ARTISET

Leitfaden zur Organisation des Datenschutzes

Massnahmen in einer Institution oder Struktur für Menschen mit Unterstützungsbedarf

1. Einführung

Im Hinblick auf das Inkrafttreten des totalrevidierten Bundesgesetzes über den Datenschutz (DSG) am 1. September 2023 sind unzählige Firmen und Organisation angehalten, technische und organisatorische Massnahmen zu treffen, um die neuen – strikteren – Anforderungen einzuhalten. Der vorliegende Leitfaden soll Institutionen und Strukturen für Menschen mit Unterstützungsbedarf bei diesem Vorhaben anzuleiten.

Im vorliegenden Dokument beziehen sich alle Angaben zu Gesetzes- und Verordnungsbestimmungen über den Datenschutz auf die revidierten Fassungen dieser Erlässe, die ab dem 1. September 2023 in Kraft treten, nämlich:

- Neues Bundesgesetz über den Datenschutz («DSG»)
- Neue Datenschutzverordnung («DSV»)

Im vorliegenden Dokument bezieht sich die Bezeichnung «Einrichtung» auf Institutionen und Strukturen für Menschen mit Unterstützungsbedarf (Menschen im Alter, Menschen mit Behinderung, Kinder und Jugendlich mit besonderen Bedürfnissen).

2. Ist-Zustand

Als Erstes sollte die Einrichtung einen **Ist-Zustand der personenbezogenen Datenerhebungen und -sammlungen im Betrieb** erstellen. Auf ihrer Webseite stellt die Föderation ARTISET eine solche **Checkliste** zur Verfügung, die dazu hilfreich sein kann. Ziel ist, sich einen Überblick zur Art und Ausmass des Handlungsbedarfs in der Einrichtung in Bezug auf den Datenschutz zu verschaffen.

3. Datenschutzkonzept

Es empfiehlt sich ein Datenschutzkonzept anhand des von ARTISET zur Verfügung gestellten **Muster-Datenschutzkonzeptes** zu erarbeiten, dies auch wenn die Erstellung eines solchen Konzepts vom Gesetz nicht verlangt wird: Ein Datenschutzkonzept trägt dem Stellenwert des Datenschutzes im Sinne der Achtung der Privatsphäre und der Persönlichkeitsrechte der Leistungsbeziehenden bzw. Bewohnenden, der Mitarbeitenden und allenfalls auch der Geschäftspartner:innen der betroffenen Einrichtung Rechnung: Das **Hauptziel** eines solchen Konzepts ist die Gewährleistung des Schutzes der Persönlichkeit natürlicher Personen vor widerrechtlicher oder unverhältnismässiger Bearbeitung von personenbezogenen Daten. So soll das Konzept als verbindliche Richtlinie die für die betroffene Einrichtung tätigen Personen darin unterstützen, datenschutzrechtlich einwandfrei zu handeln. Die Erarbeitung eines solchen Konzepts ist freiwillig; das Gesetz verlangt nicht, dass ein solches Instrument verbindlich entwickelt wird.

ARTISET

Zieglerstrasse 53, 3007 Bern
T +41 31 385 33 33
info@artiset.ch, artiset.ch

Föderation der Dienstleister
für Menschen mit Unterstützungsbedarf

Weiter wird auch empfohlen, die externen Personen und Firmen, die mit der Einrichtung im Rahmen ihres Geschäftsverkehrs in Kontakt stehen, dazu einzuladen, sich schriftlich zu verpflichten, das Datenschutzkonzept der Einrichtung einzuhalten.

4. Pflichtenheft des/der Datenschutzverantwortlichen

Jede Einrichtung muss eine:n «(Datenschutz-)Verantwortliche:n» ernennen. Diese:r kann ein:e Mitarbeiter:in der Einrichtung oder eine externe Person sein – auch eine juristische Person (Treuhandbüro zum Beispiel). Er/Sie entscheidet über den Zweck und die Mittel der Bearbeitung von personenbezogenen Daten im Betrieb (vgl. Art. 5 Bst. j DSG). Er/Sie kann «Auftragsbearbeiter:innen» Aufgaben delegieren (vgl. Art. 5 Bst. k DSG).

