DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Empfehlung zur Vernichtung von Personendaten

Herausgeber:

Datenschutzstelle
Städtle 38
Postfach 684
9490 Vaduz

Fürstentum Liechtenstein

T +423 236 60 90

info.dss@llv.li
www.dss.llv.li

Version 1.0 / September 2017

Inhaltsverzeichnis

1. Einleitung

Das Vernichten von Personendaten stellt eine Konkretisierung des in Art. 4 Abs. 2 Datenschutzgesetz (DSG) normierten Verhältnismässigkeitsprinzips dar. Der Inhaber einer Datensammlung darf nur diejenigen Daten bearbeiten, die für die Erfüllung einer jeweils konkreten Aufgabe (Zweckerreichung) unbedingt notwendig und geeignet sind. Grundsätzlich gilt, dass Personendaten zu anonymisieren oder zu vernichten sind, wenn diese für die Erreichung der Zwecke, für die sie bearbeitet wurden, nicht mehr benötigt werden.[1] Im Zeitalter des Datensammelns und der vernetzten Systeme ist die praktische Umsetzung zur Einhaltung der Bestimmungen an eine angemessene Vernichtung in vielen Fällen indes nicht trivial.

Ziel dieser Empfehlung ist es, den Inhabern von Datensammlungen[2] Hilfestellung bei der Einhaltung ihrer Verpflichtung zur Vernichtung personenbezogener Daten zu geben. Die gegenständliche Empfehlung erklärt die wesentlichen Merkmale sowie begriffliche und technische Abgrenzungen und stellt abschliessend mögliche Vorgehensweisen für die datenschutzkonforme Vernichtung vor.

Sie führt dabei *nicht* aus, wie die Auswahl einer geeigneten Methode zur Vernichtung anhand bestimmter Kriterien für eine konkrete Datenbearbeitung erfolgt. Ebenfalls ist *nicht* Inhalt, wie die Fristen für die Vernichtung zu bestimmen sind oder aus welchen Gründen (z. B. Widerruf einer Einwilligung) Daten vernichtet werden müssen oder davon Abstand genommen werden kann. Speziell die Fristen hängen in der Regel von spezialgesetzlichen Rechtsvorschriften sowie den zulässigen Zwecken einer Datenbearbeitung ab und sind für jeden Einzelfall festzulegen. In diesem Zusammenhang sollte der Dateninhaber bzw. der Verantwortliche ein Regelwerk (Löschregime) erstellen und darin insbesondere die internen Verantwortungen bestimmen.[3]

Heute (September 2017) gilt ausschliesslich das DSG. Wo zweckmässig und sinnvoll wird in der gegenständlichen Empfehlung bereits auf die Datenschutz-Grundverordnung (DSGVO) hingewiesen, die zukünftig unter bestimmten Umständen von Verantwortlichen[4] auch in Liechtenstein zu berücksichtigen sein wird. *Entsprechende Textstellen und Verweise sind kursiv geschrieben.*

Detaillierte Ausführungen zu spezifischen Bestimmungen der DSGVO, wie bspw. das Recht auf Löschung („Recht auf Vergessenwerden“) sowie das Verfahren betreffend die Informationspflicht in Bezug auf die Löschung aller Links zu Personendaten oder Kopien oder Replikationen dieser Daten aus öffentlich zugänglichen Kommunikationsdiensten[5], finden sich dagegen *nicht* in dieser Empfehlung. Hierzu wird der Ausschuss *(engl. Data Protection Board)* entsprechende Leitlinien und Empfehlungen bereitstellen.[6]

[1] Vgl. Art. 19a und Art. 25 DSG sowie *Art. 5 Abs. 1 Bst. e DSGVO*.
[2] Art. 3 Abs. 1 Bst. k DSG.
[3] Weitere Ausführungen dazu finden sich in der „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“, http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/DINLoeschkonzeptLeitlinie.pdf?__blob=publicationFile.
[4] Art. 7 Ziff. 7 DSGVO.
[5] Art. 17 Abs. 1 und Abs. 2 DSGVO.
[6] Vgl. Art. 70 Abs. 1 Bst. d DSGVO.

2. Begrifflichkeiten und Rechtsrahmen

Das *Vernichten* von personenbezogenen Daten stellt eine Form der Datenbearbeitung dar.[7] Das DSG sieht vor, dass **private Personen**[8] personenbezogene Daten zu anonymisieren oder zu vernichten haben, wenn diese für die Erreichung der Zwecke, für die sie bearbeitet wurden, nicht mehr benötigt werden[9]. Eine allgemeingültige minimale oder maximale Aufbewahrungsfrist für Personendaten findet sich im DSG sowie in der Datenschutzverordnung (DSV) nicht. Lediglich im Zusammenhang mit Videoüberwachungsbewilligungen (maximale Speicherdauer von 30 Tagen)[10] und der Protokollierung (mindestens ein Jahr)[11] kennt das DSG feste Fristen. Im Grundsatz gilt, dass die Aufbewahrung von Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Bearbeitung notwendige Mass beschränkt sein muss (Verhältnismässigkeit).[12]

Eine betroffene Person kann von Privaten zum Schutz ihrer Persönlichkeit verlangen, dass die sie betreffenden Personendaten vernichtet werden.[13]

Vernichtungsbegehren gegenüber Privaten
Die betroffene Person hat an einem (Online-)Wettbewerb mitgemacht und Kontaktdaten wie E-Mail-Adresse, Wohnort, Telefonnummer usw. bekanntgegeben. Im Anschluss bekommt die Person regelmässig Werbezuschriften. Die Person kann in diesem Fall jederzeit gegen die Zusendung von Werbung widersprechen und die Vernichtung ihrer Daten verlangen.

