SVTPT
FSPA
FSFA
FSFB

SCHWEIZERISCHER VERBAND FÜR TIERPHYSIOTHERAPIE ®
FÉDÉRATION SUISSE DE PHYSIOTHÉRAPIE POUR ANIMAUX
FEDERAZIONE SVIZZERA DELLA FISIOTERAPIA PER ANIMALI
FEDERAZIUN SVIZRA DELLA FISIOTERAPIA PER BES-CHAS

Leitfaden für die Aufbewahrung und Archivierung

Bern, 13.04.2023

Illustration: © strichfiguren – AdobeStock (bearbeitet von Physioswiss)

Die Grundlage für dieses Merkblatt wurde Physioswiss freundlicherweise zur Verfügung gestellt von der Verbindung der Schweizer Ärztinnen und Ärzte (FMH).

Schweizer Physiotherapie Verband
Association Suisse de Physiothérapie
Associazione Svizzera di Fisioterapia

Physioswiss, Dammweg 3, 3013 Bern
058 255 36 00, info@physioswiss.ch, www.physioswiss.ch

Inhalt

1. Rechtliche Anforderungen zur Aufbewahrung und Archivierung

1.1 Gesetzliche Aufbewahrungsfristen (Stand 31.10.2022)

In Gesundheitseinrichtungen fallen täglich Dokumentationen an, welche unter anderem auch Angaben (Personendaten) über Patient:innen sowie Mitarbeitende der Gesundheitseinrichtung selbst oder von Dienstleistenden beinhalten. Die Aufbewahrung dieser Dokumentationen ergeben sich aufgrund des Prinzips der Verhältnismässigkeit. Personendaten dürfen deshalb so lange aufbewahrt werden, wie sie geeignet und erforderlich sind für die Aufgabenerfüllung. Bundesgesetze und kantonale Erlasse legen zudem konkrete Aufbewahrungsfristen fest. Neben diesen kann ein Zweck zur Aufbewahrung auch darin bestehen, die Nachvollziehbarkeit einer Behandlung, einer Leistungsbeurteilung oder eines Sachverhaltes zu Beweiszwecken zu gewährleisten.

Geschäftsdaten, welche keine Personendaten enthalten, können grundsätzlich unbegrenzt aufbewahrt werden. Mindestens sind sie aber solange aufzubewahren, wie es gesetzliche Aufbewahrungsfristen vorsehen.

Zur Orientierung enthalten die nachfolgenden Tabellen eine Zusammenstellung der gesetzlich vorgesehenen Anforderungen an die Art und Dauer der Aufbewahrung. Bestehen keine gesetzlichen Regelungen zur Aufbewahrung, verlangt das Datenschutzgesetz, dass mindestens die Kriterien für die Aufbewahrung festgelegt werden (Art. 12 DSG).

Da während der gesamten Aufbewahrungsdauer sicherzustellen ist, dass der Datenschutz und insbesondere die Datensicherheit gewährleistet bleiben, ist in einem letzten Abschnitt dieses Kapitels zudem eine Checkliste enthalten, welche mögliche technische und organisatorische Massnahmen zur Aufrechterhaltung der Datensicherheit aufzeigt.

Exkurs: Übergabe/Aufgabe der Geschäftstätigkeit – Aufbewahrungspflicht Patientendokumentation

Grundsätzlich bleibt bei Aufgabe oder Übergabe der Geschäftstätigkeit die Aufbewahrungsplicht der Patientendokumentation bestehen. Hierbei wird unterschieden, mit wem die Patienten jeweils den Behandlungsvertrag abgeschlossen haben. Das heisst, wenn der Behandlungsvertrag mit einer Gemeinschaftspraxis (AG oder GmbH) geschlossen wurde, verbleibt die Aufbewahrungspflicht bei der Gemeinschaftspraxis selbst. Wurde hingegen der Behandlungsvertrag mit der/dem Physiotherapeut:in geschlossen, hat sie/er für eine angemessene Aufbewahrung der Patientendokumentation zu sorgen.