Die unterschiedlichen Pflichten des/der Datenschutzverantwortlichen einer Einrichtung sind über das Gesetz und die Verordnung über den Datenschutz verstreut (vgl. Art. 5 Bst. j DSG u. a.). Es ist daher sinnvoll, ein Pflichtenheft des/der Datenschutzverantwortliche(n) zu erstellen: So liegt eine klare und synthetische Übersicht seiner/ihrer Pflichten vor. ARTISET stellt eine entsprechende **Vorlage** zur Verfügung.

5. Bearbeitungsverzeichnisse

Die Erstellung eines oder mehrerer Bearbeitungsverzeichnisse(s) ist für Betriebe, die weniger als 250 Mitarbeitende zahlen, kein Obligatorium (vgl. Art. 12 DSG, Art. 24 DSV), ist aber auf alle Fälle sinnvoll. Damit solche Verzeichnisse ihren vollen Sinn entfalten, sollen sie auch laufend (oder mindestens regelmässig in kurzen Zeitabständen) aktualisiert werden. ARTISET stellt eine entsprechende **Vorlage** zur Verfügung.

6. Personendatensammlungen: Zugänge und Aktualisierung

Es empfiehlt sich, schriftlich festzulegen, wer im Betrieb zu welchen Personendatensammlungen Zugang hat und entsprechende Zugangsberechtigungen (Passwörter für die elektronische Ablage, Schlüssel für die Papierablage) einzurichten.

Weiter wird auch empfohlen, schriftlich festzulegen, wer dem/der betrieblichen Datenschutzverantwortlichen inhaltliche Änderungen von welchen Personendatensammlungen mitteilt, damit dieser/diese oder eine durch den/die Verantwortliche:n beauftragte Person die entsprechenden Datenbearbeitungsverzeichnisse anpasst.

7. Technische und organisatorische Schutzmassnahmen

Es empfiehlt sich, die nötigen Massnahmen umzusetzen, damit der Datenschutz der Einrichtung durch Technikgestaltung («Privacy by Design») und durch datenschutzfreundliche Voreinstellungen («Privacy by Default») gewährleistet wird (vgl. Art. 7 DSG, Art. 3 DSV). Dadurch soll die Datensicherheit gewährleistet werden (vgl. Art. 8 DSG). Durch Zugangs- und Personendatenträgerkontrollen soll verhindert werden, dass unbefugte Personen Zugang zu elektronischen Datenbeständen haben, diese verändern, zerstören oder entwenden.

Angesichts der stetigen technischen Entwicklung hütet sich die neue Gesetzgebung über Datenschutz absichtlich davor, bestimmte technische Lösungen zu verordnen –: Das Gesetz beschränkt sich darauf, von den Einrichtungen zu verlangen, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden (Art. 7 Abs. 1 DSG).

ARTISET

Zieglerstrasse 53, 3007 Bern
T +41 31 385 33 33
info@artiset.ch, artiset.ch

Die entsprechenden Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein (Art. 7 Abs. 2 DSG). Eine dem Risiko angemessene Datensicherheit muss gewährleistet werden (Art. 8 Abs. 1 DSG).

Der Einsatz von (verschlüsselten) HIN-Adressen für E-Mail mit sensiblen personenbezogenen Daten ist beispielsweise eine gute Sache. Ob ein Verkehr durch klassische E-Mail-Kanäle unzulässig wäre, kann wiederum nicht ohne Weiteres behauptet werden – mit dem Einsatz von HIN-Adressen steht man aber auf der sicheren Seite.

