Revision Datenschutzgesetz (DSG)

Checkliste für eine Standortbestimmung zum Datenschutz

Die Checkliste soll Institutionen dazu dienen,

- eine Standortbestimmung zu ihrer datenschutzrechtlich relevanten Situation vorzunehmen,
- den IST-Zustand der Bearbeitung von Personendaten natürlicher Personen (in erster Linie von Klient:innen und Mitarbeitenden) zu erheben und zu beurteilen und
- daraus mögliche Massnahmen und Veränderungen abzuleiten im Hinblick auf die Inkraftsetzung des revidierten DSG.

Unter dem Begriff Klient:innen sind in diesem Dokument alle Personen mit Unterstützungsbedarf zusammengefasst, die in einer Institutionen wohnen, arbeiten oder einzelne institutionelle Leistungen nutzen.

Diese Checkliste ist als Hilfsmittel zu verstehen. Sie erhebt nicht den Anspruch auf Vollständigkeit.

Bei Fragen stehen die Rechtsberater von ARTISET zur Verfügung.

- Hans-Ulrich Zürcher | 031 351 58 85 | zuercher@advokatur-zuercher.ch
- Christian Streit | 031 385 33 39 | rechtsberatung@artiset.ch
- Yann Golay | 031 385 33 36 | yann.golay@artiset.ch

Ein kurzer Überblick über relevante Inhalte des revidierten Datenschutzgesetzes

1. **Datenschutz** bezweckt den Schutz von **Personendaten**. Personendaten sind «alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen».

   Besonders schützenswerte Personendaten sind
   - Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
   - Daten über die Zugehörigkeit zu einer ethnischen Gruppe oder der Herkunft,
   - Daten über die Gesundheit und die Intimsphäre,
   - genetische und biometrische Daten (z. B. DNA, Fingerabdrücke, Blutbild aufgrund einer Blutentnahme),
   - Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
   - Daten über Massnahmen der Sozialhilfe.

2. Als **Datenbearbeitung** gilt «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten».

3. Als **Datensammlung** gilt jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.
   Es ist ein **Verzeichnis der Datensammlungen** zu führen (vgl. Anhang 2)

4. **Profiling**
   Profiling bedeutet die *automatisierte* Bearbeitung von Personendaten zwecks Erstellung von Verhaltensmustern und Persönlichkeitsprofilen (z.B. wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen etc.).
   Wenn die Verknüpfung von Daten eine Beurteilung von wesentlichen Persönlichkeitsaspekten zulässt (etwa bei der Bearbeitung besonders schützenswerter Personendaten), besteht ein erhöhtes Risiko einer Verletzung der Persönlichkeitsrechte und es ist deshalb die ausdrückliche Einwilligung der betroffenen Person einzuholen.

5. **Risikoanalyse/Datenschutz-Folgeabschätzung**
   Beurteilung, ob durch eine fehlerhafte Bearbeitung personenbezogener Daten ein Risiko für die Rechte der betroffenen Person entstehen kann. Um dieses potenzielle Risiko einschätzen zu können, ist die Eintrittswahrscheinlichkeit eines bestimmten Risikos und das Ausmass des potenziellen Schadens zu beurteilen. Es ist abzuwägen und zu entscheiden, ob die Datenbearbeitung angesichts ihrer Risiken vertretbar ist und wie die erkannten Risiken möglichst minimiert werden können. Die Analyse muss während 2 Jahren aufbewahrt werden.

6. Geltungsbereich des DSG und Anwendbarkeit kantonaler Datenschutzgesetze

Der Bund regelt im DSG die Datenbearbeitung durch Bundesbehörden und durch Private. Die Kantone haben die Kompetenz, die Datenbearbeitung durch kantonale Organe selbst zu regeln.
Viele kantonale Datenschutzgesetze bezeichnen als kantonale Organe auch Private (privatrechtrechtlich organisierte Vereine, Stiftungen etc.), die mit der Erfüllung öffentlicher Aufgaben beauftragt sind. Dies gilt insbesondere für Institutionen, welche aufgrund eines Leistungsvertrags mit dem Kanton Aufgaben der institutionellen Sozialhilfe erfüllen. In diesem Rahmen unterstehen sie dem kantonalen Datenschutzrecht und nicht dem DSG.

