Kanton Zürich
Sicherheitsdirektion
Kantonales Sozialamt
Soziale Einrichtungen

Fach- und Qualitätsfragen

18. Juli 2019

Hilfsmittel zur Erstellung von Regelungen zum Datenschutz und zur Aufbewahrung in Sozialen Einrichtungen

Inhalt

Nutzung dieses Dokuments

Dieses Dokument dient als Hilfsmittel zur Erstellung einer eigenen Datenschutzregelung und macht Hinweise zu Aufbewahrungs- und Archivierungsregelungen. Das Dokument erhebt keinen Anspruch auf Vollständigkeit, bzw. Tagesaktualität. Für die Erstellung dieses Dokuments wurden einerseits die gesetzlichen Grundlagen, sowie andererseits weiterführende Merkblätter und Hilfsblätter von Fachstellen sowie auch anderen Kantonen miteinbezogen. Dieses Dokument ersetzt nicht die Pflicht des/r Anwenders/-in (der Einrichtung), sich bezüglich der Datenschutzgesetzgebung laufend auf dem aktuellen Stand zu halten, die Quellen im Original beizuziehen und allfällige neue oder geänderte Anforderungen zu prüfen und zu implementieren. Bei den Erläuterungen handelt es sich teilweise um Kopien aus den beigezogenen Quellen.

Informationen zu den gesetzlichen Grundlagen im Datenschutz[1]

Das Gesetz über die Information und den Datenschutz des Kantons Zürich (IDG, LS 170.4) gilt für die öffentlichen Organe (§ 2 Abs. 1 IDG). Organisationen und Personen des öffentlichen und privaten Rechts gelten als öffentliche Organe, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind (§ 3 lit. c IDG). Bei den Einrichtungen im Kanton Zürich handelt es sich gestützt auf Art. 2 des Bundesgesetzes über die Institutionen zur Förderung der Eingliederung von invaliden Personen (IFEG, SR 831.26) um eine öffentliche Aufgabe.

Somit gelten für die Einrichtungen das IDG und das IDV (Verordnung über die Information und den Datenschutz).

[1] Quelle: Abklärung beim Datenschutzbeauftragten des Kantons Zürich, 14. Juni 2019

1 Regelungsbereiche Datenschutz

1.1 Zugriff auf physische und elektronische Daten in der Einrichtung

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Zugriffskontrolle auf physische und elektronische Daten	**Generelle Schutzmassnahmen** Informationen (alle Aufzeichnungen mit Ausnahme nicht fertig gestellter Aufzeichnungen oder persönlicher Notizen) sind durch angemessene organisatorische und technische Massnahmen zu schützen. Die Massnahmen richten sich nach den folgenden Schutzzielen: a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen, b. Informationen müssen richtig und vollständig sein, c. Informationen müssen bei Bedarf vorhanden sein, d. Informationsbearbeitungen müssen einer Person zugerechnet werden können, e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein. Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.	IDG (2007), §7
	Bearbeitung von Personendaten Personendaten dürfen bearbeitet werden, soweit dies zur Erfüllung der gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist. Dies bedeutet, dass nur diejenige Abteilung, bzw. dasjenige Personal der Einrichtung, das eine gesetzlich umschriebene Aufgabe erfüllen muss, die jeweiligen Personendaten bearbeiten darf. Bearbeiten bedeutet nicht nur aktives Bearbeiten, sondern umfasst bereits schon eine Einsichtnahme in die Personendaten. Daran ändert auch eine Regelung der Schweigepflicht der Angestellten nichts.	IDG (2007), §8

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Zugriffskontrolle auf physische und elektronische Daten	**Schutz von Personendaten** Die Einrichtungen sind gesetzlich verpflichtet, die Informationen durch angemessene organisatorische und technische Massnahmen zu schützen (§ 7 IDG). Insbesondere soll dabei das Schutzziel, dass die Informationen nicht unrechtmässig zur Kenntnis gelangen, erfüllt werden. Um die Informationen vor unberechtigten Dritten zu schützen, wäre es am einfachsten, dies über entsprechende Zugriffsberechtigungen zu regeln. Datenbearbeitungssysteme und -programme sind so zu gestalten, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind. Grundsätzlich sollten nur diejenigen Personen Zugriff auf Personendaten haben, welche diese unmittelbar für die Ausführung ihrer Tätigkeit benötigen. Die Zugriffe auf Ordner, Klienteninformationssysteme, Emails sowie die Einsicht auf Bildschirme etc., sind entsprechend zu gestalten. Die Benutzer/-innen sollten über eine individuelle Authentifizierung (Benutzername, Passwort) verfügen und Passwörter sollten stark sein (mind. 8 Zeichen, davon grosse und kleine Buchstaben, Ziffern, Sonderzeichen). Zudem müssen die Daten gegen jeglichen Zugriff von aussen geschützt werden.	IDG (2007), §7 & §11 LF EDÖB (2015), Kap. A.3 Sicherheit des Arbeitsplatzes und Kap. A.4 Identifizierung und Authentifizierung
Zutritt zu Serverräumen	Es ist festzulegen, wer Zutritt zu diesen Räumen haben soll (generell je weniger Personen, desto besser die Sicherheit). Absichtliche oder unabsichtliche Manipulationen am Server, die zur Vernichtung oder Veränderung der Daten führen könnten, müssen verhindert werden. Deshalb sind zur Sicherung der Serverräume besondere Massnahmen zu treffen.	LF EDÖB (2015), Kap. A.2
Sichere Website	Beim Betrieb einer Website sind auch rechtliche Voraussetzungen zu beachten. Ein unsachgemässer Aufbau oder Betrieb einer Website kann zu Verletzungen von Datenschutz- oder Geheimhaltungsvorschriften führen.	dsb Sichere Website (2019)

