CURAVIVA LU

wohnen · betreuen · pflegen

Informationsblatt Datenschutz
Umsetzung des neuen Datenschutzgesetzes per 1. September 2023

Für Organisationen, Angestellte oder Selbständige, welche überwiegend besonders schützenswerte Personendaten (z.B. Gesundheitsdaten) bearbeiten

1. Datenschutz / Einleitende Zusammenfassung

Das geltende Bundesgesetz über den Datenschutz (DSG; seit 1992 in Kraft) sowie die dazugehörige Verordnung bezwecken den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, deren Personendaten bearbeitet werden.

In diesem Informationsblatt wird aufgezeigt, was Datenschutz bedeutet und was das insbesondere für verantwortliche Personen bedeutet, die mit besonders schützenswerten Personendaten (v.a. Gesundheitsdaten) arbeiten bzw. solche verarbeiten.

Das neue Datenschutzgesetz, welches am 1. September 2023 in Kraft tritt, sorgt für einen noch besseren Schutz von Personendaten. Nachfolgend wird auf die wichtigsten Neuerungen, wie insbesondere dem Ausbau der «besonders schützenswerten Daten», dem «Profiling mit hohem Risiko», dem «Datenschutz durch Technik», der Datenschutzerklärung auf der Webseite, dem Verzeichnis der Bearbeitungstätigkeiten in bestimmten Fällen oder die Bussen eingegangen.

Wer bis dato bereits Personendaten gemäss dem geltenden Datenschutzgesetz korrekt bearbeitet hat, wird auch mit dem neuen Datenschutzgesetz vor keine grösseren Probleme gestellt werden. Dennoch gilt es die nachfolgenden Punkte zu berücksichtigen:

2. Ziel und Zweck des Datenschutzes

Der Datenschutz befasst sich mit der informationellen Selbstbestimmung sowie dem Schutz vor missbräuchlicher Datenbearbeitung, welche natürliche Personen in ihrer Persönlichkeit oder ihren Grundrechten einschränkt. Das Datenschutzgesetz hat seit jeher zum Zweck, diese Rechte zu schützen, indem es Vorgaben zum Umgang und zur Bearbeitung mit Personendaten definiert.

3. Neues Datenschutzgesetz (DSG) per 1. September 2023

Per 1. September 2023 treten das totalrevidierte Datenschutzgesetz (DSG), die Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) sowie die neue Verordnung über Datenschutzzertifizierungen (VDSZ) in Kraft.

Das revidierte Datenschutzgesetz und die entsprechenden Bestimmungen in den Verordnungen sorgen künftig für einen (noch) besseren Schutz der persönlichen Daten. Insbesondere wird der Datenschutz den technologischen Entwicklungen angepasst, die Selbstbestimmung über die persönlichen Daten gestärkt sowie die Transparenz bei der Beschaffung von Personendaten erhöht.

Das neue Datenschutzgesetz stellt sodann insbesondere die Vereinbarkeit mit dem europäischen Recht (DSGVO) sicher. Die Anpassungen im neuen Datenschutzrecht sind wichtig, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig ohne zusätzliche Anforderungen möglich bleibt.

3.1 Was bleibt unverändert?

Die Art und Weise der Datenbearbeitung nach dem neuen Datenschutzgesetz ändert sich nicht grundlegend. Wie bisher ist für die Bearbeitung von allgemeinen Personendaten keine ausdrückliche Einwilligung oder ein anderer Rechtfertigungsgrund nötig, sofern:

- die Bearbeitungsgrundsätze der Transparenz – insbesondere die Erfüllung der Informationspflichten –, der Zweckbindung, der Verhältnismässigkeit sowie der Datensicherheit eingehalten werden,
- die betroffene Person der Bearbeitung (vorgängig) nicht widersprochen hat
- und Dritten keine besonders schützenswerten Personendaten mitgeteilt werden.

Wie bisher braucht es nur dann eine ausdrückliche Einwilligung zum Zeitpunkt der Datenerhebung der Betroffenen, sofern besonders schützenswerte Personendaten bearbeitet werden (z.B. Gesundheitsdaten).

Es ist dafür zu sorgen, dass alle personenbezogenen Daten gelöscht oder anonymisiert werden, sobald sie für den Zweck, der deren Bearbeitung rechtfertigte, nicht mehr benötigt werden.

3.2 Die wichtigsten Änderungen und Neuerungen

- **Persönlicher und sachlicher Geltungsbereich (Art. 2 DSG)**

Das neue Datenschutzgesetz (DSG) und die dazugehörige Verordnung gelten wie bis anhin für die Bearbeitung von Personendaten durch Private und Bundesorgane. Folglich sind private Unternehmen, aber auch Vereine sowie grundsätzlich auch Privatpersonen betroffen, welche Daten natürlicher Personen bearbeiten.