Ungeachtet eines Antrags einer betroffenen Person kann der Dateninhaber bzw. der Verantwortliche von einer Vernichtung absehen, wenn ein überwiegendes Interesse oder ein Gesetz (z. B. Aufbewahrungspflichten aufgrund spezialgesetzlicher Bestimmungen) eine weitere Bearbeitung rechtfertigen.[14]

Für **Behörden**[15] gilt, dass diese in Übereinstimmung mit dem Archivgesetz dem Amt für Kultur alle Personendaten anbieten müssen, die sie nicht mehr benötigen. Die Behörden vernichten die Personendaten, die vom Amt für Kultur als nicht archivwürdig bezeichnet wurden, ausser wenn sie anonymisiert sind oder zu Beweis- oder Sicherungszwecken erhalten bleiben müssen.[16]

[7] Art. 3 Abs. 1 Bst. g DSG, *vgl. Art. 4 Ziff. 2 DSGVO*.
[8] Natürliche und juristische Personen sowie rechtsfähige Personengesellschaften, die dem Privatrecht unterstehen; Art. 3 Abs. 1 Bst. c DSG.
[9] Art. 19a DSG, *vgl. Art. 17 Abs. 1 Bst. a DSGVO*.
[10] Art. 6a Abs. 7 DSG. Siehe auch Entscheid der Datenschutzkommission DSK2010/4 vom 17. Dezember 2010, http://www.llv.li/files/dss/pdf-llv-dss-entscheid_dsk_2010-4_public.pdf.
[11] Art. 11 Abs. 2 DSV. Siehe auch Empfehlung zur Protokollierung, Pkt. 10, http://www.llv.li/files/dss/pdf-llv-dss-protokollierung_art_11_dsv.pdf.
[12] Art. 4 Abs. 2 und 3 DSG, *vgl. Art. 5 Abs. 1 Bst. c DSGVO (Grundsatz der „Datenminimierung")*.
[13] Art. 16 Abs. 2 Bst. b iVm Art. 37 Abs. 1 DSG, *vgl. Art. 17 Abs. 1 DSGVO*.
[14] Art. 17 Abs. 1 Bst. b und c DSG.
[15] Organe des Staates, der Gemeinden und von Körperschaften, Stiftungen und Anstalten des öffentlichen Rechts sowie auch Private, soweit sie in Erfüllung der ihnen übertragenen öffentlichen Aufgaben tätig sind; Art. 3 Abs. 1 Bst. d DSG.
[16] Art. 25 DSG.

Gegenüber Behörden kann eine betroffene Person in bestimmten Fällen ebenfalls die Vernichtung verlangen.[17]

Vernichtungsbegehren gegenüber Behörden aufgrund eines Spezialgesetzes
Eine betroffene Person verlangt die Vernichtung von im Schengener Informationssystem (SIS) gespeicherten Daten nach Art. 47 Abs. 2 der Verordnung über den nationalen Teil des Schengener Informationssystem (N-SIS) und das SIRENE-Büro (N-SIS-Verordnung).

Die eingesetzten IT-Systeme und die Vernichtungsprozesse müssen so ausgestaltet sein, dass nach Ablauf der Aufbewahrungsfrist bzw. Erreichung des Vernichtungszeitpunkts oder einem entsprechenden Begehren die Vernichtung zeitnah durchgeführt werden kann.[18] Dies bedeutet, dass die Struktur der Daten und die Art der Speicherung so ausgestaltet sein müssen, dass das Vernichten von Inhalten (z. B. einzelner Datenfelder, Datensätze oder vorher definierter Gruppen von Daten) einzelner Betroffener mit beherrschbarem Aufwand möglich ist. Die Granularität hängt hier 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 diese vernichtet werden können.

Gemäss DSGVO sollten Mechanismen festgelegt werden, die dafür sorgen, dass die betroffenen Personen unentgeltlich deren Löschung beantragen können und dass Anträge elektronisch gestellt werden können.[19]

Das Vernichten von Daten unterstützt die Gewährleistungsziele der Datensparsamkeit und Vertraulichkeit.

2.1 Vernichtung/Löschung

Wie die Begrifflichkeiten *Vernichten* und *Löschen* konkret voneinander abzugrenzen sind, ist weder im DSG noch in der DSGVO legal definiert. Das DSG kennt ausschliesslich die (Daten-)Vernichtung. In verschiedenen nationalen Gesetzen wird der Begriff *Löschung* vielfach synonym mit dem Begriff der *Vernichtung* verwendet.[20] In der DSGVO wird im Gegensatz zum DSG mehrheitlich der Begriff *Löschen* verwendet, wobei der Begriff *Vernichtung* ebenfalls Erwähnung findet, jedoch als eigenständige Verarbeitungshandlung zu interpretieren ist.[21]

Umgangssprachlich wird von **Vernichtung** gesprochen, wenn mit den Informationen oder dem Personenbezug auch der Datenträger selbst zerstört wird. Unter **Löschung** wird die unwiederbringliche Zerstörung oder Unkenntlichmachung und damit die irreversible Entfernung von in Datensammlungen gespeicherten personenbezogenen Daten verstanden. Dies bedeutet, dass zuvor vorhandene Personendaten nach dem Vorgang des Löschens – dem Löschprozess – nicht mehr vorhanden oder unkenntlich sind und nicht mehr rekonstruiert werden können.[22] Ein allfälliger Datenträger kann nach dem Löschen in der Regel erneut beschrieben und verwendet werden.

