Revision des Datenschutzgesetzes: Wichtigste Neuerungen

A. Einleitung

Ende September 2020 hat das Parlament nach mehrjähriger Diskussion die Revision des Datenschutzgesetzes (DSG) abgeschlossen. Das Konzept des bisherigen Gesetzes wurde beibehalten, die Revision führt aber zu etlichen Neuerungen aufgrund des technologischen Wandels und zwecks Angleichung an das Datenschutzrecht der EU (Datenschutzgrundverordnung; DSGVO).

Das revidierte DSG und die zur Zeit noch in Überarbeitung befindliche Verordnung (VDSG) werden voraussichtlich im Laufe des Jahres 2022 in Kraft treten.

Das DSG regelt wie bisher die Bearbeitung von Personendaten. Der Begriff «Datenbearbeitung» ist weit gefasst zu verstehen und umfasst insbesondere das Beschaffen, Erfassen, Organisieren, Abfragen, Analysieren, Auswerten, Verändern, Weitergeben, Speichern, Archivieren und Vernichten von Personendaten.

B. Die wichtigsten Neuerungen im Überblick

1. Anwendungsbereich

In *räumlicher* Hinsicht gilt neu das sog. «Auswirkungsprinzip». Das DSG ist somit auch auf Datenbearbeitungen im Ausland anwendbar, die sich in der Schweiz auswirken. Liefert z. B. ein Unternehmen aus Deutschland Waren an eine Kundin in der Schweiz, unterliegt die Bearbeitung ihrer Personendaten dem schweizerischen Recht.

In *persönlicher* Hinsicht gilt das neue DSG nur noch für die Bearbeitung von Personendaten *natürlicher Personen*. Die Bearbeitung von Daten juristischer Personen (z. B. Stiftungen, Vereine, AG, Genossenschaften) bzw. deren Schutz fällt neu nicht mehr darunter[1].

2. Grundsätze der Bearbeitung von Personendaten

Wie bisher müssen Personendaten rechtmässig, nach Treu und Glauben und verhältnismässig bearbeitet werden. Sie dürfen weiterhin nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft und nur im Rahmen dieses Zwecks bearbeitet werden. Die Richtigkeit der bearbeiteten Daten und deren Sicherheit durch geeignete technische und organisatorische Massnahmen müssen gewährleistet sein. Neu ist der Datenschutz technisch insbesondere durch geeignete Voreinstellungen sicherzustellen und auf das für den Bearbeitungszweck nötige Minimum zu beschränken.

[1] Den Schutz juristischer Personen stellen andere Gesetze sicher, z. B. der zivilrechtliche Persönlichkeitsschutz (Art. 27 ff. ZGB), das Urheberrechtsgesetz (URG) oder das Bundesgesetz gegen den unlauteren Wettbewerb (UWG).

Neu wird ausdrücklich geregelt, was bereits bisher galt: Personendaten sind zu vernichten oder zu anonymisieren, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. – Erforderlich sind sie weiterhin insbesondere so lange, wie dies gesetzlichen Aufbewahrungspflichten verlangen.

Neu ist auch folgende Pflicht: Wenn eine beabsichtigte Datenbearbeitung ein hohes Risiko einer Verletzung der Persönlichkeit oder der Grundrechte der betroffenen Person mit sich bringt, müssen deren Risiken vorgängig durch die/den für den Datenschutz Verantwortliche/n analysiert werden.

3. Besonders schützenswerte Personendaten

Wie *bisher* fallen darunter die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen und Sanktionen.

Neu gelten auch Daten über die Ethnie, genetische Daten sowie biometrische Daten (z. B. DNA, Fingerabdrücke), die eine natürliche Person eindeutig identifizieren, als besonders schützenswert.

Die Bearbeitung besonders schützenswerter Personendaten (z. B. die Nutzung von Informationen aus einem ärztlichen Bericht) ist (weiterhin) nur mit ausdrücklicher Einwilligung der betroffenen Person zulässig. Dies gilt auch bei «Profiling» mit hohem Risiko, d.h. jeder Art der *automatisierten* Bearbeitung von Personendaten, um sie zu dafür zu verwenden, bestimmte persönliche Aspekte (z. B. bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Aufenthaltsort) zu analysieren oder vorherzusagen und dabei eine Verknüpfung von Daten erfolgt, «die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt».

«Ausdrücklich» ist eine Einwilligung, wenn sie schriftlich oder mündlich erfolgt oder auch als Erklärung in irgendeiner Form (z. B. Kopfnicken, Handzeichen).

