



Umsetzung des neuen Datenschutzgesetzes: Schritt 1 - Vorbereitung

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

- 1.** Das neue Datenschutzgesetz wird am 1. September 2023 in Kraft treten, ohne dass es eine Übergangsfrist geben wird. Die neuen Anforderungen müssen ab dem ersten Tag erfüllt sein.
- 2.** Die notwendigen Umsetzungsmassnahmen sollten frühzeitig angegangen werden. Sie lassen sich risikobasiert und ressourcenorientiert priorisieren und in drei Umsetzungsschritte bündeln.
- 3.** Schritt 1 umfasst die Vorbereitung, Bestandaufnahme und gewisse Vorentscheide. In Schritt 2 werden externe Massnahmen implementiert. Schritt 3 fokussiert auf die Umsetzung interner Massnahmen.

1 Überblick

Der Bundesrat hat am 31. August 2022 entschieden, dass das totalrevidierte Schweizer Datenschutzgesetz (**nDSG**) **per 1. September 2023** in Kraft treten wird, inklusive der zugehörigen neuen Datenschutzverordnung (nDSV). Eine Übergangsfrist wird es nicht geben. Immerhin steht nun bis zum Inkrafttreten eine **Umsetzungszeit von rund einem Jahr** zur Verfügung.

Diese Zeit sollte gut genutzt und die Umsetzung der neuen Vorgaben frühzeitig aufgegleist werden, mit Projektende bis spätestens August 2023. Der **Aufwand für die Umsetzung** sollte - je nach individueller Ausgangslage - nicht unterschätzt werden.

2 Was ändert sich - und was bleibt gleich?

Die **Grundprinzipien des Schweizer Datenschutzrechts** bleiben gleich. Eine Datenbearbeitung benötigt (anders als unter der EU-Datenschutz-Grundverordnung (**DSGVO**)) weder eine Einwilligung noch eine spezielle Rechtfertigung, solange die allgemeinen Bearbeitungsgrundsätze eingehalten werden, die betroffene Person der Datenbearbeitung nicht ausdrücklich widersprochen hat und nicht besonders schützenswerte Personendaten an Dritte bekanntgegeben werden. Auch die **allgemeinen Bearbeitungsgrundsätze** (namentlich Rechtmässigkeit, Transparenz, Zweckbindung, Verhältnismässigkeit, Datenrichtigkeit und Datensicherheit) bleiben inhaltlich weitgehend gleich. Änderungen ergeben sich hingegen aus dem **erhöhten Detaillierungsgrad** der gesetzlichen Regelung, den weitgehenden **Vorgaben zur formalen Umsetzung** und dem neu eingeführten **Sanktionsregime**. Zudem wird der Begriff der Personendaten eingeschränkt, d.h. das nDSG wird sich nur noch auf Daten **natürlicher Personen** beziehen - juristische Personen fallen nicht mehr in seinen Schutzbereich.

3 Relevanz fristgerechter Umsetzung

Die Anforderungen des nDSG müssen ab dem 1. September 2023 erfüllt sein. Ab dann gelten auch die neuen **Sanktionsbestimmungen**. Diese sind zwar bei den Beträgen (bis CHF 250'000) nicht mit den Bussen unter der DSGVO vergleichbar (bis 4% des weltweiten Umsatzes oder EUR 20 Mio., je nachdem, welcher Betrag höher ist). Der grosse Unterschied besteht aber darin, dass unter dem nDSG die **Bussen nicht auf das Unternehmen, sondern auf die verantwortliche Person zielen**. Dies können formelle Entscheidungsträger sein (z.B. Management, Geschäftsführer, Verwaltungsrat) oder Mitarbeiter mit selbständigen Entscheidungsbefugnissen in ihrem Tätigkeitsbereich (z.B. Bereichs- oder Abteilungsleiter, Stabsstellen, zentralisierte Funktionen etc.).