[17] Art. 21 Abs. 2 Bst. c oder Art. 25 iVm Art. 38 Abs. 3 Bst. a DSG.
[18] Art. 10 Abs. 2 Bst. a DSV, *vgl. Art. 25 Abs. 1 und 2 DSGVO*.
[19] Vgl. Erwägungsgrund 59 DSGVO.
[20] Vgl. z. B. Art. 34e Abs. 1 und Art. 34i Abs. 2 Polizeigesetz (PolG).
[21] Vgl. Begriffsbestimmungen zu „Verarbeitung" in Art. 4 Ziff. 2 DSGVO: „[…] das Löschen oder die Vernichtung;".
[22] Vgl. § 3 Abs. 4 Ziff. 5 de-BDSG oder auch Basler Kommentar, 3. Auflage, DSG 21 RN 14.

Vernichtung/Löschung
Vernichten einer Festplatte z. B. durch Schreddern, wobei der Datenträger im Anschluss nicht mehr verwendet wird oder werden kann. Löschen der Festplatte z. B. durch Überschreiben sämtlicher Speicherbereiche mit Zufallswerten, wodurch diese bei Bedarf erneut beschrieben werden kann.

Beim Löschen wird zusätzlich zwischen der zuvor beschriebenen Zerstörung oder Unkenntlichmachung von Daten in der Weise, dass eine Rekonstruktion ausgeschlossen ist (*physisches Löschen*), und der Verhinderung des Zugriffs von Daten durch programmtechnische Massnahmen (*logisches Löschen*) unterschieden. Eine **logische Löschung** bezeichnet eine Massnahme, mit der erreicht wird, dass Daten automatisierter Datenbearbeitungen sämtlichen Nutzern nicht mehr zur Verfügung stehen, z. B. indem die betreffenden Daten bspw. durch das Betriebssystem als nicht mehr vorhanden interpretiert werden.[23] Ob logisches Löschen für eine konkrete Datenbearbeitung eine angemessene oder geeignete technische Massnahme im Sinne einer datenschutzkonformen Vernichtung nach dem DSG darstellt oder im Einzelfall physisch zu löschen ist, hängt insbesondere von der Art und dem Umfang der Datenbearbeitung sowie den möglichen Risiken für die betroffenen Personen ab.[24]

Rein organisatorische Massnahmen, wie z. B. ein erweiterter Zugriffsschutz oder eine Sperre, bei welcher der Dateninhaber bzw. Verantwortliche die Verfügung über die Daten nicht endgültig verliert, stellen jedenfalls kein Vernichten oder Löschen – weder physisch noch logisch – im Sinne des DSG dar.

2.2 Datenkategorien und Datenbestände

Betreffend die Löschpflicht des Verantwortlichen kennt weder das DSG noch die DSGVO Einschränkungen auf bestimmte Datenkategorien oder personenbezogene Datenbestände. Somit betrifft die Pflicht zur Vernichtung grundsätzlich alle Datenkategorien und neben dem aktiven Datenbestand ebenso sämtliche personenbezogenen Daten in Archiven und Sicherungskopien.[25]

2.3 Abgrenzung zur Anonymisierung

Anonymisieren: Ein Verfahren, welches Personendaten *unwiderruflich* auf eine solche Weise verändert, dass die betroffenen Personen weder direkt noch indirekt durch den Verantwortlichen allein sowie auch nicht unter Zuhilfenahme jedes anderen Beteiligten identifiziert werden können.[26] Vorhandene Daten müssen demnach so verändert werden, dass es selbst unter Verwendung aller Mittel, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden könnten, nicht mehr möglich ist, eine betroffene Person zu bestimmen. Ein wesentlicher Faktor dabei ist, dass die Veränderung unumkehrbar sein muss. Die Artikel-29-Datenschutzgruppe analysiert in einer Stellungnahme die

[23] Vgl. Dammann/Simitis, EG-Datenschutzrichtlinie, Anm. 16 zu Art. 12, S. 198. , sowie Urteil des österreichischen OGH 6Ob41/10p vom 15.04.2010, Abschnitt 5.3, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20100415_OGH0002_0060OB00041_10P0000_000.
[24] Art. 9 Abs. 2 DSV. *vgl. Art. 32 DSGVO*.
[25] Siehe Abschnitt 4.5, S. 13.
[26] Vgl. ISO/IEC 29100:2011, Information technology – Security techniques – Privacy Framework, Pkt. 2.2.