Keine Zustimmung ist erforderlich, wenn die Bearbeitung besonders schützenswerter Daten gesetzlich gestattet wird (z. B. Art. 84 Abs. 1 KVG, Art. 96 Abs. 1 UVG).

4. Erweiterte Informationspflicht der Datenbearbeiter

Die Informationspflicht bei der *planmässigen* Beschaffung von Personendaten wird ausgebaut. Der betroffenen Person sind im Zeitpunkt der Datenbeschaffung folgende Pflichtangaben mitzuteilen:

- Identität und Kontaktdaten der/des Verantwortlichen für Datenschutz
- die Bearbeitungszwecke
- bei einer Bekanntgabe von Daten: die Empfänger (z. B. Behörden)
- bei einer Datenbekanntgabe ins Ausland zusätzlich der Staat oder das internationale Organ (dies gilt auch für die Speicherung auf ausländischen Systemen oder in «Clouds»)
- bei indirekter Datenerhebung (falls Daten nicht bei der betroffenen Person selbst erhoben werden) zusätzlich auch die Kategorien bearbeiteter Personendaten.

Planmässig handelt, wer gewollt zu Daten gelangt, z. B. Daten von Mitarbeitenden (für die HR-Arbeit) oder Informationen über Klientinnen und Klienten erhebt.

Nicht informiert werden muss eine betroffene Person über das, was sie ohnehin schon weiss oder was sie selber an Daten zugänglich gemacht hat. Auch muss nicht jedes Mal, wenn Daten beschafft werden, erneut informiert werden, falls zwischen der früher erfolgten Information und der aktuellen Beschaffung ein gewisser zeitlicher und inhaltlicher Zusammenhang besteht (die Spitex-Fachperson muss z. B. nicht bei jedem Besuch bei derselben Patientin erneut informieren).

Keine Informationspflicht besteht, wenn ein Auskunftsgesuch offensichtlich unbegründet oder querulatorisch (z. B. innert kurzer Zeit mehrmals) gestellt wird.

5. Ausbau der Betroffenenrechte

Neu wird ein Recht der betroffenen Person auf Datenherausgabe und -übertragung geschaffen. Sie kann verlangen, dass die von ihr bekanntgegebenen Daten in «einem gängigen elektronischen Format» an sie oder an von ihr bezeichnete Dritte herausgegeben werden. Gängig ist ein «elektronisches Format», welches das automatische Einlesen der Daten in ein Computersystem in strukturierter Form ermöglicht.

Die Herausgabe bzw. Übertragung muss in der Regel kostenlos gewährt werden. Sie kann nur ausnahmsweise verweigert werden, wenn sie offensichtlich querulatorisch oder für eine missbräuchliche Nutzung verlangt wird.

6. Bezeichnung und Pflichtenheft der verantwortlichen Person in der Organisation

Der oder die «Verantwortliche» entscheidet «über den Zweck und die Mittel» der Datenbearbeitung und hat eine Reihe von Aufgaben zu erfüllen. Er/sie

- prüft die Bearbeitung von Personendaten und interveniert bei Verletzungen,
- muss deshalb Zugang zu allen Datensammlungen und Datenbearbeitungen haben,
- führt das Verzeichnis der Datenbearbeitungen (vgl. Ziffer B./7) der Datensammlungen,
- erfüllt die Informationspflichten gegenüber Betroffenen (vgl. Ziffer B./4),
- erarbeitet Vorgaben und Weisungen zur Sicherstellung des Datenschutzes,
- nimmt Risikoanalysen und Datenschutz-Folgeabschätzungen vor und dokumentiert sie.

7. Verzeichnis sämtlicher Datenbearbeitungen

Neu muss ein Verzeichnis sämtlicher Datenbearbeitungen geführt und laufend aktualisiert werden. Es muss folgende Mindestangaben enthalten:

- Identität der/des Verantwortlichen
- Bearbeitungszweck
- Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten

- die Kategorien der Empfänger
- die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer
- eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit (geeignete technische und organisatorische Massnahmen, die es ermöglichen, Verletzungen der Datensicherheit zu vermeiden)
- die Angabe des Staates bei Bekanntgabe von Daten ins Ausland sowie Bekanntgabe von Garantien, durch die ein geeigneter Datenschutz gewährleistet wird.

Art. 12 Abs. 5 DSG sieht die Möglichkeit von Ausnahmen bei weniger als 250 Mitarbeitenden vor, sofern nicht besonders viele besonders schützenswerte Personendaten bearbeitet werden.

