Bern, im Mai 2023

Revidiertes Datenschutzrecht – Neuerungen und Empfehlungen

Ausgangslage

Das totalrevidierte Datenschutzgesetz (nDSG) tritt am 1. September 2023 in Kraft. Ziel der Revision war es, das Datenschutzrecht an das europäische Recht anzugleichen und die Rechte der betroffenen Personen hinsichtlich der Selbstbestimmung und Transparenz zu stärken. Dieses Merkblatt zeigt die wichtigsten Neuerungen und den Handlungsbedarf auf.

Pflicht zur Führung eines Verzeichnisses aller Personendatenbearbeitungen

Bei jeder Beschaffung von Personendaten müssen die Betroffenen darüber informiert sein, im besten Fall erhält man die Daten von ihnen selbst und hat somit ihre Einwilligung.
Neu verlangt das Gesetz, dass ein Verzeichnis über jede Bearbeitungstätigkeit geführt und laufend aktualisiert werden muss. Das Verzeichnis muss mindestens folgendes enthalten: Wer ist die verantwortliche Person im Betrieb, was der Bearbeitungszweck, die Kategorien der Daten, die Aufbewahrungsdauer, Massnahmen zur Gewährleistung der Datensicherheit. Wie ein solches Verzeichnis auszusehen hat, wird im Gesetz nicht definiert.
Es wird davon abgeraten, Daten ins Ausland zu transferieren (z. B. Datenablage auf einem ausländischen Server), sonst gelten verschärfte Bestimmungen.

Datenlöschung

Aufgrund der Verhältnismässigkeit dürfen Datenbearbeitungen nur so weit gehen, wie sie für den verfolgten Zweck erforderlich sind. Anschliessend sind die Daten zu löschen oder anonymisieren. Was bisher galt, wird neu ausdrücklich im Gesetz geregelt und mit Busse bedroht: eine zu lange Aufbewahrung von Daten stellt eine Datenschutzverletzung dar.
Es gelten die gesetzlichen Aufbewahrungsfristen.
Patientendossiers sind in der Regel 10 Jahre aufzubewahren. Bestehen ältere Daten von Patient*innen, welche sich nicht mehr in Behandlung befinden, sind diese zu löschen.
Arbeitsrechtliche Unterlagen sind spätestens 10 Jahre nach Austritt zu löschen, nicht mehr Benötigtes wie Bewerbungsunterlagen direkt nach Beendigung des Arbeitsverhältnisses.

Datensicherheit

Das revidierte Gesetz verlangt, durch technische und organisatorische Massnahmen für eine angemessene Datensicherheit zu sorgen. Neu müssen Verletzungen der Datensicherheit dem EDÖB gemeldet werden, wenn sie voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Eine Verletzung der Datensicherheit liegt vor, wenn Personendaten verloren gehen, gelöscht, verändert oder Drittpersonen (Unbefugten) zugänglich gemacht werden. Eine Meldung muss nur erstattet werden, wenn durch die Verletzung ein hohes Risiko für negative Folgen der betroffenen Person besteht.

Recht auf Datenportabilität

Die Betroffenen haben neu das Recht, ihre Personendaten in einem gängigen elektronischen Format zu verlangen oder an Dritte übertragen zu lassen. Die Herausgabe bzw. Übermittlung muss in der Regel kostenlos erfolgen, falls dies kein übermässiger Aufwand verursacht. Gängig ist ein «elektronisches Format», welches das automatische Einlesen der Daten in ein Computersystem in strukturierter Form ermöglicht (z.B. als EXCEL, XML-File usw.).