Wirksamkeit und die Grenzen der derzeit vorhandenen Anonymisierungstechniken und spricht Empfehlungen für den Umgang mit diesen Techniken aus.[27]

Die Anonymisierung als Alternative zur Vernichtung wird in einer eigenen Richtlinie der Datenschutzstelle über die Anwendung der Anonymisierung/Pseudonymisierung im Detail dargestellt.[28] Grundsätzlich ist eine Vernichtung der Daten zu bevorzugen, wenn diese nicht mehr benötigt werden. Gemäss DSG sind die Anonymisierung und Vernichtung in ihrer Funktion zwar als gleichwertig zu betrachten, doch Daten die isoliert betrachtetet nicht personenbezogen sind, können im Zusammenhang mit Big Data unter Umständen de-anonymisiert werden.[29] Im Zusammenhang mit Big Data hat die DSS eine entsprechende Richtlinie veröffentlicht.[30]

3. Vorgehensweise zur Vernichtung

Zur datenschutzkonformen Ausgestaltung der Prozesse zur Vernichtung von Daten ist ein Verzeichnis der Datensammlungen unumgänglich. In der Praxis wird es ein Dateninhaber bzw. ein Verantwortlicher zwecks Einhaltung der jeweils geltenden Datenschutzbestimmungen ohnehin wissen müssen, welche Datensammlungen vorliegen, welche Datenkategorien darin bearbeitet werden und welche Lösch- oder Aufbewahrungsfristen jeweils vorgesehen sind.

Für bestimmte Unternehmen wird eine Verpflichtung zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten mit der DSGVO eingeführt.[31] So hat gemäss Grundverordnung der Verantwortliche, wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien in diesem Verzeichnis aufzuführen.[32] Ebenfalls mit der DSGVO wird eine umfassende Rechenschaftspflicht für den Verantwortlichen eingeführt.[33] Im Zusammenhang mit dem Vernichten/Löschen von Daten bedeutet dies, dass der Verantwortliche im Vergleich zum DSG umfangreiche zusätzliche Dokumentations- und Nachweispflichten zu erbringen hat. So hat der Verantwortliche gem. DSGVO unter anderem nachzuweisen, dass ein implementierter Vernichtungsprozess datenschutzkonform ausgestaltet ist und insbesondere sämtliche Datenbestände berücksichtigt.

3.1 Festlegung der Verantwortlichkeit

Verantwortlich für die Datenbearbeitung und somit für die ordnungsgemässe Vernichtung ist jene private Person oder Behörde, die über den Zweck und den Inhalt einer Datensammlung entscheidet.[34] Der Dateninhaber hat in seiner Rolle als Verantwortlicher festzulegen, welche Regeln für die Vernichtung in den entsprechenden Datensammlungen gelten. Aus diesen Re-

[27] „Stellungnahme 5/2014 zu Anonymisierungstechniken“, Artikel-29-Datenschutzgruppe, WP216 vom 10. April 2014.
[28] Richtlinie über die Anwendung der Anonymisierung/Pseudonymisierung, http://www.llv.li/files/dss/pdf-llv-dss-richtlinie-anonymisierung-pseudonymisierung.pdf.
[29] Vgl. Artikel-29-Datenschutzgruppe, WP 203, Opinion 03/2013 on purpose limitation, gefunden unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, S. 47.
[30] Richtlinie Big Data, http://www.llv.li/files/dss/pdf-llv-dss-richtlinie-big-data.pdf.
[31] Art. 30 DSGVO (Verzeichnis von Verarbeitungstätigkeiten).
[32] Art. 30 Abs. 1 Bst. f DSGVO.
[33] Art. 5 Abs. 2 iVm Art. 24 Abs. 1 DSGVO.
[34] Inhaber der Datensammlung, Art. 3 Abs. 1 Bst. k DSG.

geln müssen konkrete Umsetzungsvorgaben ableitbar sein. Ebenso müssen diese Regeln Massgaben für die Dokumentation beinhalten.[35]

Mit der DSGVO wird neu die gemeinsame Verantwortlichkeit für eine Verarbeitung eingeführt, wobei hier in einer Vereinbarung in transparenter Form festgelegt werden muss, wer welche Verpflichtungen erfüllt.[36]

3.2 Vernichtungszeitpunkt

Ein Dateninhaber bestimmt für jede Datenkategorie in einer Datensammlung, in der Regel basierend auf spezialgesetzlichen Rechtsnormen oder anderen vertraglichen Regelungen den Zeitpunkt, ab welchem die Daten zu vernichten sind. Dieser Zeitpunkt ist jener, nach der die Daten bei *regulärer Bearbeitung* einer verantwortlichen Stelle spätestens zu vernichten sind. Kann ein solcher Zeitpunkt begründeter Weise nicht konkret bestimmt werden, hat eine regelmässige Prüfung zu erfolgen, um festzustellen, ob die gespeicherten Daten für den konkreten Zweck noch benötigt werden.[37] Die Frist zur Vernichtung leitet sich in diesen Fällen aus den allgemeinen Prinzipien und Bestimmungen des DSG (z. B. Datensparsamkeit) ab.

Vernichtungszeitpunkt
Fixer Zeitpunkt: Mit Stichtag *x* müssen sämtliche gespeicherten Daten vernichtet sein.

Abhängig von der Erhebung: Die Daten sind sechs Monate nach der Speicherung unverzüglich zu vernichten.[38]

Abhängig von der Bearbeitung oder Auflösung eines Vertragsverhältnisses: Die Daten sind *x* Monate nach dem letzten Bearbeitungsvorgang oder Kontakt mit der betroffenen Person zu vernichten.