Mit folgenden Mitteln soll sichergestellt werden, dass der Schutz elektronisch bearbeiteter Personendaten durch die Verwendung folgender Mittel gewährleistet, wird:

- Verschlüsselung,
- Einsatz von Firewalls, Virenschutzprogrammen und HIN-Adressen für E-Mail mit sensiblen Daten
- Umsetzung von allfälligen weiteren technischen Schutzmassnahmen
- Protokollierung von Zugriffen

8. Einwilligung zur Datenbeschaffung sowie -bearbeitung

Grundsätzlich muss die betroffene Person vom / von der Datenschutzverantwortlichen über die *Beschaffung* von Personendaten, die sie betreffen, informiert werden (Art. 19 Abs. 1 DSG; es gibt aber Ausnahmen: vgl, folgenden Kapitel). Diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden. Ausserdem dürfen Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft und bearbeitet werden (Art. 6 Abs. 3 DSG). Darüber hinaus darf eine Bearbeitung von Personendaten nicht erfolgen, wenn die betroffene Person ausdrücklich dagegen opponiert (Art. 30 Abs. 2 Bst. b DSG a contrario).

Aus diesem Zusammenspiel von Gesetzesbestimmungen geht hervor, dass die betroffene Person über alle Verwendungszwecke (und dadurch über die vorgesehenen Bearbeitungen) ihrer Personendaten im Voraus informiert werden muss. Sie darf die Verwendung/Bearbeitung ihrer Personendaten ablehnen. Die Art und Weise, wie ihre Einwilligung eingeholt wird, muss keine besondere Form aufweisen (an sich, ein einfaches Zeichen genügt).

Für die Bearbeitung von *besonders schützenswerten Personendaten* (wie z.B. Informationen über den Gesundheitszustand) muss eine ausdrückliche Einwilligung der betroffenen Person vorliegen (vgl. Art. 6 Abs. 7 Bst. a DSG).

Wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat, liegt i.d.R. keine Persönlichkeitsverletzung vor (vgl. Art. 30 Abs. 3 DSG).

9. Informationspflicht der Einrichtung

Damit der/die Datenschutzverantwortliche und die betroffenen Stellen innerhalb der Einrichtung ihrer Informationspflicht gemäss Art. 19-20 DSG und Art. 13 DSV gegenüber Leistungsbeziehenden, Geschäftspartner:innen und Mitarbeitenden nachkommen können, wird empfohlen, die Einhaltung folgender Schritte/Leitplanken mittels Richtlinien sicherzustellen:

- Der/Die Datenschutzverantwortliche informiert die betroffene Person, wenn die Einrichtung Personendaten über sie beschafft – dies, auch wenn die Daten nicht bei der betroffenen Person beschafft werden.
- Der/Die Datenschutzverantwortliche ist vom Gesetz her verpflichtet, der betroffenen Person mindestens mitzuteilen:

- Die Identität und die Kontaktdaten des/der Datenschutzverantwortlichen
- Den Bearbeitungszweck
- Gegebenenfalls die Empfänger:innen oder die Kategorien von Empfänger:innen, denen Personendaten bekanntgegeben werden
- Die Kategorien der bearbeiteten Personendaten, sofern die Daten nicht bei der betroffenen Person beschafft werden
- Den Staat oder das internationale Organ und gegebenenfalls die Garantien nach Art. 16 Abs. 2 DSG oder die Anwendung einer Ausnahme nach Art. 17 DSG, sofern die Personendaten ins Ausland bekanntgegeben werden

Darüber hinaus sind folgende Modalitäten zu beachten:

