

Das neue Datenschutzgesetz (revDSG)

Am 1. September 2023 tritt in der Schweiz das neue Datenschutzgesetz (DSG) in Kraft. Ab diesem Zeitpunkt müssen die Planenden die Bearbeitung von Personendaten an die neuen Bestimmungen anpassen, unabhängig davon, ob sie als Aktiengesellschaft oder Einzelfirma organisiert sind.

Was sind die Ziele der Revision?

Ziel des revidierten DSG ist es, den Datenschutz an die technologischen und gesellschaftlichen Entwicklungen (Cloud-Computing, Big Data, soziale Netzwerke und Internet der Dinge) anzupassen.

Ein weiteres Anliegen besteht darin, ein Datenschutzniveau zu gewährleisten, das dem der Europäischen Union gleichwertig ist. Planende in der Schweiz sollen weiterhin Daten mit europäischen Unternehmen austauschen können und nicht Gefahr laufen, ihre Wettbewerbsfähigkeit zu verlieren.

Was sind die wichtigsten Veränderungen?

1. Daten natürlicher Personen (Art. 5 Bst. b revDSG)

Durch das revidierte DSG werden künftig nur noch die Daten von Privatpersonen geschützt, jedoch nicht mehr die Daten von juristischen Personen (Aktiengesellschaften (AG), Gesellschaften mit beschränkter Haftung (GmbH), Vereine, Stiftungen etc.).

2. Besonders schützenswerte Personendaten (Art. 5 Bst. c Ziff. 3 und 4 revDSG)

Mit dem neuen Gesetz wird die Definition der «besonders schützenswerten Personendaten» um genetische Daten und, sofern diese eine natürliche Person eindeutig identifizieren, biometrische Daten erweitert.

3. Aufnahme der Grundsätze «Privacy by Design» und «Privacy by Default» (Art. 7 revDSG)

Der Grundsatz «Privacy by Design» (Datenschutz durch Technik) verpflichtet den Verantwortlichen, die Grundsätze nach Art. 6 des revidierten DSG bereits ab der Planung umzusetzen, indem er angemessene technische und organisatorische Schutzmassnahmen trifft. Dabei geht es insbesondere um die Vernichtung oder Anonymisierung der Daten, die zum Zweck der Bearbeitung nicht mehr erforderlich sind.

Der Grundsatz «Privacy by Default» (Datenschutz durch datenschutzfreundliche Voreinstellungen) stellt sicher, dass die Bearbeitung von Personendaten standardmässig, d. h. ohne Eingreifen der Nutzenden, auf das für den Verwendungszweck nötige Mindestmass beschränkt wird.

Durch die Anwendung dieser beiden Grundsätze wird somit gewährleistet, dass die Bearbeitung der Daten ab der Planung und standardmässig im Einklang mit dem revidierten Gesetz erfolgt.



4. Datenschutzberaterin oder -berater (Art. 10 revDSG)

Art. 10 des revidierten DSG bietet den Planenden die Möglichkeit, eine Datenschutzberaterin oder einen Datenschutzberater zu ernennen (fakultativ). Die Datenschutzberaterin oder der Datenschutzberater ist nicht nur eine innerbetriebliche Anlaufstelle, sondern fungiert auch als Bindeglied zu der Schweizer Datenschutzbehörde.

5. Datenschutz-Folgenabschätzung (Art. 22 revDSG)

Datenschutz-Folgenabschätzungen sind zu erstellen, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann und es keinen Grund gibt, von der Erstellung einer solchen Folgenabschätzung abzusehen. Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Ein solches Risiko besteht insbesondere dann, wenn ein Profiling mit hohem Risiko oder eine umfangreiche Bearbeitung besonders schützenswerter Personendaten geplant ist.

6. Verzeichnis der Bearbeitungstätigkeiten (Art. 12 revDSG)

Das Führen eines Verzeichnisses der Bearbeitungstätigkeiten ist künftig obligatorisch. Art. 12 Abs. 2 des revidierten DSG nennt die Mindestangaben, die in diesem Verzeichnis zwingend enthalten sein müssen. Die Verordnung zum Gesetz sieht jedoch eine Ausnahme für Unternehmen und andere privatrechtliche Organisationen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt. Falls Daten ins Ausland bekanntgegeben werden sollen, ist auch eine Angabe der Staaten sowie der Datenschutzgarantien (z. B. die Standardvertragsklauseln der Europäischen Kommission) erforderlich.

7. Erweiterte Informationspflicht (Art. 19 revDSG)

Künftig muss der Verantwortliche die betroffene Person vorgängig angemessen über die Beschaffung von Personendaten im Allgemeinen und nicht mehr nur über die Beschaffung von besonders schützenswerten Daten informieren. Diese Informationspflicht gilt auch dann, wenn die Daten nicht bei der betroffenen Person beschafft werden. Der bzw. die Planende ist verpflichtet, der betroffenen Person mindestens die Identität und die Kontaktdaten des Verantwortlichen, den Bearbeitungszweck und gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, mitzuteilen.

