N

Monthly
Newsletter
December 2022

Schellenberg
Wittmer

Data

Umsetzung des neuen Datenschutzgesetzes: Schritt 3 – Interne Massnahmen

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

1.
Das Bearbeitungsverzeichnis mit der Übersicht der Datenbearbeitungen kann als zentraler Ausgangspunkt zur Umsetzung der verschiedenen Massnahmen dienen.

2.
Ein generelles internes Datenschutzreglement ist ratsam, in bestimmten Fällen kann ein spezifisches Bearbeitungsreglement Pflicht sein, und Mitarbeitende sollten entsprechend geschult werden.

3.
Für Datenschutz-Folgenabschätzungen, für Meldungen bei *Data Breaches* und bezüglich automatisierter Einzelentscheidungen sollten Zuständigkeiten, Prozesse und Vorlagen definiert werden.

1 Überblick

Das neue Datenschutzgesetz (**nDSG**) und die neue Datenschutzverordnung (**nDSV**) werden per 1. September 2023 in Kraft treten. In unserem Newsletter von Oktober 2022 haben wir einen dreistufigen **Umsetzungsplan** (***Roadmap***) vorgestellt und den ersten Schritt (Vorbereitung) beschrieben. Schritt 2 mit Fokus auf den extern wirksamen Massnahmen wurde im Newsletter von November 2022 behandelt. Hier legen wir mit **Schritt 3** den Schwerpunkt nun auf die **intern wirksamen Massnahmen** in folgenden Bereichen:

- **Verträge und Reglemente** (Auftragsbearbeitungen, Schweigepflicht, Datenschutzreglement und Schulungen)
- **Operative Prozesse** (Datenschutz-Folgenabschätzung, Meldepflicht bei *Data Breaches*, automatisierte Einzelentscheidungen)
- **Administrative / Technische Prozesse** (Bearbeitungsverzeichnis, Datenportabilität, Aufbewahrungsdauer)

2 Verträge und Reglemente

2.1 Auftragsbearbeitungen

Wenn der Verantwortliche (*Controller*) gewisse Bearbeitungen durch einen Auftragsbearbeiter (*Processor*) ausführen lässt, sieht das nDSG neu verschärfte Anforderungen vor: Im **Auftragsbearbeitungsvertrag** (*Data Processing Agreement*, **DPA**) ist sicherzustellen, dass der *Processor* die Daten nur so bearbeitet, wie dies der *Controller* selbst dürfte, und nicht ohne Einbezug des *Controllers* Unter-Auftragsbearbeiter (*Sub-Processors*) beizieht. Dazu sind entsprechende Weisungs- und Kontrollrechte sowie Zustimmungsmechanismen vorzusehen. Für die Umsetzung unter Art. 28 der EU-Datenschutz-Grundverordnung (**DSGVO**) erstellte Vorlagen **genügen den Anforderungen des nDSG**, sofern sie in der Formulierung an Schweizer Recht angepasst werden.

Erfasst werden **auch gruppeninterne Auftragsbearbeitungen**, und ein Teil der Pflichten zu den Auftragsbearbeitungen ist unter dem nDSG **neu strafbewehrt**. Bestehende DPA sollten deshalb überprüft werden, und beim Abschluss neuer DPA ist die Einhaltung der Mindestanforderungen sicherzustellen.

2.2 Schweigepflicht

Schon das geltende Datenschutzgesetz (**DSG**) stellt die **Verletzung der beruflichen Schweigepflicht** unter Strafe, ist aber auf geheime besonders schützenswerte Personendaten und Persönlichkeitsprofile beschränkt (Art. 35 DSG). Neu werden **sämtliche geheimen Personendaten** von diesem Schutz erfasst: Relevant ist somit nicht mehr die Art der Daten, sondern nur noch, ob es sich um "geheime" Daten handelt: Abgestellt wird darauf, dass die betroffene Person ein (erkennbares) schutzwürdiges Geheimhaltungsinteresse und den Willen zur Geheimhaltung hat und dass die Daten nicht bereits allgemein bekannt (oder zugänglich) sind. Wer vorsätzlich geheime Personendaten offenbart, kann unter dem nDSG mit **Busse bis zu CHF 250'000** bestraft werden.

