

# Neuerungen im Datenschutzgesetz

Andrea Giroud-Kaiser, Rechtsanwältin und Mediatorin SAV, Juni 2023

**Im Hinblick auf die Inkraftsetzung des neuen Datenschutzgesetzes und den dazugehörigen Verordnungen rechtfertigt sich ein kurzer Überblick über die relevanten Neuerungen sowie der Hinweis auf den möglichen Handlungsbedarf bei Personen oder Unternehmen, welche Personendaten von natürlichen Personen bearbeiten.**

## 1. Ausgangslage

In der Herbstsession 2020 hat das Eidgenössische Parlament das totalrevidierte Bundesgesetz über den Datenschutz (nDSG) sowie weitere, geänderte Erlasse zum Datenschutz verabschiedet. Der Bundesrat hat am 31. August 2022 entschieden, das neue Gesetz und die dazugehörigen Verordnungen auf den 1. September 2023 in Kraft zu setzen.

Das nDSG soll den Datenschutz den technologischen Entwicklungen anpassen und das schweizerische Datenschutzniveau dem europäischen Standard annähern.

## 2. Übersicht über die wichtigsten Änderungen

- Nur noch die Daten **natürlicher Personen** sind künftig vom nDSG erfasst; nicht aber jene von juristischen Personen (Art. 1 f. nDSG).
- **Genetische** und **biometrische Daten** werden in die Definition der besonders schützenswerten Daten aufgenommen (Art. 5 Bst. c nDSG).
- Die Grundsätze "**Privacy by Design**" und "**Privacy by Default**" werden eingeführt und integrieren den Datenschutz bereits in die Planung.

Privacy by Design / Datenschutz durch Technik (Art. 7 Abs. 1 nDSG): Grundgedanke dieses Prinzips ist es, den Schutz der Personendaten präventiv in der

technischen und organisatorischen Konzeption von Verarbeitungs-Systemen anzulegen. Adressat der Rechtsnorm ist der Verantwortliche (und der Auftragsbearbeiter). Welche Massnahmen zu ergreifen sind, ist anhand des Risikos, der Wirksamkeit der Massnahme, des Stands der Technik und des Aufwands festzulegen, wobei das Kostenargument selten von Massnahmen dispensiert. Beispiele möglicher Massnahmen sind: Datenminimierung, Pseudonymisierung, Datentrennung nach Zeck, selektiver Passwortschutz, Löschkonzept, verpixeln von Bilddaten etc.

Privacy by Default / Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 7 Abs. 3 nDSG): Dieser Grundsatz bezieht sich auf die datenschutzrelevanten Voreinstellungen bei Internet-Anwendungen bzw. mobilen Apps. Dabei wird der Verantwortliche verpflichtet mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt. Es soll verhindert werden, dass eine betroffene Person, welche ihre Voreinstellungen nicht ändert, hinsichtlich des Datenschutzes benachteiligt wird (z.B. muss die Zustimmung zur Verwendung der Personendaten für Werbezwecke aktiv angekreuzt werden).

- **Folgenabschätzungen** müssen durchgeführt werden, sofern ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht.

Bei der Datenschutz-Folgenabschätzung (Art. 22 nDSG) handelt es sich um eine strukturierte Risikoanalyse bezüglich eines geplanten Datenverarbeitungsprozesses. Es soll gewährleistet werden, dass die Verantwortlichen die Risiken „riskanter“ Verarbeitungsprozesse in Bezug auf die Privatsphäre und den Datenschutz angemessen berücksichtigen.

- Die **Informationspflicht wird ausgeweitet** (Art. 19 ff. nDSG). Bei jeder Beschaffung von Personendaten – und nicht mehr nur

von sogenannten besonders schützenswerten Daten – muss die betroffene Person vorläufig informiert werden.

- Ein **Verzeichnis der Bearbeitungstätigkeit** wird obligatorisch (Art. 12 nDSG). Ausgenommen von dieser Regel sind Unternehmen mit weniger als 250 Mitarbeitenden, falls deren Datenbearbeitung ein geringes Risiko für Verletzungen der Persönlichkeit der betroffenen Person mit sich bringt (Art. 24 nDSV).
- Das **Recht** einer betroffenen Person, **Auskunft** darüber zu verlangen, ob Personendaten über sie bearbeitet werden, wird ausgebaut (Art. 25 ff. und 28 nDSG).
- Eine **rasche Meldung** ist erforderlich, wenn die Datensicherheit verletzt wurde (Art. 24 nDSG). Die Verletzungen sind an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu richten, wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Betroffenen führt. In der Regel muss der Verantwortliche auch eine Meldung an die betroffenen Personen machen, wenn dies zu deren Schutz nötig ist oder der EDÖB dies verlangt.
- Der Begriff **Profiling** (die automatisierte Bearbeitung personenbezogener Daten, Art. 5 Bst. f nDSG) wurde ins nDSG aufgenommen.
- Die **Sanktionen** werden neu geregelt (Art. 60 ff. nDSG).
- Sind die entsprechenden Prozesse zur Datenbearbeitung zu optimieren und/oder zu ergänzen (z.B. durch Datenschutz-Folgenabschätzungen, Verzeichnis über die Datenbearbeitungstätigkeit etc.)?
- Verfügt das Unternehmen über eine dem nDSG entsprechende Dokumentation (u.a. Datenschutzerklärung)?
- Sind die technischen und organisatorischen Vorkehrungen ausreichend, um die Datensicherheit zu gewährleisten und wird dem Prinzip der datenfreundlichen Voreinstellungen Rechnung getragen)?

### 3. Handlungsbedarf / Checkliste

Unternehmen, welche Personendaten von natürlichen Personen bearbeiten, werden im Hinblick auf das Inkrafttreten des nDSG und den dazugehörigen Verordnungen **intern folgendes klären müssen:**

- Bearbeitet das Unternehmen Personendaten natürlicher Personen?
- Werden im Unternehmen die Vorgaben des nDSG durch geeignete Prozesse eingehalten?