4 Umsetzung in drei Schritten

Vor diesem Hintergrund bietet sich eine risikobasierte und ressourcenorientierte **Priorisierung** der Umsetzungsmassnahmen an. Mit wie viel **Aufwand für die Umsetzung** zu

rechnen ist, hängt von der bisherigen Vorbefassung mit dem Thema Datenschutz ab. Wurde z.B. die DSGVO bereits umgesetzt (z.B. aufgrund gruppeninterner Vorgaben), so werden nur punktuelle Ergänzungen der bestehenden Massnahmen nötig sein. Wurden bisher nur (oder nicht einmal) die Mindestanforderungen des geltenden DSG umgesetzt, so wird mit mehr Aufwand zu rechnen sein. Wir legen im Folgenden einen dreistufigen **Umsetzungsplan (Roadmap)** dar und führen den ersten Schritt vertieft aus. Die Schritte 2 und 3 werden in zwei Folge-Newslettern erläutert. Diese Roadmap kann bei der Umsetzung als Orientierungshilfe dienen - wird aber in jedem Fall auf die konkrete Situation und individuelle Ausgangslage anzupassen sein und muss ggf. mit branchen- und sektorspezifischen Besonderheiten ergänzt werden.

5 Zeitplan zur Umsetzung

5.1 Bis Ende 2022

Unabhängig von der Umsetzung der Vorgaben des neuen DSG müssen gemäss Vorgabe des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) die **vor dem 27. September 2021 abgeschlossene Standardvertragsklauseln (Standard Contractual Clauses (SCC))** bereits bis Ende dieses Jahres ersetzt werden. Weitere Details hierzu finden sich in unserem [Newsletter von Mai 2022](#).

In einem separaten *Workstream* sollten deshalb **bereits bis Ende 2022** die relevanten Auslandstransfers identifiziert und mit an Schweizer Recht angepassten SCC adressiert werden. Dies lässt sich ideal kombinieren mit dem unten aufgeführten Schritt 1 zur Umsetzung des nDSG, insbesondere der Beschaffung der notwendigen Informationen.

5.2 Roadmap zur Umsetzung des nDSG

Der Zeitplan zur Umsetzung ist stark abhängig davon, wie der Datenschutz bereits umgesetzt wurde, sowie vom Umfang und der Komplexität der vorgenommenen Datenbearbeitungen. Der Abschluss des Umsetzungsprojekts sollte jedenfalls vor oder per Mitte August 2023 angestrebt werden. Dabei müssen auch allfällige Abwesenheiten oder eingeschränkte Informationsflüsse während der Sommermonate Juli/August mit einbezogen werden. Idealerweise sollte diese Zeit als Puffer vorgesehen werden. Als Orientierungshilfe kann somit der folgende Zeitplan dienen:

- **Q4-2022 bis Januar/Februar 2023 - Schritt 1:** Gewisse Vorentscheide sind zu fällen, die Projektkoordination (inkl. Budgetfragen) ist anzugehen, und eine Bestandesaufnahme (inkl. der Massnahmen zur Datensicherheit) kann als Grundlage für eine Gap-Analyse dienen.
- **Ab November/Dezember 2022 bis März/April 2023 - Schritt 2:** Fokus auf die Umsetzung extern wirksamer Massnahmen (wobei die Schwerpunktsetzung stark vom jeweiligen Geschäftsbereich und von internen Vorgaben des Unternehmens bzw. der Gruppe abhängig sein wird).
- **Ab 2023 bis Mai/Juni 2023 - Schritt 3:** Fokus auf die Umsetzung interner Massnahmen (mit Priorisierung der sanktionsbewehrten Bereiche).

Ratsam ist, frühzeitig die Bereiche zu identifizieren, bei denen aufgrund der konkreten Situation ein grösserer Aufwand zu

Roadmap zur Umsetzung des nDSG

	2022	2023			
	Q4-2022	Jan / Feb	Mrz / Apr	Mai / Jun	Jul / Aug
SCC	Bestehende SCC ersetzen				
Schritt 1 → Projekt	Projektplanung / Budget Bestandesaufnahme, Verzeichnis Gap-Analyse, Datensicherheit (TOM)				Puffer während Sommerzeit für Abwesenheiten Weitere Abklärungen Unvorhergesehenes
Schritt 2 → Externes		Informationspflicht (DSE) Auslandstransfer (CH-SCC) Auskunftsrecht (DSAR)			
Schritt 3 → Internes		Auftragsbearbeitung Schweigepflicht, Reglement, Trainings DSFA, Breach Notification, Data Portability			

**nDSG tritt in Kraft:
1. September 2023**

erwarten ist (z.B. falls bei der Bestandesaufnahme umfangreiche Informationsbeschaffungen absehbar werden oder falls sich ergibt, dass eine Vielzahl von Verträgen angepasst werden muss). Nötigenfalls können solche Massnahmen dann bereits in vorgelagerten Schritten angegangen werden.