7. Rechtsmässigkeit der Datenbearbeitung

Rechtmässig ist eine Datenbearbeitung, wenn

- die freiwillige (formfrei mögliche) Einwilligung der betroffenen Person vorliegt, oder
- sie gesetzlich vorgesehen ist, oder
- die betroffene Person ihre Daten zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat, oder
- die Bearbeitung durch ein überwiegendes öffentliches oder privates Interesse gerechtfertigt ist. – Ein privates Interesse stellt u.a. die Abwicklung eines bestehenden Vertrags (z.B. Arbeitsvertrag, Betreuungsvertrag) dar.

8. Datenschutzverantwortliche:r im Unternehmen

Funktion/Aufgaben:

- prüft die Bearbeitung von Personendaten innerhalb der Institution und interveniert bei Verletzung gesetzlicher Bestimmungen
- hat Zugang zu allen Datensammlungen und Datenbearbeitungen
- führt eine Liste der Datensammlungen
- erarbeitet Vorgaben und Weisungen zur Sicherstellung des Datenschutzes
- nimmt Risikoanalysen und Datenschutz-Folgeabschätzungen vor und dokumentiert diese

Eigenschaften/Stellung:

- kann Mitarbeiter:in der Institution oder mandatierte Drittperson sein
- verfügt über die erforderlichen Fachkenntnisse
- ist organisatorisch/linienmässig so unterstellt, dass Interessenkonflikte vermieden werden (mögliche Lösung: direkte Unterstellung unter Vorstand/Stiftungsrat)

