Dr. Michael Hunziker, LL.M.
Rechtsanwalt und Notar, Solicitor (England)
MBA Digitale Transformation

Schärer Rechtsanwälte

Wichtigste Regelungen des nDSG

Das totalrevidierte Bundesgesetz über den Datenschutz («nDSG») wird voraussichtlich am 1. September 2023 in Kraft treten. Ein Hauptziel der Revision war das Angleichen der nationalen Datenschutzgesetzgebung an die geänderten europäischen Regelungen der Datenschutz-Grundverordnung («DSGVO»). Nachstehend werden die wichtigsten Neuerungen des nDSG summarisch dargelegt.

HAFTUNGSAUSSCHLUSS
Die untenstehenden Ausführungen stellen eine summarische Zusammenstellung einzelner Regelungen des nDSG dar (Stand 9. Juni 2022). Dieses Dokument wurde mit grösstmöglicher Sorgfalt erstellt. Wir übernehmen jedoch keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität dieses kostenlos bereitgestellten Dokuments. Die nachstehende Ausführung stellen insbesondere keine Rechtsberatung dar.

Die Nutzung dieses Dokuments erfolgt auf eigene Gefahr. Wir empfehlen Ihnen, die Datenschutzkonformität Ihres Unternehmens mittels einer spezifischen Rechtsabklärung sicherzustellen.

Informationspflichten

Die bereits bestehenden Informationspflichten werden erheblich erweitert. Künftig muss – *die Tatbestände von Art. 20 nDSG ausgenommen* - nicht nur über die Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen informiert werden, sondern grundsätzlich über jede beabsichtigte Beschaffung von Personendaten. Unternehmen müssen den Betroffenen dabei mind. offenlegen:

(i) Wer oder welches Unternehmen für die Datenbearbeitung verantwortlich ist (inkl. Angabe der jeweiligen Kontaktdaten);
(ii) Für welche Zwecke die Daten bearbeitet werden;
(iii) gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

Werden Daten ins Ausland weitergegeben, sind sämtliche Staaten zu nennen, in welche die Personendaten übermittelt werden. Sofern diese Staaten keinen angemessenen Datenschutz (vgl. Liste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten [EDÖB][1] resp. Bundesrats) aufweisen, muss zudem offengelegt werden, wie trotzdem ein angemessener Datenschutz sichergestellt wird.

Mit anderen Worten: Eine Datenschutzerklärung wird faktisch obligatorisch. Vorsicht aber bei Mustern aus dem Internet, diese enthalten oftmals «nur» die Informationspflichten gemäss aDSG und bilden vielfach nur Grundfälle ab.

[1] Abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html (Stand 25.05.2022)

Profiling
Zweck des Profilings ist es, identifizierte Korrelationsmuster auf neue Datensätze anzuwenden. Als Profiling bezeichnet das nDSG jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, eine maschinelle Meinungsbildung über persönliche Aspekte einer bestimmten Person (persönlicher Vorlieben, Interessen, Verhalten etc.) zu erzielen. Wenn die Zielsetzung der Bewertung nicht auf eine betroffene Person, sondern auf eine aggregierte Gruppe angewendet wird, liegt kein Profiling vor.

Vom Profilingbegriff gemäss nDSG sind weiter nur maschinelle Datenverarbeitung erfasst; der blosse Einsatz technischer Hilfsmitteln genügt noch nicht, soweit die eigentliche Analyse durch einen Menschen erfolgt. Genauso wenig ist die automatisierte Verarbeitung von reinen Sachdaten erfasst.

Wie unter dem bestehenden Recht ist Profiling weiterhin ohne Einwilligung der betroffenen Personen zulässig, soweit keine widerrechtliche Datenbearbeitung vorliegt. Die Einwilligung ist daher nur notwendig, wenn die Bearbeitungsgrundsätze aus Art. 30 Abs. 2 nDSG verletzt oder die Grundsätze gemäss Art. 6 Abs. 3 nDSG nicht eingehalten werden. Soweit durch Profiling eine andere Bestimmung des nDSG tangiert wird, sind selbstredend die dortigen Pflichten einzuhalten.

Die obenstehenden Regelungen gelten auch für Profiling «mit hohem Risiko», also Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt (entspricht einem Persönlichkeitsprofil i.S. des geltenden DSG). Für Profiling mit hohem Risiko bedarf es definitionsgemäss einer Datenschutz-Folgeabschätzung (siehe dazu unten).