1.2 Daten ausserhalb der Einrichtung: Versand und Homeoffice

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Datenschutz beim Versand von sensitiven Daten	Der Datenschutz ist beim Versand von sensitiven Daten durch geeignete Massnahmen sicherzustellen. Dies ist entweder mit einer Verschlüsselung, z.B. mittels HIN, oder mit einer Verschlüsselung des Anhangs (verschlüsselte Microsoft-Office-Datei, verschlüsseltes PDF, verschlüsselte Zip-Datei) zu gewährleisten. Eine weitere Möglichkeit besteht darin, dass Emails mit sensitiven Inhalten ohne Namen und Angaben versendet werden, so dass sichergestellt wird, dass es keine eindeutigen Rückschlüsse auf eine Person geben kann (d.h. keine AHV-Nummern, aber auch keine Initialen, die mit weiteren Angaben kombiniert werden und eindeutige Rückschlüsse auf eine Person zulassen können).	MB Sichere E-Mails (2018)

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Datenschutz bei Homeoffice	Wenn Akten zu Hause bearbeitet werden, gelten die analogen Regelungen wie bei der Datenbearbeitung in der Einrichtung (d.h. Daten und Informationen dürfen auch anderen Personen im Haushalt nicht zugänglich sein). Bei externem Datenzugriff ist u.a. der geschützte, bzw. verschlüsselte Datentransfer zu regeln. Daten und Dokumente sind vor unberechtigtem Zugriff Dritter sowie vor Diebstahl zu schützen. Daten und Dokumente müssen, wenn diese nicht mehr benötigt werden, vom Heimarbeitsplatz entfernt werden.	MB Homeoffice (2017) IDG (2007), §7
Datenschutz bei Zugriff von aussen	Wenn Personen von ausserhalb der Einrichtung auf Daten zugreifen sollen, so muss ein geschützter Zugang eingerichtet werden und die Person muss sich klar authentifizieren können. Es muss z.B. mittels Zugangscodes, Token, Badge etc. sichergestellt sein, dass es sich um eine berechtigte Person handelt. Auch persönliche Computer sind dabei auf den aktuellen Stand bezüglich Virenschutz und Firewall zu bringen.	LF EDÖB (2015), Kap. A.6 Zugang von ausserhalb der Organisation

1.3 Entbindung Schweigepflicht und Auskunftsrecht

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Entbindung der Schweigepflicht	Damit sich niemand strafbar macht, der Personendaten weitergibt, ist die Entbindung der Schweigepflicht klar zu regeln. Schweigepflichtentbindungen sollten bei Eintritt von Klienten/-innen so verfasst werden, dass der gezielte, ausschliesslich berufsbezogene Informationsaustausch zwischen allen relevanten Aussenstellen (Hausärzt/-in, Psychiater/-in, Zahnärzt/-in, Gynäkolog/-in, Angehörige, ehemaliger/zukünftiger Wohn-/Arbeitsort, etc.) sowie den internen Bezugspersonen geregelt wird. Im IDG ist geregelt, dass Personendaten bekannt gegeben werden dürfen, wenn: a) eine rechtliche Bestimmung dazu ermächtigt, b) die betroffene Person im Einzelfall eingewilligt hat oder c) es im Einzelfall zur Abwendung einer drohenden Gefahr für Leib und Leben unentbehrlich oder der notwendige Schutz anderer wesentlicher Rechtsgüter höher zu gewichten ist. Im Leitfaden «Datenschutz im Sozialbereich» wird dies auf Seite 5 ausgeführt: «Eine Einwilligung ist nur gültig, wenn die betroffene Person freiwillig und nach ausreichender Information über die Informationsflüsse und die Folgen der Bekanntgabe eingewilligt hat. Die Einwilligung hat sich sowohl auf eine bestimmte Drittperson, auf eine andere Behörde oder Fachstelle als Empfänger der Personendaten als auch auf einen klaren Gegenstand zu beschränken. Für die Bekanntgabe besonderer Personendaten ist eine ausdrückliche Einwilligung erforderlich (§ 17 Abs.1, lit. b IDG). Sie ist durch die betroffene Person schriftlich zu erteilen und von der Behörde oder Fachstelle in den Akten abzulegen. Die betroffene Person kann ihre Einwilligung grundsätzlich jederzeit widerrufen.»	IDG (2007), §16 LF DS Soz (2017) IDG (2007), §17

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Unterschriften auf der Entbindung	**Urteilsfähige und nichturteilsfähige Personen**[2] Einer urteilsunfähigen Person ist es generell nicht möglich, rechtliche Wirkungen zu erzeugen. Somit hat bei Urteilsunfähigkeit immer die gesetzliche Vertretung eine Schweigepflichtentbindung zu unterzeichnen (siehe auch Art. 378 ZGB). Urteilsfähige, verbeiständete Personen sind jedoch berechtigt, selbständig und ohne Zustimmung des gesetzlichen Vertreters eine Einwilligung zu erteilen, da es sich hierbei um ein höchstpersönliches Recht handelt. Ob es in Fällen mit Verbeiständung einer urteilsfähigen Person allenfalls noch zusätzlich der Unterschrift einer gesetzlichen Vertretung bedarf (Art von Beistandschaft), wäre im Detail mit der KESB zu klären.	ZGB, Art. 378
Persönlichkeitsschutz	Das Persönlichkeitsrecht der Personen ist zu schützen und zu gewährleisten. Dieser Schutz ist insbesondere auch bei der Informationsweitergabe an Aussenstellen, z.B. im Austausch mit Angehörigen, wahrzunehmen.	ZGB, Art. 28