- Werden die Daten nicht bei der betroffenen Person beschafft, so soll der/die Datenschutzverantwortliche ihr diese Informationen spätestens einen Monat, nachdem er/sie die Daten erhalten hat, mitteilen.
- Gibt der/die Datenschutzverantwortliche die Personendaten vor Ablauf dieser Frist bekannt, so soll er/sie die betroffene Person spätestens im Zeitpunkt der Bekanntgabe informieren.
- Diese Informationspflicht entfällt, wenn:
  - Die betroffene Person bereits über die entsprechenden Informationen verfügt
  - Die Bearbeitung gesetzlich vorgesehen ist
  - Der/Die Datenschutzverantwortliche gesetzlich zur Geheimhaltung verpflichtet ist
- Wenn die Personendaten nicht bei der betroffenen Person beschafft werden, entfällt die Informationspflicht zudem in folgenden Fällen:
  - Die Information ist nicht möglich
  - Die Information erfordert einen unverhältnismässigen Aufwand
- Darüber hinaus kann der/die Datenschutzverantwortliche die Mitteilung der Informationen in den folgenden Fällen einschränken, aufschieben oder darauf verzichten:
  - Überwiegende Interessen Dritter es erfordern
  - Die Information vereitelt den Zweck der Bearbeitung
  - Überwiegende Interessen des/der Datenschutzverantwortlichen erfordern es
  - Die Personendaten werden nicht Dritten bekannt (notabene: in diesem Rahmen gelten Einrichtungen, die zum selben Konzern gehören, nicht als Dritte)

10. Einsichts- und Auskunftsrecht der betroffenen Personen

Damit die Personen, deren Daten durch die Einrichtung behandelt werden, («betroffenen Personen») ihre Einsichts- und Auskunftsrechte gemäss Art. 25-26 DSG und Art. 16-19 DSV zielführend geltend lassen können, wird empfohlen, mittels Richtlinien die Einhaltung folgender Schritte/Leitplanken vorzusehen:

- Jede Person kann vom/von der Datenschutzverantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden
- Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall sollen ihr folgende Informationen mitgeteilt werden:
  - Identität und Kontaktdaten des/der Datenschutzverantwortlichen
  - Bearbeitete Personendaten
  - An der Sammlung Beteiligten
  - Gegebenenfalls: Datenempfänger:innen
  - Bearbeitungszweck der personenbezogenen Daten
  - Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer

    - Verfügbare Angaben über die Herkunft der Personendaten, soweit die Daten nicht bei der betroffenen Person beschafft wurden
- Die Auskunft ist innert 30 Tagen durch die Einrichtung in allgemeinverständlicher Weise und schriftlich zu erteilen
- Wenn die Erteilung der Auskunft nicht mit einem unverhältnismässigen Aufwand verbunden ist, ist sie kostenlos zu erteilen
- Widerrechtlich oder unrichtig bearbeitete sowie unrichtige Daten sollen durch die Einrichtung berichtigt oder vernichtet werden
- Jede betroffene Person kann die Bekanntgabe ihrer Daten sperren lassen, wenn sie ein schutzwürdiges Interesse nachweist
- Das Vorliegen einer automatisierten Einzelentscheidung wird gegebenenfalls der betroffenen Person mitgeteilt sowie die Logik, auf der die Entscheidung beruht (in der Praxis treffen Einrichtungen aber kaum automatisierten Einzelentscheidungen)
- Die Empfänger:innen oder die Kategorien von Empfänger:innen, denen Personendaten bekanntgegeben werden, werden gegebenenfalls der betroffenen Person mitgeteilt
- Falls die Personendaten ins Ausland bekanntgegeben werden:
    - Die Informationen nach Art. 19 Abs. 4 DSG
    - Den betroffenen Staat oder das betroffene internationale Organ und gegebenenfalls die Garantien nach Art. 16 Abs. 2 DSG oder die Anwendung einer Ausnahme nach Art.17 DSG
- Die Erteilung von Auskünften und die Einsichtsrechte können ausnahmsweise eingeschränkt oder verweigert werden, wenn ein Gesetz es vorsieht, überwiegende Interessen Dritter oder der Einrichtung entgegenstehen, die Personendaten nicht Dritten bekannt gegeben werden oder das Auskunftsgesuch offensichtlich unbegründet ist

Es empfiehlt sich, ein (summarisches) Meldeverfahren vorzusehen, damit Betroffene ihr Auskunftsrecht geltend machen und der/die Datenschutzverantwortliche sowie die betroffenen Stellen der Einrichtung den Auskunftsgesuchen effizient Folge leisten können.