Obschon durch das nDSG (meistens) keine Einwilligung verlangt ist, wird das Einholen einer ausdrücklichen Einwilligung meist zu empfehlen sein.

Verzeichnis über die Bearbeitungstätigkeit
Neu muss ein Verzeichnis über die internen Datenbearbeitungsprozesse innerhalb eines Unternehmens geführt werden. Es geht hierbei grundsätzlich um dieselben Informationen, die der Informationspflicht (Art. 19 nDSG) unterstehen. Es ist möglich, dass der Bundesrat diese Pflicht für KMU (Unternehmen bis 250 MitarbeiterInnen) in der noch zu erlassenden Datenschutzverordnung abschwächen wird.

Auftragsbearbeitungsvereinbarung
Für Unternehmen, die ihre Datenbearbeitung auslagern, muss neu aktiv sichergestellt werden, dass der Auftragnehmer die Daten nur so bearbeitet, wie es der Verantwortliche selbst tun dürfte (Art. 9 nDSG). Neu muss auch das Beiziehen von Subunternehmern genehmigt werden.

Verantwortlicher («Controller») im Sinne des Datenschutzgesetzes ist dabei diejenige Person, die über den Zweck und die Mittel der Datenbearbeitung (mit)bestimmt (Art. 5 lit. j nDSG). Bearbeitet ein Dritter die Daten im Auftrag des Controllers, so gilt er als Auftragsbearbeiter («Processor») i.S.v. Art. 5 lit. k nDSG. Der Schwerpunkt des Auftragsverhältnisses (Ziel und Zweck des Auftrags) muss dabei in der Bearbeitung von Personendaten liegen und nicht nur ein Mittel zur Auftragserfüllung darstellen (vgl. etwa bei Reisebüros oder Banken).

Für die Auslagerung der Datenbearbeitung wird der Abschluss einer schriftlichen Auftragsbearbeitungsvereinbarung empfohlen, da bei Datenschutzverletzungen eine solidarische Haftbarkeit zwischen gemeinsam verantwortlichen Personen besteht.

Meldepflicht bei Verletzungen der Datensicherheit
Sofern eine festgestellte Datensicherheitsverletzung (verlorene, gelöschte oder veränderte Daten resp. unberechtigter Zugriff) zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen führen könnte, unterstehen Unternehmen neu einer Meldepflicht gegenüber dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten («EDÖB»). Es genügt hierbei die blosse Möglichkeit einer Datensicherheitsverletzung.

Die Meldung hat so schnell wie möglich zu erfolgen, eine starre Frist (wie sie die DSGVO kennt), besteht aber nicht.

Datenschutz-Folgeabschätzung
Jedem Einsatz einer neuen Datenbearbeitungsmöglichkeit (z.B. Tracking Tools etc.) hat eine Datenschutz-Folgeabschätzung vorauszugehen («DSFA»), soweit sie zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen führen könnte. Hiermit soll eine präventive Verhältnismässigkeits- und die Datenminimierungsprüfung sichergestellt werden.

Auskunftsrecht und Datenportabilität
Jeder betroffenen Person steht ein Auskunftsrecht betreffend ihre bearbeiteten Daten zu. Es kann Auskunft verlangt werden über den Bearbeitungszweck, die Dauer der Bearbeitung, die Herkunft der Daten sowie die Datenempfänger. Die Auskunft hat für die betroffene Person grundsätzlich kostenlos zu erfolgen.

Will ein Verantwortlicher die Auskunft aufgrund überwiegenden Interesses verweigern (Art. 26 nDSG), hat er eine Interessenabwägung vorzunehmen und seinen Entscheid zu begründen.

Eine gewisse Nähe zum Auskunftsrecht weist das neue Datenportabilitätsrecht auf, verfolgt aber einen anderen Zweck und ist sachlich viel enger ausgestaltet. Das Auskunftsrecht dient der Information einer betroffenen Person, wohingegen die Datenportabilität einen Anbieterwechsel ermöglichen soll. Jede betroffene Person hat neu einen Anspruch darauf, dass die eigenen Personendaten in einer gängigen elektronischen Form herausgegeben resp. auf einen neuen Verantwortlichen übertragen werden. Umfasst sind nicht nur aktiv übermittelte Daten, sondern auch passiv «beobachtete» (z.B. Sucherlauf im Browser etc.). Der Anspruch besteht nur dann, wenn die Datenbearbeitung automatisiert erfolgt und aus einer Einwilligung oder einer Vertragsbeziehung mit der betroffenen Person resultiert. Es gilt dasselbe Verweigerungsrecht wie für das Auskunftsrecht.