Die Zeitpunkte für die Vernichtung werden jeweils für den Regelbetrieb bestimmt. Sämtliche Sonderfälle, wie z. B. Reklamationen oder Rechtsstreitigkeiten, in den jeweiligen Bearbeitungsprozessen zu berücksichtigen, ist in der Praxis schwierig. Doch der Ausweg, für sämtliche Daten sehr lange Fristen für die Vernichtung festzulegen, um mögliche Sonderfälle entsprechend berücksichtigen zu können, ist datenschutzrechtlich nicht vertretbar und unverhältnismässig.[39]

Behandlung von Sonderfällen
Für einen Geschäftsprozess ist eine gesetzliche Frist für die Vernichtung von Daten vorgesehen. Im Reklamationsfall oder einem Rechtsstreit kann notwendig sein, diese Daten über die festgelegte Frist aufzubewahren und vor automatisierter Vernichtung zu bewahren. Technisch kann dies abgebildet werden, indem die Daten entsprechend gekennzeichnet oder an anderer Stelle gespeichert werden.

In manchen Situationen werden Kopien von Daten aus dem Regelbetrieb (Datenabzüge) für besondere Verwendungen benötigt. Datenabzüge, die ausserhalb der Regelprozesse verwendet werden, müssen ebenfalls innert einer festgesetzten Frist vernichtet werden.

[35] Vgl. Richtlinie über die Pflichten des Inhabers der Datensammlung, http://www.llv.li/files/dss/pdf-llv-dss-richtlinie-pflichten-inhaber-datensammlung.pdf.
[36] Art. 26 Abs. 1 DSGVO.
[37] Art. 4 DSG (Verhältnismässigkeit), *Vgl. Art 5 Abs. 1 Bst. e iVm Erwägungsgrund 39 DSGVO*.
[38] Vgl. Art. 52a KomG.
[39] Vgl. Abschnitt 4.6, S. 14.

Bei Erreichen des festgelegten Vernichtungszeitpunkts sind die entsprechenden Daten unmittelbar dem Vernichtungsprozess zuzuführen.

3.3 Vernichtungsprozess

Unter Vernichtungsprozess wird jener Ablauf verstanden, mit dem sichergestellt wird, dass in einer Datensammlung personenbezogene Daten datenschutzkonform vernichtet bzw. gelöscht werden. Um Daten wirksam vernichten zu können, sind Massnahmen auf der Ebene der Daten, der technischen Systeme und der dazugehörigen Prozesse erforderlich. Für die Festlegung eines geeigneten Vernichtungsprozesses sind vor allem die Datenschutzanforderungen betreffend den Umfang, die Datenstruktur sowie den Speicherort zu berücksichtigen.

Vernichtungsprozess
Anforderungen an den Umfang: Sind einzelne Datenfelder, ganze Datensätzen oder gesamte Datensammlungen zu löschen oder der Datenträger selbst zu vernichten!

Datenstruktur: Beispielsweise als Datensätze in einer Datenbank, in Form von Listen in Dateien oder auch als einzelne Dokumente in einer Dateiablage (Verzeichnisstruktur).

Ort der Speicherung: Beispielsweise in einer verteilten Datenbank, in einer zentralen externen Dateiablage (z. B. auf Netzwerklaufwerken), in lokalen Kopien auf Einzelplatzrechnern oder bei einem Outsourcing-Partner.

Der Vernichtungsprozess berücksichtigt begleitende Schutzmassnahmen derart, dass eine Wiederherstellung der Daten für einen Angreifer mit dessen finanziellen oder materiellen Mitteln nicht nur erschwert oder unattraktiv, sondern auch praktisch nicht durchführbar ist. Durch die Anwendung angemessener Schutzmassnahmen können die Anforderungen an die Ausgestaltung und die damit verbundene Auswahl an technischen und organisatorischen Massnahmen anhand einer konkreten Interessensabwägung durchaus vereinfacht sein.

Der Aufwand, den der Inhaber einer Datensammlung für die Vernichtung notwendigerweise betreiben muss, entspricht dem *Stand der Technik*[40] und soll im Verhältnis zum Schutzbedarf der bearbeiteten Daten stehen. Zu berücksichtigen sind dabei jedenfalls

- die Sensitivität (Schutzbedarf) der Daten,
- die Menge (Quantität) der Daten (z. B. Anzahl der betroffenen Personen),
- die Schwere der möglichen Risiken für die Rechte und Freiheiten der betroffenen Personen,
- das Risiko der Wiederherstellung *(durch einen Angreifer)* unter Berücksichtigung begleitender Sicherheitsmassnahmen und
- die zu erwartende Stärke der Angreifer oder der von ihnen betriebene Aufwand zur Datenrekonstruktion.

Je sensibler die zu vernichtenden Daten sind, desto höhere Anforderungen sind an die technischen und organisatorischen Massnahmen zur Vernichtung zu stellen.

[40] Zum *Stand der Technik* siehe „Handreichung zum „Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (ITSiG)", TeleTrusT – Bundesverband IT-Sicherheit e.V., 2016, https://www.all-about-security.de/fileadmin/micropages/Fachartikel_25/TeleTrusT-Handreichung_Stand_der_Technik.pdf.

War eine Datenerhebung nicht rechtmässig oder handelt es sich im Hinblick auf die Zwecke ihrer Bearbeitung um unrichtige Daten, können einem Inhaber einer Datensammlung höhere Anforderungen zur Entsprechung der Bestimmungen zur Vernichtung der Daten zugemutet werden.