OdA ARTECURA
Rainweg 9H, 3068 Utzigen
071 330 01 00, info@artecura.ch, www.artecura.ch

Empfehlungen zur Umsetzung

- Datenschutzerklärung: Wo Daten gesammelt werden, muss eine Datenschutz-erklärung existieren. Ein Hinweis auf der Website oder in schriftlichen Unterlagen muss die Information enthalten, wo die Datenschutzerklärung eingesehen/abgeholt werden kann. Ob die betroffene Person es tatsächlich anschaut, spielt keine Rolle. Ein Muster zur Datenschutzerklärung finden Sie hier: https://dsat.ch/download/.
  - ⇒ Auf der Website muss kein Fenster mit einer Cookie-Erklärung aufpoppen, aber es muss ein sichtbarer Link auf die Datenschutzerklärung bestehen.
  - ⇒ Für die Anstellung von Mitarbeitenden ist etwa im Arbeitsvertrag oder im Personalreglement auf die Datenschutzerklärung zu verweisen.

- Datenschutzverantwortliche Person: Jeder Betrieb muss eine konkrete Person als Datenschutzverantwortliche*r definiert haben. Diese muss über die notwendigen Fachkenntnisse verfügten und Zugang zu allen Datensammlungen haben.
  - ⇒ Eine interne oder externe Person ist zu bestimmen und ein Pflichtenheft für die datenschutzverantwortliche Person ist zu erstellen. Ein Muster finden Sie hier: https://www.curaviva.ch/Fachwissen/Datenschutz-und-Aktenbearbeitung/PXaEp/.

- Technische und organisatorische Massnahmen für die Datensicherheit: Dabei geht es technisch um die internen Zugriffsrechte (wer hat Einsicht in welche Daten) und den Schutz gegen aussen (Firewalls).
  Organisatorisch können Weisungen und Schulungen fürs Personal sinnvoll sein.
  Zweck dieser Massnahmen ist, dass auf Personendaten nur diejenigen Personen eine Einsicht haben, welche den Zugriff für die Erfüllung ihrer Arbeit benötigen.
  - ⇒ Wer in einer Gruppenpraxis arbeitet, darf nicht die Daten aller Patient*innen einsehen können, sondern nur jene der selber betreuten Patient*innen.

- Datenbearbeitungsverzeichnis: Wer Daten bearbeitet, muss ein Verzeichnis über die Art und Weise der Datenbearbeitung führen. Darin müssen die oben genannten Mindestangaben ersichtlich sein und aktuell gehalten werden.
  - ⇒ Ein Excel- oder Worddokument mit den wesentlichen Eckwerten genügt, in der nötigen Kürze. Als Bearbeitungszweck reicht etwa «Arbeitszeiterfassung», «Lohnabrechnung», «Kundenbetreuung», als Kategorien der Personendaten reicht eine Bezeichnung wie «Kontaktdaten» oder «Arbeitszeit» und als Kategorien der betroffenen Personen z. B. «Mitarbeiter*in», «Kunde*in».

- Versand von höchstpersönlichen Daten: Beim Versenden von Personendaten sind Massnahmen zu ergreifen, damit keine unberechtigten Dritte sie einsehen können.
  - ⇒ Falls Personendaten per E-Mail versendet werden, ist ein System zu verwenden, welches die Verschlüsselung vornimmt (z. B. HIN).

- Recht auf Löschung: Wenn betroffene Personen die Löschung der sie betreffenden Daten verlangen, muss dies vorgenommen werden (ausser bei den selber zwingend benötigten Daten, etwa für Arbeitszeugnisse oder Abrechnungen).
  Zudem ist ein Löschprozess für die gesammelten Daten zu definieren, wobei die Aufbewahrungsfristen pro Datenkategorie festgelegt werden müssen.
  - ⇒ Auf jedem Dokument ist das Erstellungsdatum sowie die entsprechende Aufbewahrungsdauer gut sichtbar angebracht und es wird periodisch überprüft, ob Löschungen vorzunehmen sind.

- Recht auf Auskunft: Personendaten sind Betroffenen auf Anfrage innert 30 Tagen herauszugeben. Es ist sicherzustellen, dass die Daten innert Frist gefunden und in elektronischer Form der betroffenen Person herausgegeben werden können.
  - ⇒ Das Dokumenten-System muss exportieren können (z.B. als PDF).