Übernimmt eine Nachfolgerin (eine natürliche oder juristische Person) die Physiotherapiepraxis bzw. die weitere Behandlung der Patient:innen, bedeutet dies nicht automatisch, dass die Patientendokumentationen ihr/ihm übergeben werden dürfen resp. Sie/er Einsicht erhält. Die Einsicht darf der/dem Nachfolger:in nur gewährt werden, wenn eine vorgängige Einwilligung seitens Patient:in vorliegt. Liegt (noch) keine Einwilligung seitens der/des Patient:in vor, kann das sogenannte Zwei-Schränke-Prinzip angewendet werden. Dies bedeutet, in einen Schrank kommen die Patientendokumentationen , bei welchen die Patient:innen in die Behandlung durch die/den Nachfolger:in zugestimmt haben. In den zweiten Schrank kommen die Patientendokumentation, für welche (noch) keine Einwilligung

für die Einsicht vorliegt. Bei der elektronischen Führung von Patientendokumentation kommt grundsätzlich die gleiche Regelung zur Anwendung.

Bei Aufgabe der Tätigkeit stehen Physiotherapeut:innen weiterhin in der Pflicht, innert der gesetzlichen Frist Patient:innen Auskunft über die Patientendokumentation zu geben. Folglich haben Physiotherapeut:innen dafür zu sorgen, dass die Patientendokumentationen auf eine angemessene Art und Weise aufbewahrt werden und vor unberechtigten Zugriffen geschützt sind.
Beispielsweise lagert sie diese privat oder delegiert die Aufbewahrung an einen Dritten.

Hinweis: Zusätzlich sind die allfällig geltenden kantonalen Bestimmungen (kantonale Gesundheits- oder Patientengesetze) zu konsultieren, da diese längere Aufbewahrungsfristen oder besondere Formen der Aufbewahrung vorsehen könnten.

1.2 Übersicht gesetzliche Aufbewahrungsfristen

Gesundheitsdaten /Patientendokumentation		
Art der Unterlagen	**Aufbewahrungsdauer/-art**	**Rechtliche Grundlage**
Patientendokumentation	Aufgrund der Verjährungsfrist im Haftungsrecht ist die Patientendokumentation **20 Jahre** nach Abschluss der jeweiligen Behandlung aufzubewahren. Darüber hinaus darf sie nur mit der Zustimmung der betroffenen Person aufbewahrt bleiben. ***Hinweis:*** *Für die geltenden Aufbewahrungspflichten betreffend Dauer und Art sind jeweils die für den Standort der Physiotherapiepraxis geltenden kantonalen Gesundheitsgesetze Zu konsultieren. Für Patientendokumentationen sehen die kantonalen Bestimmungen mindestens eine Aufbewahrungspflicht von **zehn Jahren** vor. Einige Kantone erlassen allerdings für spezifische Fälle eine Aufbewahrungspflicht von **20 Jahren**. Weiter wird von wenigen kantonalen Erlassen eine Vernichtung der Unterlagen nach 20 Jahren vorgesehen, wenn dem kein überwiegendes Interesseentgegensteht.*	Art. 60 Abs. 1bis und 2 Obligationenrecht (OR)/Art. 128a OR Kantonale Gesundheitsgesetze (abhängig vom Standort der Physiotherapiepraxis)