Nicht mehr anwendbar ist das neue DSG künftig auf Daten juristischer Personen. Somit sind nur noch die Daten natürlicher Personen betroffen und geschützt.

- **Ausbau der «besonders schützenswerten» Personendaten (Art. 5 DSG)**

Als „besonders schützenswerte“ Personendaten gelten weiterhin Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; Daten über die Gesundheit, Intimsphäre sowie die Zugehörigkeit einer Ethnie oder Rasse; Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen sowie Daten über Massnahmen der sozialen Hilfe.

Der bestehende Katalog der „besonders schützenswerten“ Personendaten wird ausgebaut. Neu werden zusätzlich die digital erfassbaren Identifikationsdaten wie biometrische Daten, Fingerabdruck, Retina-Scan und genetische Daten aufgenommen.

- **Profiling / Profiling mit hohem Risiko (Art. 5 DSG)**

Neu wird der Begriff «Profiling» verwendet, welcher jede automatisierte Bearbeitung von Daten bedeutet.

Als Profiling werden Personendaten beschrieben, mithilfe derer sich ein genaues Bild über einen Menschen machen lässt. Dazu zählen Merkmale wie der Wohnort einer Person, ihre Hobbys und Interessen. Aber auch Daten wie die Entwicklung der Arbeitsleistung, wirtschaftliche Verhältnisse oder Angaben über den Gesundheitszustand eines Menschen gehören dazu.

Von «Profiling mit hohem Risiko» spricht man, wenn ein Profiling ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte (z.B. Wesenszüge) einer natürlichen Person erlaubt. Mit hoher Sensibilität verarbeitet werden dürfen solche Daten künftig zwar weiterhin, aber nur, wenn sie die Persönlichkeitsrechte nicht ausdrücklich verletzen und eine ausdrückliche Einwilligung der betroffenen Person vorliegt.

- **Datenschutz durch Technik und datenschutzfreundliche Voreinstellung (Art. 7 DSG)**

Unter dem Grundsatz des «Datenschutzes durch Technik (Privacy by Design)» versteht man, dass die für die Bearbeitung von Personendaten genutzten Systeme von Anfang an so zu gestalten sind, dass der Datenschutz eingehalten werden kann.

Unter dem Grundsatz der «datenschutzfreundlichen Voreinstellungen (Privacy by default)» versteht man, dass die Verantwortlichen die Standardeinstellungen an der Software bzw. am Gerät so zu wählen haben, dass die Bearbeitung von Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist (es dürfen nur die für den Dienst zwingend notwendigen Cookies gesetzt werden). Sämtliche Software, Hardware sowie die Dienstleistungen müssen so konfiguriert sein, dass die Daten geschützt sind und die Privatsphäre der Nutzer gewahrt wird.

- **Cookies**

Das neue Datenschutzgesetz in der Schweiz bringt kein Obligatorium für Cookie-Banner, aber eine Informationspflicht über die Verwendung von Cookies (Cookie Banner oder auch Cookie Layer sind Werkzeuge, die auf Webseiten und in Apps eingesetzt werden, um die Einwilligung von Nutzern zur Datenverarbeitung einzuholen. Mit einem solchen Banner sollen Nutzer in der Lage sein, Cookies gezielt annehmen oder ablehnen zu können). Die Schweiz übernimmt somit nicht die EU-Cookie-Richtlinie. Somit ist es grundsätzlich rechtskonform, wenn man auf Schweizer Webseiten keinen Cookie Banner einrichtet.

Allerdings sind Schweizer Webseiten-Betreiber zwingend verpflichtet, über die Verwendung von Cookies zu informieren, können diese aber generell ohne explizite Zustimmung anlegen.

Falls jedoch ein EU-Traffic auf der Webseite generiert wird - d.h. Produkte/Dienstleistungen auch Personen aus der EU angeboten werden - dann muss zwingend ein Banner eingerichtet werden. um der DSGVO zu entsprechen (vgl. Ziff. 3). In Zweifelsfällen wird empfohlen, einen entsprechenden Banner zu schalten (z.B. in Fällen von Grenzgängern oder internationalen Kongressen).

- **Informationspflicht bei der Beschaffung von Personendaten, Datenschutzerklärung (Art. 19 DSG)**

Die Informationspflicht wird gegenüber dem bisherigen Recht ausgebaut. Neu müssen Verantwortliche die betroffenen Personen über jede Datenbeschaffung angemessen informieren, nicht wie bisher nur die besonders schützenswerten Daten.