Einsatz von angemessenen Sicherheitsmassnahmen
Ausgangslage: Löschen einer auf einem PC ausschliesslich lokal gespeicherten Teilnehmerliste (Namen und E-Mail-Adressen) für eine Veranstaltung. Begleitende Massnahmen: Der Zugang zum PC (z. B. aufgrund abgesperrter Büroräumlichkeiten) ist für Unbefugte nicht möglich. Der Datenträger des Rechners wird am Ende seines Lebenszyklus ordnungsgemäss vernichtet (Schredder).

Werden die Dokumente in dieser Konfiguration in den Papierkorb verschoben, entspricht dies *keiner* Löschung im Sinne des DSG. Wird jedoch direkt (logisch) gelöscht oder der Papierkorb unmittelbar geleert und ist die lokale Festplatte zudem verschlüsselt sowie durch weitere begleitende Massnahmen vor unbefugtem Zugriff geschützt, sind die Anforderungen an eine datenschutzkonforme Vernichtung bzw. Löschung erfüllt.

Da sich die Datenstrukturen und Speicherungstechniken, sprich der *Stand der Technik*, laufend ändern, muss allenfalls eine Nachvernichtung vorgenommen werden, wenn durch die Anwendung neuer Techniken an und für sich bereits vernichtete Daten wiederhergestellt werden könnten.[41]

Bei der Ausgestaltung des Prozesses sind automatisierte Abläufe manuellen vorzuziehen. Durch die Automatisierung wird eine Durchsetzung der Vorschriften erzwungen und eine Umgehung erheblich erschwert. Werden Daten automatisiert vernichtet, kann es sinnvoll sein, weitere Prozesse zu implementieren, die jederzeit ein gezieltes Aussetzen und Unterbrechen des automatisierten Vernichtungsprozesses ermöglichen.[42]

Ist ein Bearbeitungsreglement oder *ein Verzeichnis von Verarbeitungstätigkeiten gem. DSGVO zu erstellen*, ist darin der Vernichtungsprozess allgemein zu beschreiben.[43] Der Verantwortliche oder ein möglicher Auftragsverarbeiter stellen der Datenschutzstelle das Verzeichnis auf Anfrage zur Verfügung.[44]

Der Vernichtungsprozess ist abgeschlossen, wenn die zu vernichtenden Daten nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können.

3.4 Vernichtung von Protokolldateien

Protokolldaten sind ein wesentlicher Bestandteil der Datensicherheit. Die in den Protokollen aufgezeichneten Ereignisse, wie z. B. Nutzeraktivitäten, Ausnahmen/Sonderfälle *(engl. exceptions)*, Fehler *(engl. faults)* oder andere Ereignisse betreffend die Informationssicherheit,[45] können insbesondere dazu verwendet werden, um zeitnah als auch rückwirkend Verursacher von Verletzungen des Schutzes personenbezogener Daten festzustellen, Sicherheitslücken aufzude-

[41] Basler Kommentar, 3. Auflage, DSG 21 RN 14, *vgl. Art. 32 Abs. 1 Bst. d DSGVO*.
[42] Vgl. dazu Regelbetrieb und Ausführungen in Abschnitt 4.6, S. 14.
[43] Art. 12 Abs. 2 Bst. g DSV (für Private) sowie Art. 21 Abs. 2 Bst. g DSV (für Behörden), *Art. 30 Abs. 1 DSGVO*.
[44] Art. 30 Abs. 2 DSG (für Private) sowie Art. 21 Abs. 3 DSV (für Behörden), *vgl. Art. 30 Abs. 4 DSGVO*.
[45] Vgl. ISO/IEC27002:2013, 12.4 Logging and monitoring.

cken oder die Effektivität und Effizienz von technischen und organisatorischen Sicherheitsmassnahmen zu untersuchen.

Protokolldaten sind gem. Art. 11 DSV während eines Jahres revisionsgerecht festzuhalten.[46] Für eine darüber hinausgehende Aufbewahrung finden die allgemeinen Bestimmungen des DSG zur Datenvernichtung Anwendung, wonach die Protokolle unmittelbar nach Zweckerreichung zu vernichten sind.[47] Sogenannte „Datenfriedhöfe" sind zu vermeiden.

Vernichten von Protokolldaten
Protokolldaten unterliegen der Vernichtungspflicht, wenn sie Personendaten enthalten. Dies wird in den meisten Fällen anzunehmen sein; z. B. User-IDs (direkte Bestimmbarkeit) oder Terminal-IDs oder andere Gerätekennungen (indirekte Bestimmbarkeit).

Betreffend die Bestimmung des Vernichtungszeitpunkts sind insbesondere zu berücksichtigen, welche Ereignisse in den Protokollen aufgezeichnet werden und welcher Personenkreis von der Aufzeichnung betroffen ist. So werden die Protokolldaten einer Gebäudezutrittsverwaltung, von welcher vorwiegend die Mitarbeiter betroffen sind, in der Regel früher zu vernichten sein als bspw. die Protokolldaten einer Sicherheitslösung einer eBanking-Applikation, die wesentlich mehr Angriffsvektoren bietet.