11. Bearbeitungsauftrag

Die Bearbeitung von Personendaten kann einem/einer Auftragsbearbeiter:in übertragen werden (vgl. Art. 9 DSG und Art. 7 DSV). In diesem Rahmen gilt zu beachten:

Ein solcher Auftrag muss nicht unbedingt schriftlich erteilt werden. Er kann auch mündlich oder gar durch schlüssige Handlungen anvertraut werden. ARTISET stellt eine **Vorlage** für einen detaillierten schriftlichen Auftragsvertrag. Dieser stellt die ausführliche und ‘kompakte’ Formalisierung von in der relevanten gesetzlichen Bestimmungen dar (vgl. Art. 9 DSG und auch Art. 7 DSV sowie weitere Bestimmungen und Grundsätze des Datenschutz- und Obligationenrechts). Auch wenn es nicht unbedingt erforderlich ist, einen so detaillierten Vertrag zu unterzeichnen, kann es sich trotzdem als sicherer erweisen: In der Tat muss der/die Verantwortliche sicherstellen, dass der/die Auftragsbearbeiter:in das Gesetz im selben Umfang einhält, wie er/sie selbst es tut (Sorgfaltspflicht). Ein schriftlicher Auftrag hat den Vorteil, den rechtlichen Rahmen zu klären und zu formalisieren.

Darüber hinaus muss noch erwähnt werden:

- Eine Auftragsbearbeitung ist auch zulässig, ohne dass die Person, deren Daten bearbeitet werden, ihre Einwilligung dazu geben müsste.
- Ein:e Auftragsbearbeiter:in darf die Bearbeitung nur mit vorgängiger Genehmigung des/der Verantwortlichen einem Dritten übertragen.
- Die Datenbearbeitung innerhalb der gleichen juristischen Person (Filiale, Verwaltungseinheit, Mitarbeitende) stellt grundsätzlich keine Auftragsbearbeitung dar. Es wäre also überflüssig, jeder

interne Austausch von personenbezogenen Daten zwischen Ressorts der gleichen Einrichtung mit einem Bearbeitungsvertrag zu flankieren.
- Werden Daten in einer sogenannten Cloud aufbewahrt, handelt es sich dabei grundsätzlich um einen Anwendungsfall der Auftragsbearbeitung, welche die entsprechenden Voraussetzungen erfüllen muss. Falls hierfür personenbezogene Daten ins Ausland bekanntgegeben werden, müssen zudem die entsprechenden Voraussetzungen vorliegen (s. unten).

12. Recht der betroffenen Person auf Datenherausgabe oder -übertragung

Gemäss Art. 28-29 DSG und 20-22 DSV kann jede Person von der Einrichtung die Herausgabe ihrer Personendaten, die sie ihr bekanntgegeben hat, in einem gängigen elektronischen Format und i.d.R. kostenlos verlangen, wenn die Daten automatisiert bearbeitet werden. In der Praxis dürfte eine solche automatisierte Datenbearbeitung durch Einrichtungen aber kaum erfolgen.

13. Bekanntgabe von Personendaten ins Ausland

Falls Personendaten ins Ausland bekanntgegeben werden, soll die Einrichtung die in Art. 16-18 DSG und Art. 8-12 DSV vorgesehenen Massnahmen treffen.

14. Datenschutz-Folgenabschätzungen

Wenn die Einrichtung personenbezogene Daten bearbeitet, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen können, muss der/die Datenschutzverantwortliche Datenschutz-Folgenabschätzungen im Sinne von Art. 22 DSG in jedem Fall vorgängig erstellen. Die Datenschutz-Folgenabschätzung muss eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte enthalten (Art. 22 Abs. 3 DSG).