Mitarbeiterdokumentation

Art der Unterlagen	Aufbewahrungsdauer/-art	Rechtliche Grundlagen
Personaldossier (Arbeitsverträge, Mitarbeiterdossier inkl. Beurteilungen, Arbeitszeugnissen, Bestätigungen, Aktennotizen, Verwahrungen, Kündigung etc.)	**fünf Jahre** ab Austritt der/des Mitarbeitenden, auf Papier (analog) oder elektronisch (digital), sodass der Sachverhalt nachgewiesen und jederzeit wieder lesbar gemacht werden kann.	Art. 330a OR i.V. Art. 128 OR/ Art. 46 Arbeitsgesetz (ArG) und 73 Verordnung 1 zum Arbeitsgesetz (ArGV 1)
Lohnwesen (Lohnausweise, Abrechnungen, Sozialversicherungen und Pensionskasse)	**fünf Jahre** ab Austritt der/des Mitarbeitenden, auf Papier (analog) oder elektronisch (digital), sodass der Sachverhalt nachgewiesen und jederzeit wieder lesbar gemacht werden kann.	Art. 128 Abs. 3 OR
Arbeitszeiterfassung (Erfasste Arbeitszeiten in einem Zeiterfassungssystem)	**fünf Jahre** ab Austritt des/der Mitarbeitenden, auf Papier (analog) oder elektronisch (digital), sodass der Sachverhalt nachgewiesen und jederzeit wieder lesbar gemacht werden kann.	Art. 46 Arbeitsgesetz (ArG) und 73 Verordnung 1 zum Arbeitsgesetz (ArGV 1)

Geschäftsunterlagen

Art der Unterlagen	Aufbewahrungsdauer/-art	Rechtliche Grundlagen
Rechnungen (Debitoren, Kreditoren, Jahresabschlüsse inkl. Revisionsberichten)	**zehn Jahre** ab Beendigung des Geschäftsjahres, auf Papier (analog), elektronisch (digital) oder in vergleichbarer Weise, sodass der Sachverhalt gewährleistet ist und jederzeit wieder lesbar gemacht werden kann.	Art. 958 und 958f OR
Steuerunterlagen (sämtliche Unterlagen im Zusammenhang mit Steuern)		
Spesen (Spesenbelege sowie sämtliche Unterlagen im Zusammenhang mit Spesen)		

Sonstige Dokumentation

Art der Unterlagen	Aufbewahrungsdauer/-art	Rechtliche Grundlagen
Protokolle bei automatisierter Bearbeitung von besonders schützenswerten Personendaten/Profiling	Sofern die Physiotherapiepraxis besonders schützenswerte Personendaten automatisiert bzw. digitalisiert bearbeitet und die eingesetzten Massnahmen keinen genügenden Datenschutz bieten, hat sie die Bearbeitung zu protokollieren. Die Protokolle sind während **einem Jahr** revisionsgerecht aufzubewahren.	Art. 4 Verordnung über den Datenschutz (DSV)
Datenschutz-Folgenabschätzung (DSFA) (sämtliche relevanten Unterlagen im Rahmen einer Datenschutz-Folgenabschätzung)	Mindestens **zwei Jahre** ab Beendigung der Datenbearbeitung. ***Hinweis:*** *Eine Pflicht zur Erstellung einer DSFA besteht, wenn Personendaten bearbeitet werden, welche bei einer allfälligen Verletzung der Vertraulichkeit, der Integrität oder bei einem Missbrauch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person haben könnten.* *Ausgenommen von der Pflicht zur Erstellung einer DSFA sind private Verantwortliche, welche gesetzlich zur Bearbeitung der Daten verpflichtet sind. Das bedeutet, dass privatrechtliche Gesundheitseinrichtungen aufgrund der gesetzlichen Verpflichtung zur Führung einer Patientendokumentation grundsätzlich keine DSFA vornehmen müssen.* *Dies gilt nur für die Führung der Patientendokumentation gemäss Gesetz. Sollen in Gesundheitseinrichtungen beispielsweise Cloud-Produkte eingesetzt werden, könnte eine DSFA notwendig werden, da der Einsatz einer Cloud nicht gesetzlich vorgeschrieben ist.*	Art. 14 DSV
Dokumentation Verletzung der Datensicherheit (sämtliche relevanten Unterlagen im Zusammenhang mit der Meldung zu einer Verletzung der Datensicherheit)	Mindestens **zwei Jahre** ab dem Zeitpunkt der Meldung einer Verletzung der Datensicherheit.	Art. 15 DSV

1.3 Checkliste zur Aufbewahrung und Archivierung von Personendaten

Sind die Daten aufgrund von einem oder mehreren der oben genannten oder aus anderen Gründen aufzubewahren, so ist sicherzustellen, dass die Datensicherheit auch während der Aufbewahrung gegeben ist. Die nachfolgenden Checklisten können als Hilfestellung zur Gewährung der Datensicherheit bei der Aufbewahrung beigezogen werden.