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
1	**Allgemeines / Ausgangslage**				
1.1	Wird Datenschutz in der Institution systematisch geplant und koordiniert?		▪ Grundsätze in Datenschutzkonzept festhalten ▪ Datenschutz ab Planung einer Datenbearbeitung berücksichtigen		
1.2	Wann und wie wird der Datenschutz thematisiert und Situation beurteilt in: ▪ Stiftungsrat/Vorstand? ▪ Geschäftsleitung?		▪ Erlass Datenschutzkonzept durch Stiftungsrat/Vorstand ▪ Datenschutz als Teil des Risikomanagements regelmässig auf Führungsebene behandeln		
1.3	Sind Grundsätze der Datenbearbeitung und Schutzmassnahmen bereits dokumentiert (Datenschutzkonzept, interne Reglemente und Weisungen etc.)?		▪ Datenschutzkonzept erstellen ▪ Datenschutzweisung erstellen		
1.4	Gab es bisher bereits besondere Vorfälle bzw. Probleme bzgl. Datenschutz?		Gemachte Erfahrungen berücksichtigen		
1.5	Untersteht die Institution (ausschliesslich/teilweise) dem kantonalen Datenschutzrecht?		▪ Unterstellung klären ▪ Konformität des IST-Zustands mit den Anforderungen des kantonalen und/oder eidgenössischen Rechts prüfen ▪ Bei Unterstellung unter kantonales Recht künftige Anpassungen der Gesetzgebung verfolgen und nachvollziehen		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
1.6	Form der Datenbearbeitung (elektronisch/Papierform)?		▪ Bewusste Entscheide über künftige Form treffen ▪ Digitalisierung gemäss definiertem Vorgehen vorantreiben		
2	**Verantwortung für Datenschutz in der Institution**				
2.1	Beurteilung der bisherigen Regelung/Zuständigkeit?		Gemachte Erfahrungen in künftige Regelung einfliessen lassen		
2.2	Ist die Verantwortlichkeit bereits geregelt?		▪ Verantwortliche Person bestimmen (Mitarbeiter:in oder externe Person) ▪ Pflichtenheft definieren ▪ Erste Ausbildung und spätere Fortbildung der verantwortlichen Person gewährleisten		
3	**Datensammlungen**				
3.1	Welche Datensammlungen bestehen?		Verzeichnis der Datenbearbeitungen erstellen und regelmässig aktualisieren *Hinweis:* Anforderungen an Verzeichnis werden in Anhang 2 aufgelistet		
3.2	Was beinhalten diese Datensammlungen?		Inventar bestehender Dossiers erstellen		
3.3	Wie und durch wen werden diese geführt?		Koordination der Führung und Standardisierung der Datensammlungen		
3.4	Erfolgen durch die Institution *automatisierte* elektronische Bearbeitungen von besonders schützenswerten Personendaten zwecks Erstellung von		Ausdrückliche Einwilligung der betroffenen Person einholen		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
	Verhaltensmustern und Persönlichkeitsprofilen (z.B. wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen etc.)?				
4	**Datensicherheit**				
4.1	Erfolgt die Datenbearbeitung auf der Infrastruktur der Institution oder jener eines Providers?		Vertragliche Regelungen mit dem Provider bzgl. Einhaltung der Datensicherheit aufsetzen		
4.2	Bestehen innerhalb der Institution technische und organisatorische Massnahmen zum Schutz der bearbeiteten Daten?		▪ Massnahmen überprüfen und allenfalls Sicherheit optimieren ▪ Zugriffsrechte zweckmässig regeln ▪ Zugriff durch Unbefugte verhindern		
4.3	Wie ist Zugang zu Personendaten in der Institution allgemein geregelt? Besteht eine besondere Regelung für den Zugang zu besonders schützenswerten Personendaten?		Zugang zu jeder Datensammlung definieren, für besonders schützenswerte Personendaten möglichst restriktiv, aber funktionsfähig		
4.4	Ist sichergestellt, dass alle relevanten Daten innert nützlicher Frist zur Verfügung stehen?		▪ Technische Voraussetzungen überprüfen und anpassen ▪ Zugangsregelung so definieren, dass stets mindestens eine berechtigte Person anwesend ist		
4.5	Sind die Daten vor Diebstahl, Verfälschung,		Zugangsberechtigungen und technische Situation (IT-technisch bzw. physisch wie z. B. Aufbewahrung Dossiers unter Verschluss) prüfen und allenfalls anpassen		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
	Zerstörung etc. hinreichend geschützt?				
4.6	Datenaustausch: ▪ Wie werden Personendaten ausgetauscht innerhalb Institution und mit Externen? ▪ Erfolgt der Datenaustausch per Mail geschützt?		Gesicherte Datenübermittlung mit verschlüsselter Mail oder in anderer geeigneter Weise sicherstellen		
5	**Zulässigkeit/Rechtmässigkeit der Datenbearbeitung**				
5.1	Liegt für jede Datenbearbeitung eine hinreichende Zustimmung der Betroffenen oder eine besondere gesetzliche Ermächtigung vor?		Bestehende Arbeits-/Heimverträge aktualisieren bzw. neue Verträge ergänzen mit sinngemäss folgendem Passus: *«Mit der Unterzeichnung dieses Vertrags ermächtigt die betreffende Person XXX* [Name der INSTITUTION] *ausdrücklich zur Bearbeitung der bekannt gegebenen Personendaten, soweit dies gesetzlich vorgesehen und zulässig bzw. für die Durchführung dieses Vertrags erforderlich ist und solange kein ausdrücklicher Widerspruch der betreffenden Person vorliegt.»*		
5.2	Werden Daten gemäss einem definierten Zweck bearbeitet?		Bearbeitungszwecke definieren und schriftlich festhalten		
5.3	Erfolgt die Datenbearbeitung innerhalb des definierten Zwecks?		Periodische Prüfung (Stichproben) der Bearbeitung vornehmen		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
5.4	Liegt von Klient:in eine Patientenverfügung bzw. Vorsorgeauftrag vor?		▪ Bestehende Dokumente in Klient:innen-Dossier ablegen ▪ Klient:in empfehlen, eine Patientenverfügung/Vorsorge-auftrag zu erstellen		
6	**Verwendung/Publikation von Bild-/Tonaufnahmen von Klient:innen und Mitarbeitenden**				
6.1	Werden durch die Institution Bild-/Tonaufnahmen angefertigt und verwendet? Verwendung zu welchen Zwecken?		Thema in das Verzeichnis der Datenbearbeitungen aufnehmen		
6.2	Wie wird Zustimmung der Betroffenen zur Verwendung zu Publikationszwecken eingeholt?		Zustimmung zu Verwendung für Publikation ist nur rechtsgültig, wenn sie in Kenntnis der konkreten Aufnahmen und des Zwecks im Einzelfall freiwillig und ausdrücklich erteilt wird und widerrufen werden kann. *Hinweis* Eine generell formulierte Zustimmung im Arbeits-/Heimvertrag genügt nicht		