Das neue Datenschutzgesetz enthält keine abschliessende Liste aller Pflichtinformationen, die der betroffenen Person bei der Beschaffung mitgeteilt werden müssen. Mindestens mitzuteilen sind folgende Pflichtangaben:

- Die Identität und die Kontaktdaten des Verantwortlichen im Unternehmen/Verband bzw. des Selbständigen, der die Daten bearbeitet/verarbeitet
- Die Bearbeitungszwecke
- Bei einer Bekanntgabe von Daten: die Empfänger bzw. Kategorien von Empfänger
- bei einer Datenbekanntgabe ins Ausland zusätzlich: der Staat oder das internationale Organ und ggf. die Garantie für einen geeigneten Datenschutz oder den Ausnahmetatbestand, falls keine solchen Garantien gegeben sind
- bei indirekten Datenerhebung (d.h. Daten, die nicht bei der betroffenen Person selbst erhoben werden, zusätzlich: die Kategorien der bearbeiteten Personendaten)
- die Durchführung automatisierter Einzelentscheidungen, d.h. eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.

Auf welche Art und Weise die Informationen gegenüber der betroffenen Person zu erfolgen hat, wird im DSG nicht geregelt. Es gilt kein gesetzliches Formerfordernis, aber eine angemessene Form ist zu wählen, welche dem Zweck einer transparenten Datenbearbeitung gerecht wird. Hierzu empfiehlt sich eine entsprechende Datenschutzerklärung auf der Webseite.

Das Kontaktformular der Webseite muss zwingend den Hinweis enthalten, für welchen Zweck die angegebenen Personendaten genutzt werden.

- **Verzeichnis der Bearbeitungstätigkeiten (nur) in bestimmten Fällen (Art. 12 DSG)**

Organisationen mit 250 Mitarbeitenden und mehr müssen ein Inventar über sämtliche Bearbeitungen führen.

Organisationen mit weniger als 250 Mitarbeitenden (d.h. kleinere Organisationen/Selbständige) müssen ein solches nur dann führen, wenn sie besonders schützenswerte Personendaten (z.B. Gesundheitsdaten) bearbeiten.

In diesem Fall muss der Verantwortliche ein Verzeichnis über sämtliche Bearbeitungstätigkeiten führen. Wird die Datenbearbeitung an einen Auftragsbearbeiter delegiert, müssen der Verantwortliche und der Auftragsbearbeiter je ein separates Verzeichnis führen:

- Das Verzeichnis des Verantwortlichen enthält Angaben über die

- Identität des Verantwortlichen
- den Bearbeitungszweck
- eine Beschreibung der Kategorien betroffener Personen
- der Kategorien bearbeiteter Personendaten
- die Kategorien der Empfänger
- wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer
- wenn möglich eine allgemeine Beschreibung der TOMs (Technische und organisatorische Massnahmen)
- und, falls Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Art. 16 Abs. 2 DSG.

- Das Verzeichnis des Auftragsbearbeiters enthält hingegen «nur» Angaben:

- zur Identität des Auftragsbearbeiters und des Verantwortlichen
- zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden,
- sowie die Angaben zu den TOMs und im Fall von Datenaustausch ins Ausland Angaben zum Staat

Zu den Personendaten, die beispielsweise in Arzt- oder Zahnarztpraxen bearbeitet werden, gehören unter anderem: Stamm- und Kontaktdaten von Patienten, Mitarbeitenden, Ansprechpersonen von Dienstleistern oder anderen Gesundheitseinrichtungen (z.B. Namen, Telefonnummer, Anschrift, E-Mail-Adresse oder auch das Geburtsdatum); Aufzeichnungen über den Verlauf einer Behandlung, Symptombeschreibungen, Diagnosen, Verordnungen, Reaktionen, Laborresultate,
Röntgenbilder, Medikationen, Daten über Intimsphäre wie etwa der Gesundheitszustand, das Sexualleben oder die Gefühlswelt, Daten zu Mitarbeitenden und dem Anstellungsverhältnis inklusive Leistungsbeurteilungen und Lohnabrechnungen (letztere sind auch für interne HR-Verantwortliche relevant).

- **Ausbau der Betroffenenrechte: Recht auf Datenherausgabe (Art. 25 DSG)**

Neben der Informationspflicht werden auch die Rechte der Betroffenen im DSG weiter ausgebaut. Neu wird ähnlich wie in der DSGVO ein Recht der betroffenen Person auf Datenherausgabe und -übertragung statuiert. Betroffene Personen können verlangen, dass die von ihnen bekanntgegebenen Daten in einem gängigen elektronischen Format herausgegeben werden (innerhalb von 30 Tagen).

In jedem Fall werden folgende Informationen mitgeteilt:

- die Identität und Kontaktdaten des Verantwortlichen
- die bearbeiteten Personendaten als solche

- die Bearbeitungszwecke
- die Aufbewahrungsdauer
- die verfügbaren Angaben über die Herkunft der Personendaten

Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig.