Hinweis: *Im Zusammenhang mit der Frage, ob und wie Personendaten gelöscht werden dürfen, bietet der Leitfaden für die Aufbewahrung und Archivierung eine Hilfestellung.*

Ort		
Massnahme	**Erläuterung/Hinweise**	**Check**
Zugangsverwaltung	Datenträger mit Personendaten sind an einem Ort aufzubewahren, zu dem nur ein ausgewählter Personenkreis Zugang hat. Beispielsweise in verschliessbaren Aktenschränken, Archiven, Räumen mit Schlüssel- oder Badge-System etc., wobei nur die berechtigten Personen im Besitz der Schlüssel oder eines Badges sind.	☐
Schutz vor umweltbedingten Ereignissen	Die Datenträger sind so aufzubewahren, dass diese nicht durch Wasser, Feuer oder andere umweltbedingte Ereignisse zerstört werden können.	☐

Format

Massnahme	Erläuterung/Hinweise	Check
Schutz vor Korrosion/ Papierzerfall	Datenträger sind auf eine Art und Weise aufzubewahren, dass diese nicht durch Korrosion (digitale Datenträger) oder Papierzerfall (physische Datenträger) zerstört werden können.	☐
Aktuelle Formate	Digitale Daten sind in einem Format aufzubewahren, welches langfristig gelesen werden kann. Ist dies nicht möglich, ist sicherzustellen, dass die Daten rechtzeitig in ein aktuelles Format übertragen werden. Nachfolgend aufgeführte Formate sind archivtauglich:	☐

Anwendungsbereich	Archivtaugliche Formate
Dokumente von Office (Word, Excel, Powerpoint, Outlook)	PDF/A
Text (unformatiert)	TXT
Tabellen	CSV
Datenbanken	SIARD
Digitale Bilder	TIFF oder PDF/A
Audio	WAVE
Video	MPEG-4

Hinweis: *Die Übertragung von Daten in ein anderes Format kann die Daten verändern oder andere Beeinträchtigungen hervorrufen*

Zugriff

Massnahme	Erläuterung/Hinweise	Check
Zugriffsberechtigungen	Es wird nur denjenigen Personen Zugriff auf die Daten gewährt, welche die Daten wirklich benötigen (z. B. zu Beweiszwecken im Rahmen eines Haftungsanspruches, zur Sicherstellung der Lesbarkeit etc.). Berechtigungen für den Zugriff auf Daten sind auf ein notwendiges Minimum zu beschränken (z. B. Beschränkung auf ein bis zwei Personen). Es ist sicherzustellen, dass die Berechtigungen den Gegebenheiten angepasst werden können (z. B. Mutation, Stellvertretung etc.).	☐
Schutz von Authentisierungsmitteln	Es ist sicherzustellen, dass die Authentisierungsmittel (z. B. Benutzername/Passwort, Schlüssel, Badge) während der gesamten Aufbewahrungsdauer verfügbar, aber vor dem Zugriff durch unberechtigte Personen geschützt sind.	☐
Aktuelle Verschlüsselungstechnologien	Es ist sicherzustellen, dass Verschlüsselungstechnologien zum Einsatz kommen, welche eine Entschlüsselung während der gesamten Aufbewahrungsdauer ermöglichen. Sofern die Technologien während der Aufbewahrungszeit eine Änderung erfahren, sind die Daten rechtzeitig mit einer neuen Technologie zu verschlüsseln.	☐
Back-up	Werden die Daten in Form eines digitalen Back-ups aufbewahrt, ist die Wiederherstellung des Back-ups regelmässig (Empfehlung einmal jährlich) zu testen.	☐