1.4 Einsichtsrecht und Recht am Bild

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Gewährung Einsichtsrecht	Das Recht auf Einsicht in eigene Personendaten kann gestützt auf § 20 Abs. 2 IDG geltend gemacht werden. Dieses Recht umfasst die Einsicht in alle die eigene Person betreffenden Angaben. Für die Geltendmachung ist kein Interessennachweis erforderlich – das Recht besteht voraussetzungslos. Die Auskunft wird in der Regel in Form von kostenlosen (§ 29 Abs. 2 lit. b IDG) Kopien erteilt – mit dem Einverständnis der um Auskunft ersuchenden Person ist auch eine Einsichtnahme vor Ort zulässig (§ 18 Abs. 1 IDV). Häufig wird hierbei so vorgegangen, dass die um Auskunft ersuchende Person das Dossier zunächst sichtet und dann nur von den wichtigsten Unterlagen Kopien erstellen lässt. **Anmerkungen zum Einsichtsrecht:** In der Broschüre "Datenschutz – Meine Rechte" finden sich hilfreiche Ausführungen im Zusammenhang mit der Gewährung des Einsichtsrechts.	IDG (2007), § 20 & 29 IDV (2008), § 18 Datenschutz – Meine Rechte (2014)

[2] Quelle: Abklärung beim Datenschutzbeauftragten des Kantons Zürich, 14. Juni 2019

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Das Recht am eigenen Bild	Es muss zwischen dem Fotografieren/Filmen selbst und dem Veröffentlichen unterschieden werden. Beides bedarf einer Einwilligung. Fotos dürfen nur mit der Einwilligung von Betroffenen, respektive je nach Beistandschaft mit der Einwilligung der gesetzlichen Vertretungen, aufgenommen und veröffentlicht werden. Es gilt das Recht am eigenen Bild. Bei Urteilsunfähigen wird gänzlich von Bild- und Tonaufnahmen abgeraten, die es nicht zur Erfüllung des gesetzlichen Auftrages benötigt. Ausnahmen gelten für das Fotografieren an öffentlichen Anlässen. Dort bedarf es keiner Einwilligung, denn wer sich in der Öffentlichkeit aufhält, muss in Kauf nehmen, auf einem Bild als eine unter mehreren Personen fotografiert zu werden. Für die Veröffentlichung dieser Bilder wiederum muss jedoch eine Einwilligung eingeholt werden. Zudem gilt, dass grundsätzlich auf die Veröffentlichung von Porträtaufnahmen zu verzichten ist. Die Betroffenen müssen die Möglichkeit haben, die zur Publikation vorgesehenen Bilder einzusehen. Gemäss Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) müssen sie über den Kontext der Veröffentlichung informiert werden. Eine pauschale Einwilligung zur Veröffentlichung von Bildern ist deshalb nicht ausreichend.	Abklärung beim Datenschutzbeauftragten des Kantons Zürich, 14. Juni 2019 Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/veroeffentlichung-von-fotos.html
Umgang mit Bild- und Tonaufnahmegeräten	Für die Benutzung von privaten sowie institutionellen Bild- oder Tonaufnahmegeräten (z.B. Smartphones, Kameras, etc.) während der Tätigkeit, bzw. des Aufenthaltes, sollten Guidelines für das Personal sowie die Klienten/-innen erstellt werden.	Empfehlung des Kantonalen Sozialamtes Zürich
Rückzug der Einwilligung	Gemäss EDÖB kann eine einmal erteilte Einwilligung grundsätzlich jederzeit zurückgezogen werden, mit dem Resultat, dass auch die Veröffentlichung, soweit überhaupt möglich, rückgängig gemacht werden muss. Verursacht ein solcher Rückzug einen Schaden (z. B. wenn bereits gedruckte Werbeprospekte nicht mehr verwendet werden können), kann die zurückziehende Person allenfalls dazu verpflichtet werden, diesen Schaden (teilweise) zu übernehmen. Personen, deren Bilder ohne Rechtfertigung veröffentlicht wurden, können sich jederzeit gegen die Veröffentlichung wehren und ihre Ansprüche nötigenfalls mittels Zivilklage geltend machen.	Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/veroeffentlichung-von-fotos.html