Werden allenfalls geheime Personendaten bearbeitet, sollte geprüft werden, ob dazu eine **Regelung in den Kundenverträgen** (oder in den Verträgen mit anderen Betroffenen, in AGB etc.) vorzusehen ist. In jedem Fall ratsam sind interne Vorgaben hierzu und die Sensibilisierung der Mitarbeitenden.

2.3 Datenschutzreglement und Schulungen

Im Gegensatz zur DSGVO kennt das nDSG keine allgemeine Rechenschaftspflicht. Zur **Sicherstellung der Datensicherheit** müssen aber geeignete technische und organisatorische Massnahmen (**TOM**) ergriffen und entsprechend dokumentiert werden. Die nDSV enthält hierzu weitere Vorgaben, inklusive der **Pflicht zur Erstellung eines Bearbeitungsreglements**: Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko automatisiert durchgeführt, muss ein Bearbeitungsreglement mit dem **Mindestinhalt nach Art. 5 nDSV** erstellt werden. Die vorsätzliche Nichteinhaltung der Vorgaben zu den Mindestanforderungen kann mit **Busse bis zu CHF 250'000** sanktioniert werden.

Auch wenn die Schwelle für die Pflicht zur Erstellung eines speziellen Bearbeitungsreglements nicht erreicht wird, sollte zur Umsetzung der TOM ein **allgemeines Datenschutzreglement** erlassen werden mit den Vorgaben, wie betriebsintern Personendaten bearbeitet werden, was dabei zu beachten ist und welche Zuständigkeiten bestehen. Wichtig ist, dass diese Vorgaben auch tatsächlich gelebt werden: Die Mitarbeitenden müssen mit entsprechenden **Schulungen und Trainings** auf ihre datenschutzrechtlichen Pflichten aufmerksam gemacht und in deren Umsetzung unterstützt werden. Gerade auch bezüglich der ausgeweiteten Schweigepflicht (s. oben) ist eine Sensibilisierung ratsam.

Auftragsbearbeitungen sind vertraglich abzusichern.

3 Operative Prozesse

3.1 Datenschutz-Folgenabschätzung (DSFA)

Ist eine neue Datenbearbeitung geplant, die ein hohes Risiko für die betroffene Person mit sich bringen kann, ist eine **Datenschutz-Folgenabschätzung (DSFA)** durchzuführen. Ein hohes Risiko kann sich ergeben aus Art, Umfang, Umständen und Zweck der Datenbearbeitung, insbesondere aus der Verwendung neuer Technologien (wie z.B. Künstlicher Intelligenz, **KI**). Die DSFA dient der Einschätzung der damit verbundenen Risiken und der Implementierung von risikomindernden Massnahmen (wie z.B. Datenminimierung, Anonymisierung, Zugriffsbeschränkungen etc.).

Der **Umfang und die Detailtiefe** der DSFA sind abhängig von der Komplexität und dem Risikoprofil der geplanten Bearbeitung. Bei deren Erstellung sollten das *Business* (betr. Sachverhalt) und *Legal/Compliance* (betr. Datenschutz-Aspekte) eng zusammenwirken. Führt die DSFA zur Erkenntnis, dass auch die vorgesehenen Massnahmen das

Risiko nicht genügend einschränken können, so muss vor der Umsetzung der geplanten Datenbearbeitung der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (**EDÖB**) konsultiert werden (oder der interne Datenschutzberater, sofern ein solcher formell ernannt wurde).

Unter gewissen Umständen ist ein spezielles Bearbeitungsreglement zu erlassen.