Je nach Ergebnis der vorgenommenen Datenschutz-Folgenabschätzung soll der Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) gemäss Art. 23 DSG einbezogen werden.

In der Praxis kommt es nicht selten vor, dass Einrichtungen Bearbeitungen von personenbezogenen Daten tätigen, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen können. Datenschutz-Folgenabschätzungen sollen entsprechend häufig vorgenommen werden.

15. Ablage und Vernichtung von Personendaten

Personendaten, die für einen bestimmten Zweck erhoben werden, dürfen nur so lange aufbewahrt werden, wie dies für die Erfüllung dieses Zwecks notwendig ist (Art. 6 Abs. 4 DSG). Werden sie nicht mehr benötigt, sind sie zu anonymisieren oder zu löschen/vernichten, sofern nicht überwiegende Gründe die weitere Aufbewahrung rechtfertigen.

So ist von Fall zu Fall zu prüfen:
- Wie lange die in der Einrichtung bearbeiteten personenbezogene Daten benötigt werden,
- Ob für bestimmte Daten eine gesetzliche Aufbewahrungspflicht besteht
- Oder ob ein überwiegendes Interesse an der weiteren Aufbewahrung dieser Daten besteht.

Deshalb empfiehlt es sich, mittels Richtlinien sicherzustellen, dass:
- Personendaten, die für die Bearbeitung nicht mehr benötigt werden, aufbereitet und während einer bestimmten oder bestimmbaren Dauer abgelegt werden.

- Personendaten von untergeordneter Bedeutung unmittelbar nach Erreichen des Bearbeitungszwecks vernichtet werden (physisch zerstört oder elektronisch unwiederbringlich gelöscht).

16. Automatisierte Datenbearbeitung

Wie bereits erwähnt dürften automatisierte Datenbearbeitungen durch Einrichtungen in der Praxis kaum erfolgen. Falls automatisierte Datenbearbeitungen trotzdem vorgenommen werden, ist zu beachten:

- Überall wo besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet werden, ist das Speichern, das Verändern, das Lesen, das Bekanntgeben, das Löschen und das Vernichten der Daten zu protokollieren (vgl. Art. 4 DSV). Das ist aber keine Pflicht, wenn präventive Massnahmen den Datenschutz gewährleisten.
- Sofern besonders schützenswerte Personendaten in grossem Umfang durch die Einrichtung automatisiert bearbeitet werden, soll ein Reglement für automatisierte Bearbeitungen im Sinne von Art. 5 DSV erarbeitet werden. Das Reglement muss insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten (vgl. Art. 5 Abs. 2 DSV).

17. Profiling

Profiling bedeutet, Daten zu verwenden, um bestimmte persönliche Aspekte einer Person zu bewerten – etwa Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel (vgl. Art. 5 Bst. f DSG). Das Profiling setzt eine automatisierte Bearbeitung von Personendaten voraus.

In der Praxis dürfte eine solche automatisierte Datenbearbeitung durch die Einrichtungen kaum erfolgen. Deswegen sind die gesetzlich vorgesehenen besonderen Schutzmechanismen gegenüber dem Profiling im vorliegenden Rahmen kaum relevant – und werden hier nicht näher beschrieben.

18. Meldung von Verletzungen des Datenschutzes

Es empfiehlt sich ein (summarisches) Meldeverfahren vorzusehen, damit der/die Datenschutzverantwortliche allfällige Verletzungen des Datenschutzes durch die Einrichtung beim Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) effizient melden kann (vgl. Art. 24 DSG und Art. 15 DSV).

Yann Golay Trechsel / 29.10.2024

ARTISET

Zieglerstrasse 53, 3007 Bern
T +41 31 385 33 33
info@artiset.ch, artiset.ch