Nachvollziehbarkeit

Massnahme	Erläuterung/Hinweise	Check
Schutz vor unberechtigter Veränderung	Es ist sicherzustellen, dass Veränderungen an aufbewahrten Daten ersichtlich und nachvollziehbar sind. • Papierdokumente und Wechseldatenträger: z.B. Liste mit manuell eingetragener Protokollierung • Digitale Datenträger: z.B. Protokollierung von Änderungen (Logging), auch während der Aufbewahrung	☐
Schutz der Protokollierung	Systeme zur Protokollierung sowie Protokolle sind vor unbefugtem Zugriff und vor Manipulation zu schützen.	☐

Zusammenarbeit mit Dritten

Massnahme	Erläuterung/Hinweise	Check
Vertragliche Bestimmungen	Werden Dritte in die Aufbewahrung involviert, ist sicherzustellen, dass vertragliche Vorgaben zur Aufbewahrung vereinbart sind und die Einhaltung dokumentiert wird. ***Hinweis:*** *Beim Beizug von Dienstleistenden für die Aufbewahrung ist sicherzustellen, dass die Dienstleistenden sorgfältig ausgewählt, über ihre Pflichten instruiert und regelmässig überprüft werden. Es wird empfohlen, eine Geheimhaltungserklärung durch die Dienstleistenden unterzeichnen zu lassen. Eine Vorlage kann hier heruntergeladen werden.*	☐
Behandlung bei Verletzung der Datensicherheit	Werden Dritte in die Aufbewahrung involviert, ist sicherzustellen, dass das Vorgehen bei Verletzung der Datensicherheit definiert ist.	☐
Vertraglich vereinbarte Herausgabe	Werden Dritte in die Aufbewahrung involviert, ist sicherzustellen, dass eine Herausgabe der Daten bei Beendigung der Zusammenarbeit erfolgt.	☐

Erfüllung der Vorgaben

Massnahme	Erläuterung/Hinweise	Check
Kontrolle der Aufbewahrungsfristen	Die Fristen zur Aufbewahrung sind sichergestellt und Personendaten werden nach Ablauf der Frist unverzüglich und unwiderruflich gelöscht oder vernichtet.	☐
Dokumentation	Die Fristen zur Aufbewahrung und die anschliessende Löschung/Vernichtung sind zu dokumentieren.	☐

2. Rechtliche Grundlagen Löschung

2.1 Allgemeines

Dieses Dokument bietet eine Hilfestellung dafür, wann Personendaten gelöscht bzw. vernichtet werden können bzw. müssen und was dabei zu beachten ist.

Personendaten dürfen nur zu einem bestimmten Zweck bearbeitet werden und soweit sie für diesen geeignet und erforderlich sind. Sobald die Personendaten für den Zweck der Bearbeitung nicht mehr erforderlich sind, sind sie zu löschen bzw. zu vernichten oder zu anonymisieren.

Betroffene Personen haben zudem das Recht, die Löschung ihrer Personendaten zu verlangen, sofern kein Rechtfertigungsgrund mehr für deren Bearbeitung besteht. Rechtfertigungsgründe sind Verjährungsfristen und Aufbewahrungsfristen. Diese sind je nach Fallkonstellation unterschiedlich geregelt.

2.2 Recht auf Löschung der betroffenen Person

Bei einem Gesuch auf Löschung sind folgende Punkte zu beachten:

- Die gesuchstellende Person ist zu identifizieren.
- Es ist zu prüfen, ob gesetzliche Aufbewahrungspflichten oder andere zwingende Gründe vorliegen, die gegen eine Löschung bzw. Vernichtung der Daten sprechen. Liegen keine solchen Gründe vor, sind die Personendaten zu löschen bzw. zu vernichten.
- Es ist eine Rückmeldung an die gesuchstellende Person zu erteilen, ob die Daten auf ihr Gesuch hin gelöscht wurden. Wurden ihre Daten nicht gelöscht, so ist ihr dies unter Angabe der Gründe mitzuteilen.