1.5 Sicherheit der Datenträger und Datensicherung

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Vorgehen bei der Verschlüsselung von Datenträgern	Daten werden nicht nur auf zentralen Servern und PCs gespeichert, sondern auch auf zahlreichen externen Speichermedien (USB-Sticks, externe Festplatten, CD-ROM oder weitere Geräte). Es passen immer mehr Daten auf immer kleinere Datenträger. Sicherzustellen sind folgende Themenbereiche: – Die Angestellten kennen die Gefahren, die das Anschliessen eines unbekannten externen Datenträgers an ihren PC mit sich bringen kann. – Es ist sichergestellt, dass externe Datenträger, die besonders schützenswerte („sensible“) Personendaten oder Persönlichkeitsprofile enthalten, verschlüsselt werden. – Die externen Datenträger werden unter Verschluss aufbewahrt. – Ein Verfahren zur Vernichtung der Datenträger wird eingerichtet. Die dazu notwendigen Instrumente stehen zur Verfügung.	LF EDÖB (2015), Kap. B.5
	Zu Verschlüsselungen steht im LF EDÖB (Kap. B.4): Der Verschlüsselungsalgorithmus und insbesondere die Länge des Schlüssels sind proportional zur Sensibilität der Daten. Die Verschlüsselungsschlüssel werden gesichert. Nur eine begrenzte Anzahl Personen hat Zugang zu den Schlüsseln.	LF EDÖB (2015), Kap. B.4
Nutzung des Internets	Der Umgang mit dem Internet (z.B. Zugriff auf Seiten, Download, etc.) sollte für das Personal und die Klienten/-innen (sofern sie über den Anschluss/Server der Institution Zugriff aufs Internet haben) festgelegt werden. Auch gibt es vom Eidgenössischen Datenschutzbeauftragten Hilfestellungen zu diversen Themen wie z.B.: Internetpranger: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/internetpranger.html Webtracking: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/webtracking.html	Empfehlung des Kantonalen Sozialamtes Zürich
Datensicherung	Die Integrität und Verfügbarkeit der Daten eines Systems müssen gesichert sein. Darum ist ein Datensicherungsverfahren festzulegen. Aus Datenschutzperspektive ist hierbei primär der Schutz vor unberechtigtem Zugriff relevant. Werden im Falle einer Fehlmanipulation oder einer missbräuchlichen Bearbeitung Daten vernichtet oder beschädigt, muss geregelt sein, wie diese Daten wiederhergestellt werden können. Hierfür ist gemäss unter anderem eine Sicherungsstrategie notwendig. Anmerkung: Damit die Daten für die Einrichtung jedoch auch im Ausnahmefall zugänglich sind, ist auch ein funktionierendes Backup-System erforderlich.	LF EDÖB (2015), Kap. B.6

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Benutzung von Smartphones	Bei der Benutzung betrieblicher Smartphones sind die Datenschutzregelungen zu berücksichtigen. Der Datenschutzbeauftragte des Kantons Zürich hat zwei Hilfestellungen zum Datenschutz im Umgang mit Smartphones herausgegeben, welche auf verschiedene Fragestellungen eingehen (z.B. Lokalisieren des Smartphones, Verhindern von unerwünschten App-Zugriffen, Sicheres Löschen, Datenschutzfreundliche Nutzung von Karten, Sichere Online-Speicherung, Zusätzlicher Zugriffschutz für Daten und Apps, Sicheres Speichern der Passwörter, Schutz vor Trojanern und Spyware, Sicheres Kommunizieren, Verschlüsselung von Dateien).	MB Datenschutzfreundliche Apps (2018) MB Smartphone-Sicherheit – 7 goldene Regeln

1.6 Auslagerung von Arbeiten und Nutzung von Clouds

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Auslagerung von Arbeiten	Wenn Arbeiten ausgelagert werden, sind Massnahmen zu ergreifen, damit auch bei der auswärtigen Lagerung und Bearbeitung dieser Daten die Datenschutzgesetzgebung eingehalten wird. Dies bedeutet., dass die Einhaltung der Datenschutzregelungen vertraglich geregelt wird und insbesondere auch die Übermittlung von Daten gesichert ist. Der Datenschutzbeauftragte vom Kanton Zürich hat einen Leitfaden zum «Bearbeiten im Auftrag» herausgegeben, der diese Punkte detailliert regelt und auch eine Checkliste bereitgestellt, welche Punkte vertraglich zu regeln sind.	LF EDÖB (2015) Kap. B.8 MB Bearbeiten im Auftrag (2018)
Cloudcomputing	Gemäss Merkblatt Cloud Computing ist die Inanspruchnahme von Cloud Services ein «Bearbeiten im Auftrag» gemäss § 6 IDG. Der Auftraggeber verbleibt gemäss IDG für den Umgang mit Informationen verantwortlich. Es ist deshalb detailliert und schriftlich in einem Vertrag festzuhalten, wer wofür im Sinne des IDG verantwortlich ist (siehe Leitfaden «Bearbeiten im Auftrag» Kap. 7 «Checkliste Vorgehen» und Kap. 8 «Überblick AGB und Vertragsbestimmungen»).	IDG (2007), § 6 MB Cloud Computing (2017) MB Bearbeiten im Auftrag (2018)
Nutzung von Cloud-basierten Online-Speicherdiensten	Gemäss Merkblatt Online-Speicherdienste (2018) ist «die Nutzung von Cloud-basierten Online-Speicherdiensten, wie zum Beispiel Dropbox, Team-Drive, Microsoft OneDrive oder Google Drive einfach, führt aber zu erhöhten Risiken betreffend Verletzungen der datenschutzrechtlichen Rahmenbedingungen und damit zusammenhängend der Persönlichkeitsrechte». Bei der Speicherung der Daten in der Cloud ergeben sich gemäss Merkblatt Online-Speicherdienste (2018) folgende Risiken: – Datenverlust – Verlust der Verfügbarkeit, der Vertraulichkeit und der Integrität – Nichtdurchsetzbarkeit des Löschens – Unsichere Clientsoftware	MB Online-Speicherdienste (2018)

