NIEDERER KRAFT FREY

Revidiertes Schweizer Datenschutzgesetz

Klientenanlass

Clara-Ann Gordon
András Gurovits
Janine Reudt-Demont

Zürich — 13. Juli 2021

Überblick

1. Einführung
2. Häufig gestellte Fragen
3. Übersicht der wichtigsten Neuerungen
4. Profiling
5. NKF Compliance Checkliste
6. Q&A

Revision des Schweizer Datenschutzgesetzes (DSG)

- Das aktuelle Datenschutzgesetz stammt aus dem Jahr 1992
- Technologische Entwicklungen und die DSGVO erforderten die Überarbeitung
- Parlamentarische Verabschiedung im Herbst 2020
- Es wurde kein Referendum ergriffen
- Die Bundesverwaltung erarbeitet derzeit die entsprechenden Verordnungen (Vernehmlassung läuft bis 14. Oktober 2021)

§

Wichtige Erkenntnisse	
	– Keine Kopie der DSGVO: hoher Abstraktionsgrad und Technologieneutralität – Erneute Anerkennung der Datenschutzgleichwertigkeit durch die EU voraussichtlich im Q2 2021 – Keine allgemeine Übergangsfrist: bis 2022 müssen Unternehmen bereit und im Einklang mit dem revidierten DSG sein

NKF

Häufig gestellte Fragen

- **Extraterritorialität des DSG?** Auswirkungsprinzip: Das Gesetz wird auch auf Unternehmen mit Sitz im Ausland anwendbar sein, wenn sie Personendaten bearbeiten und sich diese Datenbearbeitung in der Schweiz auswirkt.
- **Wir sind DSGVO-konform. Haben wir trotzdem noch To Do's?** Ja!
- Es gibt noch **zahlreiche Unterschiede** in Bezug auf die DSGVO:
  - Die Liste der Pflichtinformationen für Betroffene ist in der DSGVO nicht abschliessend
  - Länder, in die Daten exportiert werden, müssen in der DSE aufgeführt sein
  - Keine allgemeine Rechenschaftspflicht (keine Governance-Pflicht), kein Verbot der Datenbearbeitung, wenn kein Rechtfertigungsgrund vorliegt, sondern Bearbeitung ist generell erlaubt, wenn keine Verletzung der Persönlichkeit einer betroffenen Person vorliegt, etc.
  - Unsere Erfahrung zeigt, dass DSGVO oft nicht zu 100 % umgesetzt wurde
- **Wichtigste Änderung**: verschärfte Sanktionen bei Verstössen (bis zu CHF 250'000.-; ad personam)
- **Beste Vorgehensweise**: GAP-Analyse zwischen aktuellem ⇔ Zielzustand

Übersicht der wichtigsten Revisionen I

- DSG nicht mehr anwendbar auf personenbezogene Daten von juristischen Personen (Art. 1)
- DSG anwendbar, wenn Auswirkungen in der Schweiz, auch wenn die Bearbeitung im Ausland stattfindet (Art. 3)
- Neue Terminologie: "Profiling mit hohem Risiko", "Datensicherheitsverletzung", "Verantwortlicher", "Auftragsbearbeiter" (Art. 5)

- Einführung neuer Konzepte des "privacy by design" und des "privacy by default" (Art. 7)
- TOMs zur Vermeidung von Datenschutzverletzungen (Art. 8)
- Freiwillige Bestellung des DPO [*Datenschutzberater*] (Art. 10)
- Verhaltenskodex (Art. 11)
- Verzeichnis von Bearbeitungstätigkeiten (Art. 12)
- Zertifizierung (Art. 13)
- Vertreter (Art. 14)

NKF

Übersicht der wichtigsten Revisionen II

- Erhöhte Informationspflicht bei Erhebung von personenbezogenen Daten (Art. 19-21)
- Datenschutz-Folgenabschätzung (Art. 22, 23)
- Benachrichtigung bei Verletzung der Datensicherheit (Art. 24)
- Recht auf Zugang (Art. 25, 26)