8. Verschärfung der Sanktionen

Neu sieht das DSG strafrechtliche Sanktionen in Form einer Busse von bis zu CHF 250'000 vor. Sie zielen hauptsächlich auf Leitungspersonen und nur ausnahmsweise auf die ausführenden Mitarbeitenden ab.

Eine Bestrafung setzt eine *vorsätzliche* Verletzung von Datenschutzbestimmungen voraus.

C. Anwendbarkeit des DSG auf Spitex-Organisationen?

Das DSG gilt für die Bearbeitung von Personendaten durch Bundesorgane und Private. Als Private sind grundsätzlich auch Spitex-Organisationen (in der Rechtsform Verein, Stiftung, AG etc.) zu betrachten.

Eine wichtige Ausnahme betrifft in der Regel aber Spitex-Organisationen, welche aufgrund eines Leistungsvertrags (mit einem Kanton oder Gemeinden) tätig sind. Gemäss vielen kantonalen Datenschutzgesetzen gelten sie in diesem Fall als «mit der Erfüllung öffentlicher Aufgaben beauftragt» (oder ähnlich formuliert) bzw. als «öffentliches Organ», so z. B. in den Kantonen Zürich (§ 3 Abs. 1 Bst. c IDG), Bern (Art. 2 Abs. 6 Bst. b KDSG), Aargau (§ 3 Abs. 1 Bst. c Ziffer 2 IDAG), Luzern (§ 2 Abs. 8 KDSG) und St. Gallen (Art. 2 Abs. 1^{bis} DSG).

Spitex-Organisationen unterstehen **dem kantonalen Datenschutzrecht**, *soweit* sie im Rahmen eines kantonalen oder kommunalen Leistungsauftrags tätig sind. Geht ihre Tätigkeit bzw. ihr Leistungsangebot über einen derartigen Leistungsauftrag hinaus, gilt hierfür das **Datenschutzrecht des Bundes (DSG).** Liegt somit eine «gemischte» Angebotssituation vor, ist aus Gründen der Praktikabilität zu empfehlen, die gesamte Tätigkeit der Spitex-Organisation datenschutzmässig an jenem Recht zu orientieren, welches die höheren Anforderungen stellt, in der Regel somit am DSG.

Für die datenschutzrechtliche Unterstellung nicht relevant ist die Unterscheidung in KVG-/nicht-KVG-Leistungen oder die Gemeinnützigkeit einer Organisation.

Es ist davon auszugehen, dass die kantonalen Datenschutzgesetze in nächster Zeit an das revidierte DSG angepasst werden und die inhaltliche Bedeutung der soeben

im Punkt C erwähnten Unterscheidung zwischen kantonaler und nationaler Gesetzgebung allmählich abnehmen wird.

D. Ausblick und Empfehlung

Das Inkrafttreten des DSG bewirkt keinen direkten Handlungsbedarf für Spitex-Organisationen, die dem Datenschutzrecht eines Kantons unterstehen.

Gleichwohl ist *allen* Spitex-Organisationen zu empfehlen, einen verantwortungsbewussten Umgang mit der Datenschutzthematik sicher zu stellen und sich in folgenden Schritten auf die DSG-Konformität ihrer Tätigkeit vorzubereiten:

1) Allgemeine Übersicht zur eigenen Situation erstellen und u.a. analysieren:
   - Welchen Bestand an Daten haben wir?
   - Wo und wie werden Daten durch wen bearbeitet?
   - Wie ist der Zugang zu den Daten geregelt?
   - Genügen wir den Anforderungen an die Datensicherheit, Speicherbegrenzung, Archivierung etc.?
   - Besteht Handlungsbedarf (technisch, organisatorisch, personell)?
   - Wer ist für den Datenschutz verantwortlich?

   Für diese Analyse ist evtl. externe Unterstützung beizuziehen („Datenschutz-Audit“ durchführen).

2) Gemäss Ergebnissen der Analyse gezielt Massnahmen ergreifen (technisch, organisatorisch, personell; evtl. extern unterstützt)

3) Mitarbeitende für Thematik sensibilisieren

4) Datenschutzkonzept erstellen, Datenschutz als Teil des Risikomanagements etablieren und regelmässig auf Managementebene beurteilen (in der Regel intern, allenfalls periodisch ein externes Audit durchführen lassen)

Hans-Ulrich Zürcher, 31.1.2022