2 Regelungsbereiche Aufbewahrung und Archivierung

2.1 Grundlagen Aufbewahrung und Archivierung[3]

Themenbereich	Erläuterungen
Lebenszyklen der Ablage	Die Aufbewahrung/Archivierung lässt sich in drei Hauptphasen (Lebenszyklen) unterteilen: – die laufende Ablage, – die ruhende Ablage und – das Archiv. Die Prinzipien Rechenschaftsfähigkeit und Nachvollziehbarkeit ziehen sich durch den ganzen Lebenszyklus der Verwaltungsunterlagen. Die Vorgaben zur Ablage/Archivierung sollten schriftlich festgehalten sein (z.B. Weisung zur Informationsverwaltung inkl. Aktenplan), so dass eindeutig ist, wer, wann, wie und wo für die Archivierung zuständig ist (inkl. Zuständigkeit betreffend Vernichtung nach Ablauf der Aufbewahrungsfrist).
Laufende Ablage	Während der Dauer der Aufgabenerfüllung werden die Dossiers in einer laufenden Ablage aufbewahrt. Es empfiehlt sich, Eintrittsdossiers von Klienten/-innen und dem Personal zentral abzulegen, anstatt es in verschiedenen Bereichen einer Institution aufzubewahren. Dies unterstützt die gezielte Archivierung zu einem späteren Zeitpunkt.
Ruhende Ablage	Ist ein Geschäftsfall abgeschlossen, wird das Falldossier als erledigt abgeschrieben; das Dossier geht in eine ruhende Ablage. Der Zweck dieser Aufbewahrung ist nicht mehr der Ursprüngliche (gesetzliche Aufgabenerfüllung), hängt aber mit diesem eng zusammen. Zweck der ruhenden Ablage ist die Aufbewahrung zu Beweiszwecken bei späteren Streitfragen oder zum erneuten Beizug des Dossiers, wenn innert der Aufbewahrungsfrist ein Geschäftsfall auftritt, der mit dem Vorherigen zusammenhängt. Beim Übergang in die ruhende Ablage sollten alle Unterlagen vernichtet werden, die für den Fall nicht mehr relevant sind, zum Beispiel Handnotizen, Kopien und Mehrfachexemplare, Entwürfe, Versandlisten usw.
Archivierung	Mit der Archivierung findet eine Zweckänderung statt: Die Dossiers werden nicht mehr zum Zweck der Aufgabenerfüllung des öffentlichen Organs, sondern zum Zweck der historischen Überlieferung aufbewahrt. Werden Aktenbestände in das Archiv übernommen, sind die Informationen und Nachweise dem ursprünglichen Organ entzogen.
Aufbewahrungs-frist	Informationen sind solange aufzubewahren, als für die Arbeit regelmässig darauf zurückgegriffen werden muss. Hierzu sollte ein «Aktenplan" erstellt werden. Die Akten werden während einer im Aktenplan festgelegten Aufbewahrungsfrist aufbewahrt. Gibt es keine spezialgesetzliche Aufbewahrungsfrist, gilt die im IDG und Archivgesetz geregelte maximale Aufbewahrungsdauer von 10 Jahren (§ 5 Abs. 2 IDG, § 8 Abs. 1 Archivgesetz, LS 170.6). Diese Frist läuft ab dem Zeitpunkt, in welchem das Dossier geschlossen wird und gilt für physische sowie digitale Akten.

[3] MB Informationsverwaltung (2017)

Themenbereich	Erläuterungen
Aufbewahrungs-ort	Die Dossiers sind so aufzubewahren, dass Unberechtigte keine Kenntnis davon erlangen. Die in den Unterlagen enthaltenen Personendaten müssen in angemessener Weise geschützt werden. Die Schutzvorkehrungen sind abhängig von der Wahl des Mediums. Bei der elektronischen Datenaufbewahrung empfehlen sich beispielsweise folgende Sicherheitsmassnahmen: – Verschlüsselung von sensiblen Informationen mit Hardwarekomponenten oder Software – Regelmässige Absicherung der Daten durch Sicherungskopien (Back-ups) – Automatische Protokollierung der Veränderung von Informationen. Nach Ablauf der Aufbewahrungsfrist müssen die Akten dem zuständigen Archiv angeboten werden. Dieses entscheidet, welche Akten übernommen werden. Massgebend für die Archivwürdigkeit von Informationen sind rechtliche, kulturelle und wissenschaftliche Kriterien. Informationen, die nicht archiviert werden, sind sicher zu vernichten (§ 5 Abs. 3 IDG). Stellen Sie sicher, dass keine physischen sowie digitalen Schattendossiers existieren und alle Dokumente gesamthaft archiviert werden, bzw. vernichtet werden.