3.2 Meldepflicht bei Data Breaches

Mit dem nDSG wird neu die Pflicht zur **Meldung von Verletzungen der Datensicherheit (*Data Breach Notification*)** eingeführt. Falls die Datensicherheit verletzt wird (z.B. durch Verlust von Daten, ob auf Papier oder digital, durch unerlaubte Zugriffe etc.), muss der **EDÖB** informiert werden, sofern diese Verletzung voraussichtlich zu einem hohen Risiko für die Betroffenen führt. Das nDSG sieht keine bestimmte Frist für die Meldung vor; diese hat aber **so rasch als möglich** zu erfolgen, wobei man sich an der 72-Stunden-Frist gemäss DSGVO orientieren kann. Die **Betroffenen** sind zu informieren, wenn es zu ihrem Schutz erforderlich ist (z.B. weil Kreditkarten gesperrt oder Passwörter gewechselt werden müssen) oder wenn es der EDÖB verlangt.

Zur Umsetzung der Meldepflicht sollten **Zuständigkeiten und Prozesse** definiert werden, damit klar ist, wer in der hektischen Zeit unmittelbar nach Entdeckung eines *Data Breaches* welche Entscheidungen nach welchen Kriterien fällt, und wie diese umzusetzen sind. Die Meldepflicht ist zwar (im Gegensatz zur DSGVO) nicht strafbewehrt, deren Verletzung kann aber zu Reputationsschäden führen (und allenfalls eine Untersuchung durch den EDÖB auslösen).

Ebenfalls berücksichtigt werden sollten **zusätzliche gesetzliche oder vertragliche Meldepflichten**. Bei vertraglichen Meldepflichten ist oft unklar, gegenüber welchen Vertragspartnern eine solche besteht. Es sollte deshalb - auch um vertragliche Haftungsfolgen zu vermeiden - eine gesonderte Übersicht solcher Meldepflichten erstellt (und aktuell gehalten) werden, damit im Bedarfsfall schnell reagiert werden kann.

3.3 Automatisierte Einzelentscheidungen

Automatisierte Einzelentscheidungen (AEE) sind KI-Ermessensentscheide, die ohne menschliches Zutun erfolgen und auf die Betroffenen eine relevante Auswirkung haben: So ist z.B. die automatische Einblendung personalisierter Werbung auf einer Website keine AEE, die rein KI-basierte Aussortierung einer Stellenbewerbung hingegen schon. Zurzeit sind AEE noch wenig verbreitet, ihr Einsatz wird aber mit fortschreitender Digitalisierung und Automatisierung zunehmen.

Werden AEE eingesetzt, so sind zusätzliche Vorgaben zur **Informationspflicht** bzw. zur **Datenschutzerklärung** zu beachten und es sind **spezielle Anhörungs- und Prüfprozesse** vorzusehen. Diese Pflichten sind teilweise **strafbewehrt**. Der Einsatz von AEE sollte deshalb frühzeitig identifiziert und adressiert werden (z.B. wenn neue Software mit AEE-Funktionen implementiert wird).

4 Administrative / Technische Prozesse

4.1 Bearbeitungsverzeichnis

Auf die Bedeutung des **Bearbeitungsverzeichnisses** haben wir bereits in unserem Newsletter von Oktober 2022 hingewiesen: Das Bearbeitungsverzeichnis ist das **zentrale Instrument zur Umsetzung des nDSG**, da die Übersicht über die Datenbearbeitungen als Ausgangspunkt für alle Massnahmen dient. Sowohl der Verantwortliche (*Controller*) wie auch der Auftragsbearbeiter (*Processor*) müssen grundsätzlich ein Bearbeitungsverzeichnis führen, wobei Art. 12 nDSG dafür je unterschiedliche Vorgaben zum Mindestinhalt aufstellt.

Zu **Form und Aufbau** hingegen bestehen keine Vorgaben. Man kann dazu auf am Markt verbreitete Software-Lösungen abstellen oder - gerade bei einfacheren Verhältnissen - selbst ein Verzeichnis erstellen (z.B. in Word oder Excel). Hilfreich ist, wenn sich der Aufbau möglichst pragmatisch an den **vorgenommenen Datenbearbeitungen** orientiert, da dies die direkte Verwendung der Information für weitere Massnahmen vereinfacht. Wird der Aufbau eher an technischen Aspekten ausgerichtet (z.B. an den verwendeten Applikationen), so kann dies bei der Erstellung einen gewissen Zuordnungsaufwand einsparen, reduziert jedoch auf lange Frist die einfache Handhabung und Weiterverwendung dieser Informationen.