6 Schritt 1: Vorbereitung

6.1 DSGVO-Beurteilung

Vorgängig sollte abgeklärt werden, ob aufgrund des Geschäftsmodells bzw. der vorgenommenen Datenbearbeitungen die **Vorgaben der DSGVO** zu beachten sind (Art. 3 Abs. 2 DSGVO). Falls ja, ist dies bei der Umsetzung des nDSG zu berücksichtigen. Falls nicht, stellt sich die Frage, ob nicht trotzdem die Vorgaben der DSGVO umgesetzt werden sollen (z.B. aus Reputationsgründen oder falls im Rahmen eines internationalen Konzerns bereits DSGVO-konforme Grundlagen vorliegen, auf denen aufgebaut werden kann).

Bestehen bereits DSGVO-konforme Prozesse und entsprechende Dokumente, sind diese ein guter Ausgangspunkt zur Umsetzung des nDSG. Da es auch unter dem nDSG gewisse Unterschiede zur DSGVO gibt, müssen zusätzlich zu den bestehenden DSGVO-Massnahmen gewisse "**Schweizer Add-Ons**" umgesetzt werden. Dies betrifft insbesondere die Bereiche Auslandstransfers, Datenschutzerklärungen und Auskunftsbegehren. Weitere Details hierzu finden sich in unserem [Newsletter vom Dezember 2021](#).

6.2 Projektkoordination

Zur **Vorbereitung** der Umsetzung sollten frühzeitig eine geeignete Projektkoordination aufgesetzt und die notwendigen Ressourcen und Ansprechpersonen identifiziert und miteinbezogen werden. Dazu gehören auch Know-how-Träger aus datenschutzrelevanten Bereichen (wie z.B. Marketing, IT, HR etc.), deren Detailkenntnisse über die unternehmensinternen Prozesse und Datenbearbeitungen für die Umsetzung unabdingbar sind.

6.3 Bestandesaufnahme

Im Rahmen der Bestandesaufnahme erfolgt sodann die Sammlung der zur Umsetzung notwendigen Informationen. Ziel sollte sein, den **Datenbestand**, die vorgenommenen **Datenbearbeitungen** sowie allfällige **Auslandstransfers** zu identifizieren.

bereits bestehende Dokumente (z.B. konzerninterne Verzeichnisse) sowie Checklisten zu den relevanten Punkten zurückgegriffen werden. Liegen die Informationen nicht bereits vor, so können diese durch Interviews mit den relevanten Ansprechpersonen beschafft werden.

6.4 Bearbeitungsverzeichnis

Zur zentralen Sammlung und Konsolidierung der Informationen sollte bereits zu diesem Zeitpunkt das **Bearbeitungsverzeichnis** erstellt werden (Art. 12 nDSG). Es besteht zwar eine **Ausnahme** zur Führung eines Bearbeitungsverzeichnisses bei weniger als 250 Mitarbeitenden, sofern keine Risiko-Bearbeitungen vorgenommen werden (Art. 24 nDSV). Aber auch Unternehmen, die unter diese Ausnahmebestimmung fallen, müssen sich im Detail mit ihren Bearbeitungstätigkeiten auseinandersetzen und die restlichen Vorgaben des nDSG umsetzen. In den meisten Fällen ist es deshalb ratsam, auch dann ein Bearbeitungsverzeichnis zu führen, wenn dazu keine gesetzliche Pflicht besteht.

6.5 Datensicherheit

Da Abklärungen (und allenfalls notwendige Anpassungen) im Bereich der **Datensicherheit** erfahrungsgemäss zeitintensiv sind, sollte dieser Punkt bereits in Schritt 1 adressiert werden. Als Teil der Bestandesaufnahme sollten deshalb der Umfang und die Angemessenheit der **technischen und organisatorischen Massnahmen (TOM)** zur Gewährleistung der Datensicherheit geprüft und dokumentiert werden. Ob weitere Massnahmen nötig sind, lässt sich zumeist erst unter Einbezug der identifizierten Datenkategorien, deren Nutzungszweck und der vorgenommenen Bearbeitungen beurteilen. Die nDSV sieht dazu vor, dass die Angemessenheit der TOM anhand des **Schutzbedarfs** der betroffenen Daten und des **Risikos** für die Persönlichkeit oder Grundrechte der Betroffenen zu beurteilen ist, und enthält Hinweise, wie dabei vorzugehen ist bzw. welche Kriterien dabei zu beachten sind (Art. 1-5 nDSV).