2.2 Aufbewahrung von Personaldossiers

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Aufbewahrung der Personaldossiers	Nach Erstellung einer Personalakte obliegt dem/der Arbeitgeber/-in eine Aufbewahrungspflicht, welche, je nach Personalakte und Erstellungsdatum, unterschiedlich ist, maximal jedoch 10 Jahre nach Austritt beträgt. **Allgemeine Bemerkungen** Das Personaldossier umfasst in der Regel Angaben zu Personalien, Bewerbungsunterlagen, Referenzauskünfte, Assessmentunterlagen oder Gutachten, Arbeitsvertrag und Vertragsanpassungen, Angaben über Absenzen und Ferien, Lohn- und Versicherungsdaten, Qualifikationen, besuchte Weiterbildungen, Verwarnungen, Aktennotizen über besondere Vorkommnisse, Arztzeugnisse sowie die Korrespondenzen zwischen Arbeitnehmer/-in und Arbeitgeber/-in. Die Daten des Personaldossiers dürfen nur durch das Personalwesen bearbeitet werden und nur jenen Personen zugänglich sein, die sie für die Ausführung ihrer Tätigkeit benötigen. Es darf keine geheime Aktenführung, z.B. in Form von «Schattendossiers» erstellt werden. **Daten zur Erstellung eines Arbeitszeugnisses** Die zehnjährige Verjährungsfrist von Art. 127 OR gilt nach vorherrschender Auffassung u. a. auch für den Anspruch auf Erstellung, Begründung, Korrektur oder Ergänzung eines Arbeitszeugnisses. Diese Ansprüche können bis zehn Jahre nach Beendigung des Arbeitsverhältnisses geltend gemacht werden. Von der Aufbewahrungspflicht betroffen sind in erster Linie Angaben über Art und Dauer des Arbeitsverhältnisses, zur Aufgabenbeschreibung und zum Verantwortungsbereich, Beurteilungen von Leistung, Verhalten und Führung, Laufbahn und Weiterbildung, Angaben zum Austrittsgrund aber auch über besondere Vorkommnisse. Relevant für die Erstellung eines Arbeitszeugnisses sind in der Regel nur die letzten zwei Mitarbeiterbeurteilungen. Im Hinblick auf hängige Rechtsstreitigkeiten werden bis zu deren Beendigung jene Akten aufbewahrt, die als Beweismittel benötigt werden. Wenn z.B. Angestellte knapp vor Ablauf der zehnjährigen Verjährungsdauer Ansprüche geltend machen, so dürfen die benötigten Beweismittel bis zur Beendigung der Rechtstreitigkeit, d.h. bis zum Ablauf der entsprechenden Rekursfristen, aufbewahrt werden. Die Aufbewahrungsdauer der benötigten Beweismittel kann sich in solchen Fällen bis über die zehnjährige Aufbewahrungspflicht erstrecken. **Akten, die den Angestellten gehören** Bewerbungsunterlagen wie z.B. Lebenslauf, frühere Arbeitszeugnisse, Ausbildungsdiplome, Arbeitsproben, Fotos und ähnliche Akten, die den Angestellten gehören und an denen der Arbeitgeber kein berechtigtes Interesse mehr hat, müssen diesen spätestens bei Beendigung des Arbeitsverhältnisses zurückgegeben werden. In der Regel sollte dies jedoch bereits nach Ablauf der Probezeit geschehen.	ABH (2017) OR Art. 127 Art. 330a OR Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/9--taetigkeitsbericht-2001-2002/aufbewahrung-des-personaldossiers.html

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Aufbewahrung der Personaldossiers	**Akten, die dem/der Arbeitgeber/-in gehören** Akten, die dem/der Arbeitgeber/-in gehören, an denen er/sie aber kein berechtigtes Interesse mehr hat, müssen spätestens bei Beendigung des Arbeitsverhältnisses vernichtet werden. Der/die Arbeitgeber/-in kann solche Dokumente auch den Angestellten aushändigen. Es geht hier insbesondere um frühere Qualifikationsunterlagen, die für die Erstellung und Begründung eines Arbeitszeugnisses nicht mehr benötigt werden, aber auch um graphologische, psychologische oder medizinische Gutachten sowie um Persönlichkeitstests. Solche Dokumente sollten in der Regel bereits eins bis zwei Jahre nach Erstellung vernichtet, bzw. zurückgegeben werden.	Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/9--taetigkeitsbericht-2001-2002/aufbewahrung-des-personaldossiers.html

2.3 Aufbewahrung der Klienten/-innen-Dossiers

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Aufbewahrung der Dossiers der Klienten/-innen	Folgende Akten über Nutzende (Klienten/-innen) sind 10 Jahre (ab Austritt) aufzubewahren: – Anmeldeformular, Aufenthaltsvertrag – Medizinische Akten (die Aufbewahrungsfrist beginnt bei Behandlungsabschluss) – Bewohner/innendokumentation (Förder- bzw. Begleitplanung) – Journaleinträge[4] – Protokolle von Standortgesprächen – Dokumentation der zielorientierten, agogischen Planung – Akten über besondere Ereignisse (z.B. Grenzverletzungen, Unfall) – Dokumentation von freiheitseinschränkenden Massnahmen – Kündigungsschreiben und Austrittsbericht	ABH (2017)

[4] Anmerkung: Die Einrichtung hat sicherzustellen, dass Journale so erstellt sind, dass eine sichere Aufbewahrung nach Austritt und eine anschliessende Archivierung, bzw. Vernichtung der Daten, gewährleistet ist.

2.4 Entsorgung von Personendaten nach der Aufbewahrungsdauer

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Vernichtung von physischen und elektronischen Daten	Mechanismen zur endgültigen Vernichtung (besonders) schützenswerter Daten müssen vorgesehen werden. Daten auf Papier sollten mit dem Aktenvernichter (oder einer gleichwertigen Methode) vernichtet werden. Die Daten auf der Festplatte zu löschen, reicht nicht aus; sie dürfen nie mehr zugänglich sein. Der Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes empfiehlt, CD-ROM und andere mobile Datenträger physisch zu vernichten und empfiehlt auch den Umgang bezüglich Vernichtung von Sicherungskopien zu regeln.	LF EDÖB (2015), Kap. B.7

2.5 Aufbewahrung von Akten der Einrichtung

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Allgemeine Akten der Einrichtung	Für folgende Unterlagen ist eine Aufbewahrung von 10 Jahren (nach Ablauf des Geschäftsjahrs/nach Geschäftsabschluss) festgehalten: – strategische Unterlagen (Leitbild, Betriebskonzept etc.) – Leistungsvereinbarungen – interne und externe Auditberichte – Protokolle von Heimleitungssitzungen (sofern keine sensitiven Informationen über Personen aufgeführt sind) – Personalbefragungen – Weitere geschäftsrelevante Unterlagen Für allgemeine Kontrollblätter (z.B. Temperaturkontrollen, Apothekenkontrollen, etc.), für die keine gesetzliche Aufbewahrungsfrist existiert, ist zu überlegen, welches der maximale Kontrollrhythmus einer externen Kontrolle ist und wie hoch das Risiko ist, wenn dieser Nachweis nicht mehr vorhanden wäre. Anhand dieser Überlegungen ist eine sinnstiftende Aufbewahrungszeit festzulegen.	ABH (2017)