7	**Verhältnismässigkeit der Datenbearbeitung**				
7.1	Ist die bisherige Datenbearbeitung auf das notwendige Mass beschränkt?		Beschränkung der Datenerhebung auf den Bearbeitungszweck (z.B. Arbeitsvertrag)		
7.2	Ist sichergestellt, dass Daten für einen zulässigen Zweck erhoben, nur zu diesem Zweck bearbeitet und nicht zweckentfremdet genutzt werden?		Gebot der Zweckbindung in Datenschutzkonzept festhalten		
7.3	Werden Daten «auf Vorrat» (ohne konkreten und		Verbot der «Vorratsbearbeitung» im Datenschutzkonzept festhalten		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
	eindeutigen Zweck) erhoben und gespeichert?				
7.4	Ist sichergestellt, dass Daten nur so lange gespeichert sind, wie dies der Bearbeitungszweck dies erfordert?		Gebot der Speicherbeschränkung in Datenschutzkonzept festhalten. *Hinweis* Siehe zu Erforderlichkeit der Bearbeitung auch die Themen «Archivierung» und «Löschung»		
8	**Bekanntgabe/Weitergabe von Daten an Dritte**				
8.1	Werden Daten der Beistandschaft bekannt gegeben?		Bekanntgabe dokumentieren bzw. protokollieren		
8.2	Werden Daten Dritten (Behörden, Ärzt:innen/ Spitälern, Versicherungen etc.) bekannt gegeben?		▪ Orientierung der betroffenen Person ▪ Sichere Datenübermittlung vorsehen		
8.3	Werden Daten ins Ausland bekannt gegeben?		▪ Vor Bekanntgabe Risiken (länderspezifisch) beurteilen (allenfalls nach Rücksprache mit ICT-Provider) ▪ Orientierung der Betroffenen *Hinweis* Als Bekanntgabe ins Ausland gilt auch die Datenspeicherung in einer Cloud auf einer Server-Infrastruktur, die sich physisch im Ausland befindet.		
9	**Orientierung der Betroffenen über Datenbearbeitung**				
9.1	Wann und wie werden Betroffene über Datenbearbeitung orientiert?		▪ Orientierung der Betroffenen sicherstellen und evtl. anpassen ▪ Bei planmässiger Datenbeschaffung muss im Erhebungszeitpunkt informiert werden über		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
			- Person/Kontaktdaten des/der betrieblichen Datenschutzverantwortlichen - Bearbeitungszweck - Zeitraum der Datennutzung - Empfänger, falls Daten Dritten bekannt gegeben werden *Hinweis* «Planmässige Datenbeschaffung» bedeutet, dass gewollt Daten erhoben werden. Empfehlung: Orientierung über Datenbearbeitung erfolgt stets schriftlich (in Arbeits-/Heimvertrag oder in Zusatzdokument zu diesen Verträgen)		
9.2	Befindet sich auf der institutionseigenen Website eine Datenschutzerklärung?		Bestehende Datenschutzerklärung überprüfen bzw. eine solche neu hochladen		
10	**Auskunfts-/Einsichtsrechte von Betroffenen**				
10.1	Wie werden Auskunfts-/Einsichtsrechte bisher gewährleistet?		Auskunfts-/Einsichtsrechte im Datenschutzkonzept festhalten, unter Berücksichtigung der folgenden Anforderungen: ▪ Grundsätzlich jederzeitiges und voraussetzungsloses Auskunfts-/Einsichtsrecht ▪ Grundsätzliche Kostenlosigkeit (Ausnahme bei unverhältnismässigem Aufwand; Kostenverrechnung muss im Voraus bekanntgegeben werden) ▪ Beschränkung oder Verweigerung bei überwiegendem öffentlichem oder privatem Interesse stellt die Ausnahme dar und ihre Voraussetzungen sind definiert		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
11	**Übergabe der Daten an die Betroffenen**				
11.1	Wie werden den Betroffenen ihre Daten bisher übergeben?		Überblick verschaffen und dokumentieren, wie dies bis heute geschieht		
11.2	Ist die Institution in der Lage, Personendaten inskünftig «in einem gängigen elektronischen Format» zu übergeben?		Massnahmen treffen, um Daten entsprechend elektronisch übergeben zu können		
12	**Personaldossiers**				
12.1	Wird ein einziges, umfassendes Dossier pro Mitarbeiter:in in der Personalabteilung geführt?		Alle für eine Mitarbeiter:in relevanten Daten sind in einem einzigen Dossier zusammenführen		
12.2	Wer hat Zugang?		Zugang klar und evtl. differenziert regeln		
12.3	Werden besonders schützenswerte Daten besonders geschützt/separat aufbewahrt?		Schutz prüfen und allenfalls verbessern *Hinweis* Besonders schützenswert sind u.a. Arztzeugnisse und –berichte; Informationen von Unfall-, Krankentaggeld-, Invalidenversicherung; Informationen über gewerkschaftliche Tätigkeit etc.		
12.4	Bestehen «Schattendossiers» (bei Vorgesetzten)?		«Schattendossiers» sind zwingend zu verbieten und zu vernichten		
13	**Klient:innendossiers**				
13.1	Wird ein umfassendes Dossier pro Klient:in geführt?		Überblick verschaffen, wie das heute geschieht und dokumentieren		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
13.2	Wer führt diese Dossiers?		Überblick verschaffen, wie das heute geschieht und dokumentieren		
13.3	Wer hat Zugang zu Dossiers?		Zugang klar und evtl. differenziert regeln		
13.3	Werden besonders schützenswerte Daten besonders geschützt/ separat aufbewahrt?		Schutz prüfen und allenfalls verbessern *Hinweis* Besonders schützenswert sind u.a. Arztzeugnisse und -berichte; ärztliche Behandlungen, Medikamentation und Therapien; Informationen von Unfall-, Krankentaggeld-, Invalidenversicherung; Informationen betreffend Religion, Intimsphäre etc.		
14	**Archivierung von Daten**				
14.1	In welcher Form werden Daten bis heute aufbewahrt?		Grundsätzlich digitale Archivierung fördern *Hinweis* Aufbewahrung in Papierform ist nur selten vorgeschrieben (z.B. für Geschäfts- und Revisionsbericht; Art. 958 f Abs. 2 OR). Daten müssen getrennt nach Art, strukturiert, datiert und chronologisch aufbewahrt werden.		
14.2	Wie lange werden Daten bis heute aufbewahrt?		Archivierungsgrundsätze definieren (in Datenschutz- oder Archivierungskonzept) unter Berücksichtigung gesetzlicher Aufbewahrungsfristen bzw. orientiert an allgemeinen Verjährungsfristen gemäss Bundesrecht und kantonalen Bestimmungen (z.B. in Archivierungsgesetz, Sozialhilfegesetz etc.) *Hinweis* Bundesrechtliche Aufbewahrungsbestimmungen und Verjährungsfristen sind in Anhang 1 dargestellt		
14.3	Wer hat Zugang zu Datenarchiv?		Zugang klar regeln (Grundsatz: so viele Personen wie nötig, so wenige wie möglich).		

