierung und Pseudonymisierung

Als weitere, jedoch nicht unumstrittene, Möglichkeit nennt etwa die Datenschutzbeauftragte des Fürstentums Lichtenstein die (ledigliche) Überschreibung und damit die vermeintliche Unkenntlichmachung der jeweiligen personenbezogenen Daten mittels Ersetzung durch eine zufällige Abfolge von Buchstaben und/oder Zahlen (nicht rückführbare **Anonymisierung** oder **Pseudonymisierung**).

Die Datenschutzbeauftragte Lichtenstein setzt eine solche Methode einer «physischen oder digitalen» Löschung gleich (vgl. «Empfehlung zur Vernichtung von Personendaten», Datenschutzstelle Fürstentum Lichtenstein vom September 2017, abrufbar unter https://www.fsdz.ch/file-docs/16_-_pdf-llv-dss-empfehlung-vernichtung-von-daten_1.pdf, zuletzt besucht am 30.8.2019).

Gemäss einer neusten Studie der Universität Zürich ist die Anonymität bei einer Anonymisierung nicht immer gewährleistet. Durch das sogenannte «Linkage-Verfahren» können nämlich die vielen **öffentlich** zur Verfügung gestellten Daten und insbesondere deren nicht anonymisierte Details miteinander verknüpft werden. Dadurch kann die eigentliche Information wieder gefunden und die vermeintliche Anonymisierung somit aufgehoben werden (vgl. Beitrag der SRF Tagesschau vom 1.9.2019, abrufbar unter https://www.srf.ch/play/tv/tagesschau/video/wenn-gerichtsurteile-ploetzlich-oeffentlich-zugaenglich-sind?id=756bd4dc-c9b5-42eb-8931-9077cd934fff, zuletzt besucht am 2.9.2019).

4. Empfehlung

Wir empfehlen Ihnen, mit der Aufbereitung der Grundlagen sowie mit der Ausarbeitung eines Datenlöschungskonzeptes nach diesen Grundsätzen zu beginnen. Da jeder Datenlöschungsfall anders gelagert ist, können keine Mustervorlagen zur Verfügung gestellt werden. Sie können jedoch aus den obenstehenden Unterlagen eruieren, welche Nachweisdokumente im Rahmen eines Löschungskonzeptes unbedingt mitberücksichtigt werden müssen.

Wir empfehlen Ihnen zudem aus Erfahrung, zuerst mit der Erstellung eines umfassenden **Dateninventars** in Bezug auf die relevanten Daten zu starten und dieses Dateninventar mit einer Bewertung (personenbezogene Daten; nicht personenbezogene Daten) zu ergänzen. Zudem sollten Sie

ein Nachweisdokument erstellen oder dessen Inhalte direkt im obigen Dateninventar integrieren, welche **Ansprechgruppen** (alle Verantwortlichen und alle Nutzer der Daten) **Zugriff zu welchen Daten** haben. Dies ist massgeblich für die Frage, wer zu welchen Daten seinen Input bezüglich einer Löschung abgeben darf und kann. Schliesslich ist die **operative Umgebung** in einem **Betriebsschema** schematisch darzulegen. Alsdann ist nach dem obigen Verfahren vorzugehen und die dargestellten weiteren Unterlagen auszuarbeiten.

Wir empfehlen zudem, in Vertragsunterlagen keine Details zum Löschungskonzept festzulegen, sondern nur einen neuen Grundsatz dazu in allgemeiner Form (wer macht was mit wem bis wann in welcher Form) festzuhalten; im Übrigen die Details in einem **separaten Anhang** zu den massgeblichen Verträgen festzulegen. Die Technik schreitet bezüglich der Datenlöschung derart rasant voran, dass die technischen und organisatorischen Leitlinien, Weisungen oder Vorgaben in jedem Falle viel schneller wieder angepasst werden müssen als die übrigen Vertragsklauseln. Es macht daher Sinn, im Falle eines Anpassungsbedarfs nur den Anhang zu ändern, ohne ein aufwendiges Anpassen und Unterzeichnen eines neuen Vertragswerkes durchführen zu müssen.

FSDZ Rechtsanwälte & Notariat AG
Lukas Fässler
Rechtsanwalt