Bei neuen Datenbearbeitungen mit hohem Risiko ist eine DSFA durchzuführen.

4.2 Datenportabilität

Unter dem Stichwort der **Datenportabilität** hat der Verantwortliche den Betroffenen die automatisiert bearbeiteten Personendaten herauszugeben, die **diese ihm selbst bekanntgegeben** haben oder die der Verantwortliche über sie **bei der Nutzung eines Dienstes** (z.B. eines Online-Dienstes) **oder Gerätes** (z.B. eines Fitness-Trackers) gesammelt hat. Nicht herausgegeben werden müssen Daten, die der Verantwortliche selbst durch eigene Auswertung aus den gesammelten Daten generiert hat (z.B. das individuelle Nutzerprofil, das aus den gesammelten Daten erstellt wurde). Die Daten müssen in einem gängigen elektronischen Format herausgegeben werden.

Damit eine Herausgabe überhaupt möglich ist, muss sichergestellt werden, dass die Personendaten einer betroffenen Person **identifiziert**, von anderen Daten **isoliert** und

nötigenfalls in ein gängiges elektronisches Format **migriert** werden können. Die Pflicht, die Systeme und Prozesse entsprechend aufzusetzen, ergibt sich dabei aus dem Grundsatz von ***Privacy by Design*** (Art. 7 nDSG).

4.3 Aufbewahrungsdauer

Aus dem **Grundsatz der Datenminimierung** folgt, dass Daten zu **löschen** sind, wenn sie nicht mehr für den ursprünglichen Zweck erforderlich sind. Ausnahmen hiervon bedürfen einer Rechtfertigung, etwa aufgrund gesetzlicher oder vertraglicher Aufbewahrungsvorschriften oder bei überwiegendem Interesse des Verantwortlichen (z.B. solange die Daten noch in einem möglichen Rechtsstreit Verwendung finden können).

Die Umsetzung sollte durch Erstellung eines **Aufbewahrungsreglements** mit Festlegung der Aufbewahrungsdauer je Datenkategorie und den zur Löschung nötigen Schritten erfolgen. Hierbei müssen die **Löschprozesse** auch angestossen (z.B. durch Setzen eines "Ablaufdatums" für Datenbestände) und umgesetzt werden (z.B. durch jährliche Archivierungs- und Löschroutinen).

5 Fazit und Ausblick

Gerade im Bereich der intern wirksamen Massnahmen bringt das nDSG **relevante neue Pflichten** mit sich, die nicht unterschätzt werden sollten. Deren Umsetzung selbst ist keine "*Rocket Science*", bringt aber nicht unerheblichen Aufwand mit sich und sollte deshalb zeitnah an die Hand genommen werden.

Wie die Roadmap zur Umsetzung aussehen kann, haben wir im Newsletter von Oktober 2022 behandelt, die extern wirksamen Massnahmen im Newsletter von November 2022. Dieser Newsletter zu den intern wirksamen Massnahmen schliesst unsere dreiteilige Serie zur Umsetzung des nDSG ab.

Roland Mathys
Partner Zürich
roland.mathys@swlegal.ch

Dr. Samuel Klaus
Partner Zürich
samuel.klaus@swlegal.ch

Vincent Carron
Partner Genf
vincent.carron@swlegal.ch

Dr. Catherine Weniger
Counsel Genf
catherine.weniger@swlegal.ch

Schellenberg Wittmer AG
Rechtsanwälte

Zürich
Löwenstrasse 19
Postfach 2201
8021 Zürich / Schweiz
T +41 44 215 5252
www.swlegal.com

Genf
15bis, rue des Alpes
Postfach 2088
1211 Genf 1 / Schweiz
T +41 22 707 8000
www.swlegal.com

Singapur
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapur 049909
T +65 6580 2240
www.swlegal.sg