7 Schritte 2 und 3

Auf Grundlage der Vorbereitung in Schritt 1 legt **Schritt 2** den Fokus auf die Massnahmen mit Aussenwirkung und allfälliger Sanktionsfolge. Dazu zählen folgende Themenbereiche, welche wir im nächsten Newsletter beleuchten werden:

- Informationspflicht und Datenschutzerklärungen (**DSE**)

Als Arbeitsgrundlage für die weiteren Schritte sollte einfach greifbar festgehalten werden, wer im Unternehmen welche Personendaten zu welchem Zweck erhebt, nutzt oder anderweitig bearbeitet, ob dies mit Hilfe externer Dienstleister erfolgt, ob dabei Personendaten ins Ausland übermittelt werden bzw. ob von dort darauf zugegriffen wird (und falls ja, welche Länder dies betrifft), wo die Personendaten gespeichert werden etc. Als **Hilfsmittel für die Bestandesaufnahme** kann auf allgemeine Vorlagen,

- Auskunftsrecht (*Data Subject Access Request*, **DSAR**)
- Auslandtransfers und Standardvertragsklauseln (*Standard Contractual Clauses*, **SCC**)

In **Schritt 3** wird der Fokus auf die **internen Massnahmen, Prozesse und Dokumente** gelegt, mit Priorisierung der vom nDSG mit Sanktionen bewehrten Bereiche. Folgende Themen werden wir somit im dritten Newsletter adressieren:

- Auftragsbearbeitung (Auslagerung von Datenbearbeitungen)
- Automatisierte Einzelentscheidungen (**AEE**)
- Berufliche Schweigepflicht
- Internes Datenschutzreglement und Schulungen
- Meldepflicht bei Verletzung der Datensicherheit
- Datenschutz-Folgenabschätzungen (**DSFA**)
- Datenportabilität (*Data Portability*)
- Aufbewahrungsdauer (*Data Retention*)

8 Fazit und Ausblick

Die Umsetzung des nDSG sollte nicht auf die leichte Schulter genommen werden. Bei Verstössen drohen empfindliche, auf die Entscheidungsträger gerichtete Sanktionen. Die Umsetzung selbst ist keine "*Rocket Science*", bringt aber Aufwand mit sich und sollte sorgfältig geplant und zeitnah begonnen werden.

Die konkrete Umsetzung kann in drei Schritte gegliedert werden, bezogen auf **(1) Vorbereitungsmassnahmen, (2) Umsetzung externer Massnahmen sowie (3) Umsetzung interner Massnahmen**. Den ersten dieser Schritte haben wir oben ausgeführt, den konkreten Handlungsbedarf für die beiden weiteren Schritte zeigen wir in den nächsten Monaten in zwei Folge-Newslettern auf.



Roland Mathys
Partner Zürich
roland.mathys@swlegal.ch



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



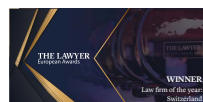
Vincent Carron
Partner Genf
vincent.carron@swlegal.ch



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

Der Inhalt dieses Newsletters stellt keine Rechts- oder Steuerauskunft dar und darf nicht als solche verwendet werden. Sollten Sie eine auf Ihre persönlichen Umstände bezogene Beratung wünschen, wenden Sie sich bitte an Ihre Kontaktperson bei Schellenberg Wittmer oder an eine der oben genannten Personen.

Schellenberg Wittmer AG ist Ihre führende Schweizer Wirtschaftskanzlei mit mehr als 150 Juristinnen und Juristen in Zürich und Genf sowie einem Büro in Singapur. Wir kümmern uns um alle Ihre rechtlichen Belange – Transaktionen, Beratung, Prozesse.



Schellenberg Wittmer AG
Rechtsanwälte

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

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

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