Dachverband gemeinnütziger Stiftungen der Schweiz

DSG-Checkliste: Welche Dokumente müssen nach neuem Datenschutzgesetz erstellt werden?

Die Totalrevision des Datenschutzgesetzes wurde am 25. September 2020 nach langem Hin und Her von den Eidg. Räten beschlossen. Zurzeit wird noch die Verordnung ausgearbeitet. Am 1. September 2023 soll das neue Datenschutzgesetz (nDSG) schliesslich in Kraft treten. Dieses Datum ist für alle Datenbearbeiter von grosser Bedeutung, denn für die Umsetzung der gesetzlichen Vorgaben ist keine Übergangsfrist vorgesehen. Beim Inkrafttreten müssen also alle gesetzlichen Vorgaben bereits umgesetzt sein.

Nachfolgend finden Sie eine Übersicht der wichtigsten Dokumente.

1. Gesetzlich vorgeschriebene Dokumente

1.1. Die Datenschutzerklärung (Erfüllung der Informationspflicht)

Das Erstellen einer Datenschutzerklärung wird vom Gesetz zwar nicht ausdrücklich verlangt, es ist aber der einfachste Weg, der gesetzlich vorgeschriebenen Informationspflicht nachzukommen. Gemäss Art. 19 nDSG muss der für die Datenverarbeitung Verantwortliche die Person, deren Daten bearbeitet werden, nämlich angemessen über die Beschaffung der Personendaten informieren. Diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

Dabei sind der betroffenen Person bei der Beschaffung diejenigen Informationen mitzuteilen, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.

Mittels Datenschutzerklärung wird die betroffene Person einerseits über die Datenbearbeitung an sich und andererseits über ihre Rechte aus dem Datenschutzgesetz informiert. Dabei gilt es die gesetzlichen Mindestanforderungen gemäss Art. 19 Abs. 2 nDSG zu beachten. So sind die Identität und die Kontaktdaten des Verantwortlichen und der Bearbeitungszweck anzugeben. Gegebenenfalls sind die Empfängerinnen oder die Kategorien von Empfängerinnen, denen Personendaten bekanntgegeben werden, zu nennen.

Da es sehr wichtig ist, die gesamte Datenbearbeitung klar und transparent darzulegen und auch den Bearbeitungszweck klar zu nennen, muss eine Datenschutzerklärung der effektiven Datenbearbeitung entsprechen. Es empfiehlt sich daher, genau zu prüfen, was es an Informationen in der Datenschutzerklärung

braucht. Wir empfehlen Ihnen daher, sich in dieser Angelegenheit von einem Experten beraten zu lassen. proFonds erteilt Ihnen gerne Auskünfte und vermittelt Ihnen einen Experten.

1.2. Die Datenschutz-Folgenabschätzung

Bei der Datenschutz-Folgenabschätzung (Art. 22 nDSG) handelt es sich um ein präventives Risikomanagement-Instrument. Also ein Dokument, das die Einschätzung ermöglichen soll, ob die geplante Datenbearbeitung ein Risiko darstellen könnte.

Der Verantwortliche soll die aus seiner Bearbeitung resultierenden Risiken vorgängig erkennen und entsprechende Gegenmassnahmen definieren, sofern eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann. Ob ein hohes Risiko vorliegt, ist im Einzelfall zu überprüfen und hängt von verschiedenen Faktoren ab (Art der bearbeiteten Daten, Umfang und Dauer der Datenbearbeitung).

Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Ein solches ist insbesondere anzunehmen, wenn umfangreich besonders schützenswerte Daten bearbeitet oder systematisch umfangreiche öffentliche Bereiche überwacht werden besonders schützenswerte Daten sind bspw. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten, Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen sowie Daten über Massnahmen der sozialen Hilfe.

Die Datenschutz-Folgenabschätzung enthält 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.

1.3. Das Verarbeitungsverzeichnis

Der Verantwortliche wie auch alle Auftragsbearbeiter sind gemäss Art. 12 nDSG verpflichtet, je ein Verzeichnis über ihre Bearbeitungstätigkeiten zu führen.