Werden die Daten nicht bei der betroffenen Person beschafft, so teilt der oder die Planende ihr zudem die Kategorien der bearbeiteten Personendaten mit.

Werden die Personendaten ins Ausland bekanntgegeben, so teilt der oder die Planende der betroffenen Person auch den Staat oder das internationale Organ mit.

8. Auskunftsrecht der betroffenen Person (Art. 25 revDSG)

Auf entsprechendes Verlangen teilt der Verantwortliche der betroffenen Person, in der Regel innerhalb von 30 Tagen, diejenigen Informationen mit, die erforderlich sind, damit die Person die ihre nach dem revidierten DSG zustehenden Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Dabei handelt es sich insbesondere um die Identität und die Kontaktdaten des Verantwortlichen, die bearbeiteten Personendaten als solche, den Bearbeitungszweck und die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer.

Der Verantwortliche muss kostenlos Auskunft erteilen. Der Bundesrat kann Ausnahmen vorsehen, namentlich wenn der Aufwand unverhältnismässig ist.



9. Meldung von Verletzungen der Datensicherheit (Art. 24 revDSG)

Eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, ist dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) rasch zu melden.

Checkliste der zu ergreifenden Massnahmen

- Erfassen der beschafften privaten Daten und Bewertung der Risiken für die Rechte und Freiheiten der natürlichen Personen.
- Angemessene Information der betroffenen Person ab der Beschaffung über die Bearbeitung ihrer Personendaten. Diese Informationen können insbesondere durch die Veröffentlichung einer Datenschutzerklärung zur Einsichtnahme durch die betroffenen Personen, durch Vertragsdokumente oder auch mündlich mitgeteilt werden. ¹

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ² (EDÖB) empfiehlt, dass die Informationen zumindest Antworten auf die folgenden Fragen liefern sollten:

- Wer ist verantwortlich für die Datenbearbeitung?
 - Welche Personendaten werden gesammelt?
 - Zu welchen Zwecken werden die gesammelten Personendaten bearbeitet?
 - Wie lange werden diese gesammelten Personendaten aufbewahrt?
 - Welche Wahlmöglichkeiten zur Bearbeitung ihrer Daten stehen den Nutzenden zu?
 - Welche Daten werden an Dritte weitergegeben und für welche Zwecke?
 - Welche Dienstleistungen oder Produkte insb. auch von Dritten werden eingebunden und wie können die Nutzenden der damit verbundenen Datenübermittlung widersprechen?
 - Über welche Kontaktadresse können Fragen zur Datenbearbeitung gestellt werden bzw. wo können Datenschutzrechte (z. B. Auskunft, Berichtigung, Löschung, Widerspruch, Portabilität) geltend gemacht werden?
 - Welchen Gesetzen untersteht die Datenbearbeitungspraxis des Anbieters?
- Gewährleistung von Datenschutz durch Technik («Privacy by Design») und durch datenschutzfreundliche Voreinstellungen («Privacy by Default»).
 - Ernennung einer internen Datenschutzberaterin oder eines Datenschutzberaters oder Beauftragung einer externen Stelle.
 - Einführen interner Datenschutzrichtlinien oder -regeln. Diese Massnahmen sollten es den Planenden ermöglichen, schnell auf Anfragen von betroffenen Personen zu ihren Daten zu reagieren und mit Verletzungen der Datensicherheit adäquat umzugehen.

¹ CHARLET François, Protection des données en entreprise, Basel 2023, S. 65

² www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeit_wirtschaft/datenschutzerklaerung.html



- Erstellen eines Verzeichnisses der Datenbearbeitungstätigkeiten, wenn der oder die Planende hierzu verpflichtet ist.
- Überprüfung der aktuellen Verträge auf ihre Übereinstimmung mit dem revidierten DSG.
- Ergreifen angemessener Sicherheitsmassnahmen, einschliesslich derer Aktualisierungen.

Schlussfolgerung

Die Revision des Datenschutzgesetzes wird dafür sorgen, dass die Bearbeitung von Personendaten ab dem Zeitpunkt ihrer Beschaffung transparenter wird. Wir empfehlen den Planenden, bis zum 1. September 2023, dem Datum des Inkrafttretens des revidierten DSG, interne Massnahmen zu ergreifen, um die Transparenz der Bearbeitung von Personendaten gemäss den gesetzlichen Bestimmungen zu gewährleisten. Um auch den zusätzlichen Aufwand in Grenzen zu halten, sollten diese Massnahmen zudem eine Erleichterung des Verfahrens im Zusammenhang mit Auskunftersuchen der betroffenen Personen ermöglichen. Abschliessend weisen wir die Planenden auf das neue Sanktionssystem des revidierten DSG hin. Demnach droht privaten Personen, die gegen Bestimmungen des Bundesgesetzes über den Datenschutz verstossen, künftig eine Busse von bis zu 250'000 Franken (Art. 60 ff. revDSG).