2.6 Aufbewahrung von Akten der Buchhaltung

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Aufbewahrung der Buchhaltungsunterlagen	Für folgende Unterlagen gilt eine Aufbewahrung von 10 Jahren (nach Ablauf des Geschäftsjahrs): – Akten der Buchhaltung – Jahresrechnung – Bilanz – Revisionsberichte – Kostenrechnungen – Jahresbericht – Geschäftsbücher – Buchungsbelege – Quittungen, Garantiescheine – Bank- und Postunterlagen – Steuerunterlagen – Spendenunterlagen	ABH (2017)

2.7 Aufbewahrung von Akten der Trägerschaft

Zu regeln sind:	Erläuterungen	Verweise/Hilfsmittel
Aufbewahrung der Akten der Trägerschaft	Für folgende Unterlagen ist eine Aufbewahrung von 10 Jahren festgehalten: – Akten der Trägerschaft (nach Ablauf des Geschäftsjahrs) – Beschlüsse – Protokolle	ABH (2017)
Ewige Aufbewahrung	Für folgende Akten wird eine Aufbewahrung ohne zeitliche Befristung empfohlen: – wichtige Verträge – Unterlagen zu Liegenschaften (inkl. Bauvorhaben) – historisch interessante Dokumente über die Einrichtung	ABH (2017)
Auflösen einer Trägerschaft oder Einrichtung	Bei der Auflösung einer Trägerschaft oder Einrichtung ist mit dem Staatsarchiv Kontakt aufzunehmen, um die Anforderungen zur Aufbewahrung der Akten zu erfahren.	

3 Ausgewählte Begriffsdefinitionen

Themenbereich	Erläuterungen
Daten-/Informationssicherheit	Die Daten-/Informationssicherheit umfasst alle Massnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten/Informationen.
Datenschutz	Der Datenschutz umfasst alle Massnahmen zur Verhinderung einer unerwünschten Bearbeitung von Personendaten und deren Folgen.
Informationsschutz	Der Informationsschutz legt, im Hinblick auf die Wahrung der Interessen eines Landes oder einer Organisation, die Vertraulichkeitsstufen für Informationen (INTERN, VERTRAULICH, GEHEIM) fest.
Personendaten (IDG Art. 3)	Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen.
Besondere Personendaten (IDG Art. 3)	Besondere Personendaten: Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, wie Informationen über 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, 2. die Gesundheit, die Intimsphäre, die Rassenzugehörigkeit oder die ethnische Herkunft, 3. Massnahmen der sozialen Hilfe, 4. administrative oder strafrechtliche Verfolgungen oder Sanktionen.
Risikostufen bei Personendaten (Quelle: LF EDÖB 2015)	1. Geringes Risiko: Personendaten, deren Missbrauch in der Regel für die betroffene Person keine besonderen Folgen hat, beispielsweise Name, Vorname, Adresse und Geburtsdatum oder Informationen, die in den Medien erschienen sind, soweit sie nicht in einem sensiblen Zusammenhang stehen. 2. Mittleres Risiko: Personendaten, deren Missbrauch die wirtschaftliche Situation oder die gesellschaftliche Stellung der betroffenen Person beeinträchtigen kann. Dazu gehören beispielsweise Angaben über eine Mieterin oder einen Mieter oder über die beruflichen Verhältnisse einer Person. 3. Hohes Risiko: Personendaten, deren Missbrauch zu einer schweren Beeinträchtigung der wirtschaftlichen Situation oder der gesellschaftlichen Stellung führen kann. Dazu gehören Daten zur Gesundheit, besonders schützenswerte („sensible“) Personendaten und Persönlichkeitsprofile. 4. Sehr hohes Risiko: Personendaten, deren Missbrauch das Leben der betroffenen Person gefährden kann. Dazu gehören Adressen von V-Leuten der Polizei, von Zeuginnen und Zeugen in bestimmten Strafverfahren oder von Personen, die aufgrund ihrer Gesinnung oder ihrer religiösen oder politischen Zugehörigkeit bedroht sind.
Datensammlung	Nach schweizerischem Recht ist eine Datensammlung jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.

4 Verzeichnis der Quellen

Gesetze

IDG (2007)	Gesetz über die Information und den Datenschutz (IDG), Kanton Zürich, Stand 12.02.2007 https://www.zh.ch/internet/de/rechtliche_grundlagen/gesetze/erlass.html?Open&Ordnr=170.4
IDV (2008)	Verordnung über die Information und den Datenschutz (IDV), Kanton Zürich, Stand 28.05.2008 (https://www.zh.ch/internet/de/rechtliche_grundlagen/gesetze/erlass.html?Open&Ordnr=170.41)
ZGB (2019)	Schweizerisches Zivilgesetzbuch (ZGB), Stand 1. Januar 2019, (https://www.admin.ch/opc/de/classified-compilation/19070042/index.html)
ArchivG (1995)	Archivgesetz (ArchivG), Kanton Zürich, Stand 24.09.1995 (https://www.zh.ch/internet/de/rechtliche_grundlagen/gesetze/erlass.html?Open&Ordnr=170.6)
ArchivV (1998)	Archivverordnung (ArchivV), Kanton Zürich, Stand 09.12.1998 (https://www.zh.ch/internet/de/rechtliche_grundlagen/gesetze/erlass.html?Open&Ordnr=170.61)