3. Technische Anforderungen an die Löschung

3.1 Definition der Löschung/Vernichtung

Mit dem Begriff der Vernichtung von Daten ist in der Regel die physische Vernichtung von Daten oder die unwiderrufliche Löschung von digitalen Daten gemeint. Während unter der physischen Vernichtung die Zerstörung eines Datenträgers (Papierdokumente, USB-Sticks, CDs etc.) verstanden wird, fällt unter den Begriff der Löschung die Unkenntlichmachung von gespeicherten Daten. Anders als bei der Vernichtung bleibt der Datenträger bei der Löschung erhalten.
Ebenfalls als Unkenntlichmachung von Daten kann grundsätzlich die Verschlüsselung von Daten angesehen werden, wenn die zugehörigen Schlüssel, welche für die Entschlüsselung notwendig sind, entsorgt werden.

3.2 Organisatorisches

Für die fristgerechte Löschung wird die Ausarbeitung eines Vorgehens bzw. Prozesses empfohlen, in welchem definiert wird, was wann und unter welchen Voraussetzungen gelöscht/vernichtet werden muss. Eine Hilfestellung hierfür bietet allenfalls das Verzeichnis der Bearbeitungstätigkeiten, welches eine Übersicht darüber bietet, welche Daten wie lange

aufbewahrt werden müssen (siehe dazu auch die Vorlage Verzeichnis der Bearbeitungstätigkeiten). Sofern ein Rechtfertigungsgrund zur weiteren Aufbewahrung gegeben ist, ist von einer Löschung abzusehen. Ein Rechtfertigungsgrund wäre zum Beispiel die Einwilligung des Patienten für die weitere Aufbewahrung.

3.3 Berücksichtigung Spezialfälle

Personendaten sind unter Berücksichtigung von gesetzlichen Aufbewahrungsfristen und Verjährungsfristen, in der Folge nach Ablauf der spezifischen Frist, unwiderruflich zu löschen bzw. zu vernichten. Daten, welche sich in Archiven, auf Sicherungskopien oder in E-Mails befinden, sind von dieser Regelung nicht ausgenommen. Nachfolgend werden daher zu beachtende Punkte sowie Beispielverfahren als Hilfestellung aufgezeigt.

3.3.1 Archive

Daten bzw. ganze Datenbestände, die langfristig verfügbar sein sollen oder müssen, aber nicht mehr verändert werden müssen, werden häufig in hausinterne Archive verlegt. Sofern kein Rechtfertigungsgrund zur weiteren Aufbewahrung gegeben ist, sind die archivierten Datenbestände gemäss den gesetzlich vorgegebenen Fristen zu vernichten.

Um eine rechtzeitige Vernichtung gewährleisten zu können, empfiehlt es sich beispielsweise, einen Prozess für eine jährliche Aussortierung zu definieren. Werden Datenbestände zudem vor der Verlegung ins Archiv deutlich gekennzeichnet (z. B. Jahr der Verlegung und Aufbewahrungsfrist), erleichtert dies die Aussortierung.

3.3.2 Back-ups

Eine Absicherung /ein Back-up ist zwingend zum Schutz vor Datenverlust zu installieren. Back-ups mit kurzen Sicherungszyklen (z. B. täglich, wöchentlich) werden üblicherweise regelmässig überschrieben. Werden die Originaldaten im Produktivsystem gelöscht, verschwinden diese Daten demnach in den folgenden Back-ups ebenfalls.

In Back-ups mit langen Sicherungszyklen (z. B. monatlich, jährlich) hingegen bleiben diese Daten weiterhin vorhanden. Im Falle einer Wiederherstellung würden diese Daten rekonstruiert, womit die Löschung der Daten rückgängig gemacht wird.

Um sicherzustellen, dass gelöschte Daten auch nach der Wiederherstellung eines Back-ups gelöscht bleiben, empfiehlt es sich, einen Prüfprozess einzurichten. Dabei kann beispielsweise eine Liste geführt werden, auf welcher mit pseudonymisierten Daten (z. B. Patientennummer) festgehalten wird, welche Datensätze gelöscht wurden. Wird ein Back-up wiederhergestellt, kann anhand dieser Liste geprüft werden, ob auch gelöschte Datensätze wiederhergestellt wurden. Ist dies der Fall, können die Daten erneut umgehend aus dem Produktivsystem gelöscht werden. Wird auf der Liste zudem das Datum der ursprünglichen Löschung festgehalten, könnte der Eintrag nach dem letzten langfristigen Back-up wieder entfernt werden.