Soweit das Vernichten selbst protokolliert wird, dürfen in diesen Protokollen keine Daten enthalten sein, für die eine Verpflichtung zur Vernichtung besteht.[48]

4. Verfahren zur Vernichtung/Löschung

Nicht alle Verfahren zur Vernichtung der Daten sind für jede Datenbearbeitung gleichermassen geeignet. Dies hängt vor allem vom verwendeten Datenträger und der Struktur der gespeicherten Daten im weitesten Sinn ab.[49] Es sollen im Folgenden die wichtigsten Verfahren zur Vernichtung und Löschung kurz beschrieben werden. Im Weiteren findet sich ein Überblick über Methoden zur Vernichtung und Löschung von Daten im BSI-Grundschutzkatalog.[50]

4.1 Vernichtung von Datenträgern

Im Zusammenhang mit Datenträgern, sowohl von physischen (z. B. Papier) als auch elektronischen (z. B. Festplatten), wird bei der Vernichtung neben der gespeicherten Information auch der Datenträger selbst auf eine solche Weise verändert (zerstört), dass die darauf gespeicherten Daten nicht mehr gelesen werden können und eine Wiederherstellung nach dem Stand der Technik nicht möglich ist.[51]

Vernichtung von Datenträgern
Das Schreddern von Papier oder digitalen Datenträgern wie Festplatten oder USB-Sticks.

[46] Art. 11 Abs. 2 1. Satz iVm Art. 11 Abs. 1 DSV.
[47] Art 4 Abs. 2 (Verhältnismässigkeit) und Abs. 3 DSG (Zweckbindung).
[48] Vgl. „Empfehlung zur Protokollierung (Art. 11 DSV)", http://www.llv.li/files/dss/pdf-llv-dss-protokollierung_art_11_dsv.pdf.
[49] Vgl. M 2.167, „Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten", BSI-Grundschutzkatalog.
[50] M 2.433, „Überblick über Methoden zur Löschung und Vernichtung von Daten", BSI-Grundschutzkatalog, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02433.html.
[51] Basler Kommentar, 3. Auflage, DSG 21 RN 15, DIN 66399, Vernichtung von Datenträgern.

4.2 Überschreiben

Überschreiben der Informationen einzelner Datenfelder (Daten oder Attribute von Daten), die auf elektronischen Datenträgern gespeichert wurden, mit Hilfe von Löschprogrammen (z. B. so genannte Wipe-Tools), oder komplettes Überschreiben ganzer Datenträger mit speziellen Lösch- oder Anwendungsprogrammen. Dabei ist sicherzustellen, dass diese für die Verwendung mit den jeweiligen Datenträgern geeignet sind.

Überschreiben von Flash-basierten Solid-State-Disks
Moderne auf Flash-Speicher-Technologien basierende SSDs unterstützen verschiedene Methoden der Nutzungsverteilung, wodurch Schreibvorgänge bestmöglich auf alle Speicherzellen gleich häufig verteilt werden. Dies hat Einfluss auf die Wiederherstellbarkeit von auf solchen Datenträgern gespeicherten Daten. Diese sogenannten Wear-Levelling-Algorithmen sind entsprechend zu berücksichtigen.

Ein Hauptnachteil des Überschreibens liegt darin, dass Daten auf defekten Datenträgern oder Datenträgern mit schadhaften Speicherbereichen mit Hilfe einer Softwarelösung im Regelfall nicht einwandfrei gelöscht werden können.

Abseits der automatisierten Datenbearbeitung können Inhalte und Personendaten durch Schwärzen bestimmter Stellen in Papierakten „überschrieben“ werden. Hierbei ist jedoch darauf zu achten, dass in vielen Fällen das blosse Schwärzen des Namens oder anderer direkter Identifikatoren nicht ausreichend ist, um die Anonymität der betroffenen Personen zu wahren.[52]

4.3 Löschen eines Entschlüsselungsschlüssels

Das Löschen eines Entschlüsselungsschlüssels von verschlüsselt gespeicherten Daten kann in Abhängigkeit verschiedenster Faktoren im Zusammenhang mit der eingesetzten Kryptographie allenfalls eine Massnahme darstellen, um eine gewisse Zeitspanne bis zur Löschung der Daten selbst oder bis zur physikalischen Vernichtung des Datenträgers zu überbrücken. Es muss jedoch zwingend durch begleitende technische und organisatorische Massnahmen sichergestellt sein, dass bis zum Löschen der Daten oder dem Vernichten des Datenträgers der Schutz der Rechte der betroffenen Personen gewährleistet ist.

4.4 Vernichtung bei einer Auftragsdatenbearbeitung

Entscheidend ist hier, dass der Auftraggeber immer für die Daten und deren rechtmässige Bearbeitung verantwortlich bleibt. Der Auftraggeber hat Sorge dafür zu tragen, dass der Auftragsdatenbearbeiter die Personendaten nur so bearbeitet, wie er/sie es selbst tun dürfte.[53] Dies betrifft auch die Vernichtung der beim Auftragsbearbeiter gespeicherten Daten.

Gerade bei der Nutzung von Cloud-Diensten – eine Form der Auftragsdatenbearbeitung – sind deshalb zum Zweck der Beweissicherung die datenschutzrelevanten Elemente und die Anforderungen in Bezug auf Massnahmen zur Vernichtung schriftlich, z. B. in Form einer vertraglichen

[52] Vgl. Abschnitt 2.3.
[53] Art. 19 Abs. 1 Bst. a) DSG, *vgl. Art. 5 Abs. 2 DSGVO*.

Vereinbarung oder in einer anderen Form, zu dokumentieren.[54] Der Anbieter der Cloud-Dienste ist zu verpflichten, sich an die in Liechtenstein geltenden Datenschutzbestimmungen zu halten und diese vollumfänglich zu akzeptieren.