Leitfaden und Merkblätter

LF EDÖB (2015)	Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, Eidg. Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), August 2015, Quelle (Stand 25.03.2019): https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2016/03/leitfaden_zu_dentechnischenundorganisatorischenmassnahmendesdate.pdf.download.pdf/leitfaden_zu_dentechnischenundorganisatorischenmassnahmendesdate.pdf https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/veroeffentlichung-von-fotos.html (Stand 25.03.2019
LF DS Soz (2017)	dsb Leitfaden Datenschutz im Sozialbereich, Datenschutzbeauftragter Kanton Zürich, Oktober 2017, Quelle (Stand 25.03.2019): https://dsb.zh.ch/internet/datenschutzbeauftragter/de/publikationen/anleitungen/_jcr_content/contentPar/form_1/formitems/datenschutz_im_sozia/download.spooler.download.1510747708773.pdf/Leitfaden_Datenschutz_im_Sozialbereich.pdf
Cloud Computing (2017)	dsb Merkblatt Cloud Computing, Datenschutzbeauftragter Kanton Zürich, Oktober 2017, Quelle (Stand 25.03.2019): https://dsb.zh.ch/dam/dsb/publikationen/formulare_und_merkblaetter/Merkblatt_Cloud_Computing.pdf
Online-Speicherdienste (2018)	dsb Merkblatt Online-Speicherdienste, Datenschutzbeauftragter Kanton Zürich, Juli 2018, Quelle (Stand 25.03.2019): https://dsb.zh.ch/dam/dsb/publikationen/formulare_und_merkblaetter/Merkblatt_Online_Speicherdienste.pdf
Bearbeiten im Auftrag (2018)	dsb Leitfaden «Bearbeiten im Auftrag», Datenschutzbeauftragter Kanton Zürich, Juli 2018, Quelle (Stand 25.03.2019): https://dsb.zh.ch/dam/dsb/publikationen/leitfaeden/Leitfaden_Bearbeiten_im_Auftrag.pdf
Merkblatt Sichere E-Mails (2018)	dsb Merkblatt Sichere E-Mails, Datenschutzbeauftragter Kanton Zürich, Juli 2018, Quelle (Stand 2.5.2019): https://dsb.zh.ch/dam/dsb/publikationen/formulare_und_merkblaetter/Merkblatt_Selbstdatenschutz-Sichere-E-Mails.pdf

Leitfaden und Merkblätter

MB Homeoffice (2017)	Merkblatt Homeoffice, Kanton Luzern, Dienststelle Personal, Juni 2017, Quelle (Stand 25.03.2019): https://www.lukath.ch/wp-content/uploads/2017/09/15_Merkblatt_Home_Office.pdf
Opferhilfe (2013)	Kantonale Opferhilfestelle, Richtlinien betreffend Datenschutz und Schweigepflicht, Kanton Zürich, Dezember 2013, Quelle (Stand 25.03.2019): https://opferhilfe.zh.ch/internet/justiz_inneres/opferhilfe/de/beratungshilfe/_jcr_content/contentPar/morethemes/morethemesitems/richtlinien_datensch.spooler.download.1462777212699.pdf/Richtlinien_Schweigepflicht.pdf
MB Informationsverwaltung (2017)	dsb Merkblatt Informationsverwaltung, Datenschutzbeauftragter Kanton Zürich, Oktober 2017, Quelle (Stand 25.03.2019): https://dsb.zh.ch/dam/dsb/publikationen/formulare_und_merkblaetter/Merkblatt_Informationsverwaltung.pdf
ABH (2017)	Departement für Wirtschaft, Soziales und Umwelt des Kantons Basel-Stadt Amt für Sozialbeiträge, Behindertenhilfe, Richtlinien zur Aufbewahrung und Archivierung von Akten, Ausgabe 12.2017, Quelle (Stand 25.03.2019): https://www.asb.bs.ch/alter-behinderung/behindertenhilfe/aufsicht-und-qualitaet.html#page_section3_section7
LF Informationsverwaltung (2010)	Staatsarchiv des Kantons Zürich – Anleitung Weisung Informationsverwaltung, Anleitung zum Erstellen einer Weisung bzgl. Informationsverwaltung inkl. Aktenplan, Juli 2010, Quelle (Stand 25.03.2019): https://staatsarchiv.zh.ch/internet/justiz_inneres/sta/de/verwaltung/aktenfuehrung/_jcr_content/contentPar/downloadlist/downloaditems/merkblatt_weisung_zu.spooler.download.1395764133865.pdf/AnleitungWeisungInformationsverwaltung.pdf
Datenschutz Meine Rechte (2014)	dsb Merkblatt «Datenschutz - Meine Rechte», Datenschutzbeauftragter Kanton Zürich, August 2014, Quelle (Stand 10.07.2019): https://dsb.zh.ch/internet/datenschutzbeauftragter/de/aktuell/medienmitteilungen/2014/neue_broschuere_datenschutz_meine_rechte/_jcr_content/contentPar/downloadlist_0/downloaditems/brosch_re_datenschut.spooler.download.1411453467914.pdf/Datenschutz_Meine_Rechte.pdf
Sichere Website (2019)	dsb Merkblatt «Sichere Website», Datenschutzbeauftragter Kanton Zürich, August 2019, Quelle (Stand 11.07.2019): https://dsb.zh.ch/internet/datenschutzbeauftragter/de/aktuell/mitteilungen/2019/merkblatt-sichere-website--aktualisierung-zwei-faktor-authentifi/_jcr_content/contentPar/downloadlist/downloaditems/338_1562746499599.spooler.download.1562745855091.pdf/Merkblatt-Sichere-Website.pdf