#	Thema / Prüfpunkte	Resultat Beurteilung IST-Zustand	Vorschläge für Massnahmen	Termin	Verantwortlich
14.4	Ist die Sicherheit archivierter Daten gewährleistet?		▪ Sicherheitssituation generell überprüfen ▪ Massnahmen zum Schutz archivierter Daten vor Diebstahl, Zerstörung (durch Wasser, Feuer, Ungeziefer etc.) ▪ Schutz elektronisch archivierter Daten vor Veränderung, Löschung etc. ▪ Künftige Lesbarkeit elektronisch archivierter Daten sicherstellen		
15	**Löschung von Daten**				
15.1	Erfolgt die Löschung rechtssicher?		▪ Definitive Lösung elektronischer Daten sicherstellen ▪ Physische Daten vor Ort vernichten (schreddern) oder in speziellen Schredder-Containern der Vernichtung zuführen		
15.2	Sind Löschungstermine geregelt und in differenzierter Weise definiert?		Löschungstermine regeln (in Datenschutzkonzept oder speziellem Löschkonzept), unter Berücksichtigung ▪ gesetzlich definierter Aufbewahrungsfristen ▪ des Grundsatzes, dass Archivierungsdauer zweckmässig beschränkt sein soll		
16	**Instruktion und Sensibilisierung der Mitarbeitenden**				
16.1	Wie werden Mitarbeitende bisher bezüglich Datenschutz instruiert und sensibilisiert ▪ generell? ▪ konkret?		▪ Bekanntmachung aller Datenschutz-relevanten internen Regelungen (Datenschutzkonzept, Weisungen etc.) ▪ Regelmässige allgemeine Instruktion und Sensibilisierung im Rahmen einer internen Weiterbildung ▪ Situative Beratung und Unterstützung einzelner Mitarbeiter:innen und Anleitung der korrekten Handhabung durch Vorgesetzte bzw. betrieblicher Datenschutzverantwortliche:r anhand festgestellter konkreter Fehler/Mängel		