Es wird empfohlen, eine Vorgehensweise für eine rasche Beantwortung möglicher Anfragen betroffener Personen vorzubereiten.

- **Meldung von Verletzungen an EDÖB (Art. 24 DSG)**

Nach dem neuen DSG müssen Verantwortliche eine Verletzung der Datensicherheit (z.B. Datenverlust, Cyberangriff), die zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen können, so rasch als möglich dem EDÖB (Eidg. Datenschutz- und Öffentlichkeitsbeauftragter) und allen potenziell betroffenen Parteien melden, um Sanktionen oder andere Komplikationen zu vermeiden.

- **Datenschutzberaterin oder -berater (Art. 10 DSG)**

Private Unternehmen können fakultativ nach Art. 10 DSG eine Datenschutzberaterin oder einen Datenschutzberater ernennen. Diese können, müssen aber nicht in einem arbeitsvertraglichen Verhältnis zum Unternehmen stehen.

Datenschutzberatern und -beraterinnen muss es erlaubt sein, ihren Standpunkt bei Meinungsverschiedenheiten der Unternehmensleitung zur Kenntnis zu bringen. Die Verantwortlichkeiten bei Datenschutz und Informationssicherheit können bzw. müssen in jedem Unternehmen unabhängig von der Einsetzung eines Datenschutzberaters im Sinn von Art. 10 DSG geregelt werden.

Falls eine Datenschutzberaterin/Datenschutzberater bestellt wird, muss deren/dessen Name und Kontaktdaten in der Datenschutzerklärung angegeben werden.

- **Strafbarkeit / Bussen**

In Bezug auf die Strafbarkeit ist insbesondere zu berücksichtigen, dass ab dem 1. September 2023 die Verletzung gewisser Pflichten eine Strafbarkeit begründet, welche nicht das Unternehmen trifft, sondern die dafür verantwortliche natürliche Person. Die verantwortlichen Personen können sowohl Mitglieder der Geschäftsleitung als auch andere entscheidungsbefugte Personen im Unternehmen oder aber auch diejenigen Personen sein, welche eine Pflichtverletzung (z.B. Verletzung der Geheimhaltung) begangen haben. Im Schweizer Recht ist jedoch nur die vorsätzliche Begehung strafbar.

Bei Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 60 DSG) oder Verletzung von Sorgfaltspflichten (Art. 61 DSG) können Personen mit bis zu Fr. 250.000.-- gebüsst werden. Lediglich die vorsätzliche Begehung ist umfasst, nicht auch Fahrlässigkeit. Vorsatz ist die Ausführung der Tat mit Wissen und Willen. Vorsätzlich handelt bereits, wer die Verwirklichung der Tat für möglich hält und in Kauf nimmt (sog. Eventualvorsatz).

- **Haftung (zu unterscheiden von der strafrechtlichen Busse)**

Wie bereits im bestehenden DSG, aber im Unterschied zur DSGVO, haftet nicht das Unternehmen für die Verletzung des nDSG, sondern die für die Verletzung verantwortliche natürliche Person innerhalb des Unternehmens.

Die Botschaft zum neuen DSG stellt jedoch klar, dass hierbei nicht auf den Handlungsverantwortlichen abgestellt wird, sondern auf den Organisationsverantwortlichen. Die Haftung von Leitungspersonen wird mit dem Verweis auf Art. 6 VStrR in Art. 64 nDSG verdeutlicht. Nur so kann sichergestellt werden, dass Personen in Führungspositionen für die Verletzungen haften und nicht der frisch eingestellte Angestellte.

4. Empfehlungen

- Überprüfung der (vorhandenen) Einstellungen zu «Datenschutz durch Technik» und «datenschutz-freundliche Voreinstellung» inkl. Cookies gemäss Seiten 3/4.
- Überprüfung und Anpassung der Datenschutzerklärung(en) auf der Webseite gem. Seite 4.
- Überprüfung, dass alle Auftragsbearbeitungen durch Dritte vertraglich abgesichert sind
- Überprüfung der organisatorischen Verantwortlichkeiten für den Datenschutz
- Erstellung eines Verarbeitungsverzeichnisses, sofern ein solches notwendig ist (S. 4/ 5).
- Definition der Prozesse zur Bearbeitung von Auskunfts-, Berichtigungs- und Löschungsbegehren und von Widersprüchen zur Datenbearbeitung (Seite 6)
- Definition der Prozesse zur Meldung von Verletzungen der Datensicherheit (vgl. Seite 6)
- Definition der Prozesse zur Löschung und Archivierung von Daten
- Information der betroffenen Mitarbeitenden über ihre berufliche Schweigepflicht