Werden im Rahmen des Cloud-Service Personendaten ins Ausland bekannt gegeben, sind zusätzlich die Vorschriften zu berücksichtigen, die die Zulässigkeit grenzüberschreitender Datentransfers regeln.[55]

4.5 Archive und Sicherungskopien (Backups)

Archive und Sicherungskopien *(engl. Backups)* sind von der Vernichtung nicht ausgenommen. Weder das DSG noch die DSGVO sieht hier eine Ausnahme vor. Der Vernichtungsprozess hat demnach die Datenspeicherungen in Archiven und Backups entsprechend zu berücksichtigen.

Archive dienen dazu, Daten langfristig zur Verfügung zu haben. Daten werden häufig in Archive verlegt, wenn an Datensätzen oder an den aktiven Datenbeständen keine Veränderungen mehr vorgenommen werden, sie jedoch aus zulässigen Gründen weiterhin aufbewahrt werden müssen. Ein Archiv kann unterschiedliche Datenarten mit unterschiedlichen Fristen für die Vernichtung enthalten. Hinsichtlich des Archivs müssen die betroffenen Personendaten aktiv durch den Verantwortlichen vernichtet werden.[56]

Sicherungskopien dienen, im Gegensatz zum Archiv, ausnahmslos der Datenwiederherstellung nach einem Datenverlust, wie z. B. aufgrund eines Systemausfalls. Es gibt verschiedenste Backup-Strategien. Bei einer häufig verwendeten Strategie (dem Generationenprinzip oder Grossvater-Vater-Sohn-Prinzip) wird bspw. jeweils zu einem bestimmten Zeitpunkt (z. B. nach jedem Arbeitstag, wöchentlich, monatlich usw.) eine Datensicherung auf einen Datenträger (Festplatte, Band o.ä.) vorgenommen. Regelmässig werden dabei die vorherigen Datensicherungen überschrieben. Werden Daten im Originaldatenbestand vernichtet, sind diese in den späteren Datensicherungen ebenfalls nicht mehr vorhanden und können deshalb auch im Rahmen einer nachträglichen Datenwiederherstellung nicht mehr rekonstruiert werden.

Lediglich auf jenen Sicherungsmedien auf denen der Zeitraum zwischen der Vernichtung aus dem Originaldatenbestand und der anschliessenden Datensicherung entsprechend lange ist, bspw. bei den monatlichen oder gar halbjährlichen Datensicherungen, kann es vorkommen, dass bereits vernichtete Daten bis zum Überschreiben noch auf den bestehenden Sicherungsmedien gespeichert sind. In jenen Fällen hat der Verantwortliche, z. B. nach einem Datenverlust, dafür Sorge zu tragen, dass durch ausgleichende und angemessene technische und organisatorische Massnahmen keine Datenwiederherstellung von bereits im Originaldatenbestand vernichteten Daten von den erwähnten Sicherungsmedien stattfindet.

Im besten Fall sind Backup-Systeme dergestalt konzipiert, dass die entstehenden Datensicherungen eine Vernichtung der relevanten Daten auch im Nachhinein ermöglichen.

[54] Art. 19 Abs. 3 DSG, *vgl. Art. 28 Abs. 3 DSGVO*.
[55] Vgl. Art. 8 DSG.
[56] Vgl. Abschnitt 4.1 oder 4.2, S. 11 f.

4.6 Aussetzen von Vernichtungsprozessen

Ausnahmen von den festgelegten Fristen der Vernichtung können sich bei Fehlern in Programmen oder fehlerhaften Datenbeständen ergeben. In diesen Fällen ist zu prüfen, ob kurzfristig in einer Sondersituation die Frist zur Vernichtung von Daten ausgesetzt werden kann.[57] Durch angemessene und geeignete ausgleichende Massnahmen muss jedoch sichergestellt werden, dass die Aussetzung des Vernichtungsprozesses begrenzt wird, der betroffene Datenbestand möglichst klein und der Zeitraum der Aussetzung verhältnismässig ist. Als Kriterien für die Ausgestaltung der Aussetzung können z. B. die Sensitivität der Daten sowie die Massnahmen zur Zweckbindung der Daten herangezogen werden. Bei Rückkehr in den Regelbetrieb müssen alle Daten der Ausnahmeregelung vernichtet werden.

5. Weitere Informationen

- Richtlinie über die Anwendung der Anonymisierung/Pseudonymisierung http://www.llv.li/files/dss/pdf-llv-dss-richtlinie-anonymisierung-pseudonymisierung.pdf
- Empfehlung zur Protokollierung (Art. 11 DSV) http://www.llv.li/files/dss/pdf-llv-dss-protokollierung_art_11_dsv.pdf
- DIN Deutsches Institut für Normung e.V., Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Leitlinie_zur_Entwicklung_eines_Loeschkonzepts.pdf
- Der Bayerische Landesbeauftragte für den Datenschutz informiert zum Thema Datenträgerentsorgung – Orientierungshilfe, https://www.datenschutz-bayern.de/technik/orient/oh_datentraegerentsorgung.pdf
- Der Bayerische Landesbeauftragte für den Datenschutz, Orientierungshilfe: Protokollierung, https://www.datenschutz-bayern.de/technik/orient/oh_protokollierung.html
- EDÖB, Datenvernichtung, http://www.edoeb.admin.ch/datenschutz/00683/00803/00818/index.html

[57] Unter Berücksichtigung von Art. 4 Abs. 2 (Verhältnismässigkeit).