Recht auf menschliches Gehör
Automatisierte Einzelentscheide müssen neu offengelegt werden, soweit sie über eine reine «Wenn-Dann» Entscheidung hinausgehen und mit Rechtsfolgen für die betroffene Person verbunden sind resp. diese erheblich beeinträchtigt. Denkbar sind etwa Anwendungsfälle im Bereich automatisierter Bewerbungsprozesse oder Versicherungsverträge.

Es muss die Möglichkeit bestehen, dass ein automatisierter Entscheid durch eine natürliche Person überprüft werden kann (sog. Recht auf menschliches Gehör).

Ausgedehnte Schweigepflicht
Neu besteht eine Schweigepflicht betreffend alle geheimen Personendaten, von denen jemand in beruflicher Ausübung Kenntnis erlangt. Erfasst sind alle Daten, die der Kunde einer Dienstleisterin in der berechtigten Erwartung mitgeteilt hat, dass diese sie vertraulich behandelt. Ein formelles Vertragsverhältnis wird nicht verlangt, ebenso wenig, dass die Daten besonders schützenswert sind.

Es wird empfohlen, alle Vertragspartner unmissverständlich darauf hinzuweisen, dass geheime Daten weitergleitet werden können. Wer sich absichern will, sollte vor einer Datenweitergabe die Einwilligung der Vertragspartner einholen. Stand heute ist davon auszugehen, dass es möglich sein wird, die ausgedehnte Schweigepflicht mittels eines «General-Waivers» vertraglich weitestgehend wegzubedingen.

Strafbestimmungen
Unter dem nDSG wird der Bussenrahmen beträchtlich (auf bis zu CHF 250'000.00) erhöht. Die Bussen richten sich sodann nicht gegen das Unternehmen, sondern treffen die für ein Unternehmen tätigen, entscheidtragenden, natürlichen Personen direkt (gemeint sind Leitungspersonen). Es ist davon auszugehen, dass diese Bussen nicht versichert werden können und nicht durch das Unternehmen bezahlt bzw. zurückbezahlt werden dürfen. Es bestehen die folgenden (neuen) Straftatbestände:

- Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten, wobei betreffend die Auskunftspflicht nur eine falsche oder unvollständige Auskunft strafbar ist, nicht aber eine unterlassene Auskunft;

- Verletzung der Sorgfaltspflichten: Unzulässiger Datenexport ins Ausland oder mangelhafte Auftragsbearbeitungsverträge;

- Verletzung der (abstrakten) Datensicherheit (Mindestanforderungen aber noch nicht konkretisiert durch den Bundesrat);

- Verletzung der ausgedehnten beruflichen Schweigepflichten;

- Nichtbefolgen einer Verfügung des EDÖB: Die Kompetenzen des EDÖB wurden erheblich erweitert. So kann er nun, sofern genügend Anzeichen einer Verletzung des Datenschutzes bestehen, eine Untersuchung einleiten, die Anpassung von Datenbearbeitungen und die Löschung von Personendaten **verfügen**; jedoch obliegt dem EDÖB weiterhin keine Sanktionshoheit.

Weiterhin wird nur vorsätzliches Handeln bestraft, wobei aber die Abgrenzung zwischen strafloser bewusster Fahrlässigkeit und strafbarem Eventualvorsatz in der Praxis sehr schwierig sein dürfte. Gehilfen werden weiterhin nicht bestraft werden, da es sich um Übertretungsstraftatbestände handelt.

Wie unter geltendem Recht sind alle Strafbestimmungen Antragsdelikte, die eines Strafantrags durch die betroffene Person bedürfen. Der Antrag der betroffenen Person muss innert drei Monaten ab Kenntnis der Täterschaft erfolgen. Der EDÖB hat weiterhin kein Antragsrecht, er kann lediglich Anzeige erstatten.