Zusätzlich zu einem solchen Prüfprozess ist durch technische und organisatorische Massnahmen sicherzustellen, dass auch die Zugriffsrechte auf die wiederhergestellten Daten geprüft werden.

3.3.3 E-Mails

Sofern E-Mails Patientendaten der/des einzelnen Patient:in beinhalten, sind sie in der Patientendokumentation zwingend abzulegen. Wenn die Patientendokumentation gemäss den gesetzlich vorgegebenen Aufbewahrungsfristen gelöscht wird, ist sicherzustellen, dass die damit verbundenen E-Mails ebenso gelöscht werden.

3.4 Sicherheitsanforderungen an die Löschung

Die gewählten Lösch- und Vernichtungsmethoden haben die endgültige Löschung zu gewährleisten. Dies bedeutet, dass eine Methode zu wählen ist, welche die Wiederherstellung der gelöschten Personendaten verunmöglicht. Methoden, bei denen die Wiederherstellung der Personendaten möglich ist, sind nicht datenschutzkonform (z. B. einfache Entsorgung von Personendaten in Abfallsäcken/Müllcontainern oder die virtuelle Verlegung in den Papiereimer auf dem Desktop/in der Cloud).

In der nachfolgenden Tabelle werden mögliche Methoden aufgezeigt, die eine sichere Löschung gewährleisten können. Die Ausführungen basieren dabei insbesondere auch auf einem Merkblatt zur Vernichtung elektronischer Daten[1], welches von der Datenschutzbeauftragten des Kantons Zürichs publiziert wurde.

[1] https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_vernichten_elektronischer_daten.pdf

Art der Vernichtung	Beschreibung	Bewertung
Physische Vernichtung	Mechanische Zerstörung eines Datenträgers (Schreddern, Einschmelzen etc.). Als Datenträger gelten beispielsweise CDs, USB-Sticks, Disks, aber auch Papier etc. ***Hinweis:*** *Werden für die Löschung/Vernichtung externe Dienstleister beigezogen, so ist sicherzustellen, dass der Prozess ausreichend sicher und nachvollziehbar ist und keine Weiterverwendung der Datenträger möglich ist. Der Prozess sollte regelmässig überprüft werden. Die Praxis bleibt in der Verantwortung.*	Die datenschutzkonforme Löschung ist grundsätzlich gewährleistet.
Magnetische Löschung	Spezielle Löschgeräte ermöglichen durch eine spezifische Magnetisierung das Löschen der Informationen ganzer Festplatten, sodass die Reproduktion von Daten unmöglich oder weitgehend erschwert wird. Solche Löschgeräte können selbst bei defekten Festplatten noch wirksam eingesetzt werden. Dieses Verfahren eignet sich für magnetische Datenträger wie Festplatten und Magnetkarten/-bänder (LTO, DLT, DAT, Audiokassetten, Videokassetten).	Die Unwiderruflichkeit der Löschung ist gegeben. Allerdings werden die Datenträger durch den Vorgang funktionsunfähig.
Wipen/technisches Überschreibungen	Einzelne Dateien oder auch ganze wiederbeschreibbare Speichermedien können durch mehrmaliges Überschreiben mit zufälligen Zeichenfolgen (Wipen) nachhaltig gelöscht werden. Dieses Verfahren eignet sich nicht für moderne Systeme mit flüchtigen elektronischen Speichermedien (Solid State Disks, SSD).	Die Unwiderruflichkeit der Vernichtung ist gegeben.
Löschen von Daten auf nicht flüchtigen elektronischen Speichermedien (Solid State Disks)	Meistens sind elektronische Speichermedien mit Löschbefehlen versehen (z.B. ATA Secure Erase). Verfügt das Speichermedium über keinen Löschbefehl, so wird empfohlen, die Daten vorgängig zu verschlüsseln und den Schlüssel zu löschen.	Die Unwiderruflichkeit der Vernichtung ist teilweise gegeben.