Anhang 1: Aufbewahrungsfristen / Allgemeine Verjährungsfristen gemäss Bundesrecht

Gegenstand	(längste) Verjährungsfrist	gesetzliche Grundlage	Bemerkungen
Geschäftsbücher, Geschäftsbericht, wichtige Belege für Buchhaltung	10 Jahre	Art. 957ff. OR	Die Buchführungspflicht «erfasst diejenigen Geschäftsvorfälle und Sachverhalte, die für die Darstellung der Vermögens-, Finanzierungs- und Ertragslage des Unternehmens (wirtschaftliche Lage) notwendig sind» (Art. 957a Abs. 1 OR). Aufzubewahren sind insbesondere Geschäftsbücher und Buchungsbelege, wozu unter Umständen auch Geschäftskorrespondenz im Zusammenhang mit einem Geschäftsvorfall gehört. Wichtige Belege können unter Umständen auch Arbeits- und Heimverträge sein.
Allgemeine arbeitsrechtliche Ansprüche	5 Jahre	Art. 128 OR	
Daten mit Relevanz für Arbeitszeugnis	10 Jahre		Frist gemäss Rechtsprechung
Lohndaten und arbeitsrechtliche Dokumente mit steuerrechtlicher Relevanz	10 Jahre	Art. 958f Abs. 1 OR; Art. 126 Abs. 3 DBG	
Dokumentation der Einhaltung von Pflichten gemäss Arbeitsgesetz (insbesondere Arbeitszeitkontrollen)	5 Jahre	Art. 73 Abs. 2 Verordnung 1 zum Arbeitsgesetz	
Schadenersatz/Genugtuung bei Körperverletzung/Tötung eines Menschen	3/20 Jahre	Art. 60 Abs. 1bis und Art. 128a OR	Kann frühere Mitarbeitende und ehemalige Klient:innen betreffen
Geschlechtsdiskriminierende Verstösse	3 Monate	Art. 8 Abs. 2 Gleichstellungsgesetz	
Leistungen von oder Beiträge an Sozialversicherungen bzw. Pflicht zu deren Rückerstattung	5 Jahre	Art. 24 und 25 ATSG	Bei *Unfällen* während Arbeitsverhältnis wird jedoch Aufbewahrung der Personalakten während 10 Jahren, bei schweren Unfällen oder Berufskrankheiten während 30 Jahren empfohlen (ad hoc-Empfehlung UVG Nr. 09/87; https://www.koordination.ch/fileadmin/files/ad-hoc/1987/09-87.pdf)

Anhang 2: Anforderungen an ein Verzeichnis der Bearbeitungstätigkeiten

Betriebliche Datenschutzverantwortliche müssen ein Verzeichnis sämtlicher Datenbearbeitungen mit folgende Mindestangaben führen:

- Identität von betrieblichen Datenschutzverantwortlichen
- Bearbeitungszweck
- Kategorien betroffener Personen
- Kategorien bearbeiteter Personendaten
- Kategorien der Datenempfänger
- Aufbewahrungsdauer der Personendaten oder Kriterien zur Festlegung dieser Dauer
- allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit (geeignete technische und organisatorische Schutzmassnahmen)
- Angabe des Staates bei Bekanntgabe von Daten ins Ausland sowie Bekanntgabe von Garantien, durch die ein geeigneter Datenschutz gewährleistet wird