Das Verarbeitungsverzeichnis ist eine generelle Beschreibung der Bearbeitungstätigkeiten und keine Liste von konkreten Datenbearbeitungen. Auch hier stellt das Gesetz Mindestanforderungen auf.

Keine Pflicht zur Führung eines Verarbeitungsverzeichnisses haben Unternehmen, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt. Gemäss E-VDSG ist von einer solchen Datenbearbeitung mit geringfügigen Risiken auszugehen, wenn nicht umfangreich besonders schützenswerte Personendaten bearbeitet werden und kein

Profiling mit hohem Risiko (für die Grundrechte der betroffenen Person) durchgeführt wird. Von einem solchen hohen Risiko spricht man, es zu einer Verknüpfung von Daten kommt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

2. Verordnungsrechtliche Vorgaben

2.1. Das Bearbeitungsreglement

Das nDSG sieht keine Pflicht zur Erstellung eines Bearbeitungsreglements vor. Eine solche soll aber auf Verordnungsebene (Art. 4 E-VDSG) eingeführt werden.

Demnach müssen der Verantwortliche wie auch alle Auftragsbearbeiter dann ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie umfangreich besonders schützenswerte Personendaten bearbeiten oder wenn sie ein Profiling mit hohem Risiko durchführen.

Das Reglement muss mindestens folgende Angaben enthalten: Bearbeitungszweck; Kategorien betroffener Personen, Kategorien bearbeiteter Personendaten, Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer, Herkunft der Personendaten, Art ihrer Beschaffung, technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit, Zugriffsberechtigungen, Art und Umfang der Zugriffe, Massnahmen zur Datenminimierung, Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung, Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.

Ob die Pflicht zur Führung eines Bearbeitungsreglements trotz fehlender gesetzlicher Grundlage in der Verordnung bleibt, ist derzeit noch unklar.

3. Empfohlene Dokumente

3.1. Das Auskunftsformular

Gemäss Art. 25 nDSG kann jede betroffene Person vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Welche Informationen in welchem Fall mitgeteilt werden müssen, definiert das Gesetz in Art. 25 Abs. 2 nDSG.

Selbst wenn ein Auskunftsformular gesetzlich nicht vorgeschrieben ist, empfiehlt es sich, ein solches zu erstellen, um durch standardisierte Auskunftserteilungen effizientere interne Abläufe zu ermöglichen.

3.2. Vertrag über die Auftragsbearbeitung Gewährleistung eines angemessenen Datenschutzes

Gemäss Art. 9 nDSG kann die Bearbeitung von Personendaten einem Auftragsbearbeiter übertragen werden (sog. Auftragsbearbeitung). Wird die Datenbearbeitung an einen Dritten delegiert, bleibt der Verantwortliche, der die Bearbeitung von Personendaten dem Auftragsbearbeiter überträgt, für den Datenschutz verantwortlich. Aus diesem Grund darf eine Auftragsbearbeitung auch nur dann erfolgen, wenn die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Des Weiteren muss er sicherstellen, dass der Auftragsbearbeiter dem DSG oder einem ausländischen Gesetz untersteht, das einen gleichwertigen Datenschutz gewährleistet. Ist dies nicht der Fall, so muss der Verantwortliche den Datenschutz durch die Ausgestaltung des Vertrags (Abgabe von Garantien oder Verwendung von Standardvertragsklauseln) sicherstellen.

Der Anhang 1 zum E-VDSG enthält eine Liste mit Staaten, welche einen angemessenen Datenschutz gewährleisten. Diese Liste wird periodisch überprüft. Staaten ohne angemessenen Datenschutz werden entfernt. Für Verantwortliche, die ihre Datenbearbeitung an einen Dritten mit Sitz im Ausland delegieren, empfiehlt sich eine regelmässige Kontrolle dieser Liste.

Für weitere Informationen stehen wir Ihnen gern zur Verfügung.

proFonds, Dachverband gemeinnütziger Stiftungen der Schweiz
Tel. 061 272 10 80
info@proFonds.org
www.proFonds.org