- Datenübertragbarkeit (Art. 28)
- Untersuchung (Art. 49)
- Zuständigkeiten des EDÖB (Befugnisse Art. 50, Massnahmen Art. 51)
- Strafrechtliche Sanktionen (Art. 60-64)
- Zuständigkeit für strafrechtliche Sanktionen (Art. 65)

NKF

Profiling I

- **Persönlichkeitsprofil** (Art. 3 lit. d DSG) vs. **Profiling** (Art. 5 lit. f und f^{bis} revDSG)
  - → mögliches Ergebnis der Datenverarbeitung vs. Form der Datenverarbeitung
- Kriterium der **Automatisierung** → Bearbeitung in elektronischer Form
- Kriterium der **Bewertung** → inhaltliche Auseinandersetzung mit der Datenbasis
- Kein Kriterium: Quantum, d.h. wenige Daten können reichen
- "Swiss Finish": Profiling (Art. 5 lit. f revDSG) vs. Profiling **mit hohem Risiko** (Art. 5 lit. f^{bis} revDSG)

Profiling II

Beispiel 1

Onlineshop, der das Surfverhalten von Nutzern automatisiert (d.h. mit Hilfe von künstlicher Intelligenz oder Algorithmen) analysiert und diesen dann Kaufempfehlungen unterbreitet.

Profiling: Ja

Beispiel 2

Registrierung eines Wohnortwechsels in ein bestimmtes Quartier und Verarbeitung dieser Information mit dem Schluss auf die Bonität dieser Person.

Profiling: Ja

Beispiel 3

Einteilung von Kunden in Alterskohorten.

Profiling: Nein

NKF Compliance Checkliste I

Thema	Artikel im revDSG	Kriterien	Was ist neu?
Geltungsbereich *Ist Ihr Unternehmen betroffen?*	Art. 2, 3	☐ Bearbeitung von Personendaten in der Schweiz ☐ Bearbeitung von Personendaten ausserhalb der Schweiz, aber mit Wirkung in der Schweiz	Territorialer Geltungsbereich: "Auswirkungen" der Datenbearbeitung in der Schweiz lösen die Anwendbarkeit des revidierten DSG aus.
Daten *Welche Art von Daten sind betroffen?*	Art. 5	☐ Personendaten (alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen) ☐ Besonders schützenswerte Personendaten (Daten über religiöse, ideologische, politische, gewerkschaftliche Ansichten oder Aktivitäten; Gesundheit; Intimsphäre; Rasse oder ethnische Herkunft; genetische Daten; biometrische Daten; Daten über Verwaltungs- oder Strafverfahren und Sanktionen; Daten über Massnahmen der sozialen Sicherheit)	Daten von juristischen Personen sind nicht länger durch das revidierte DSG geschützt. Genetische Daten und biometrische Daten (die eine natürliche Person eindeutig identifizieren) sind neu explizit in der Definition der besonders schützenswerten Daten aufgezählt. Die bisherige Pflicht zur Registrierung von Datensammlungen entfällt.
Profiling *Führen Sie ein Profiling durch?*	Art. 5, 6	☐ Profiling: automatisierte Bearbeitung personenbezogener Daten zur Beurteilung bestimmter persönlicher Aspekte einer natürlichen Person ☐ Profiling mit hohem Risiko: Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person darstellt	Profiling ist vergleichbar mit dem "Persönlichkeitsprofil" gemäss geltendem Recht. Für ein Profiling mit hohem Risiko für die Persönlichkeit der betroffenen Person gelten dieselben qualifizierten Anforderungen an die Datenbearbeitung wie für "besonders schützenswerte Personendaten". Das bedeutet insbesondere, dass, sofern eine Einwilligung der betroffenen Person in die Bearbeitung erforderlich ist, diese ausdrücklich erfolgen muss.

NKF Compliance Checkliste II

Datensicherheit *Sind Ihre Daten sicher?*	Art. 7, 8	Der Verantwortliche und der Auftragsbearbeiter müssen die Datensicherheit durch angemessene technische und organisatorische Massnahmen gewährleisten: ☐ Angemessene technische und organisatorische Massnahmen (sog. TOMs) ☐ Umsetzung der Grundsätze "Privacy by Design" und "Privacy by Default"	Neu müssen technische und organisatorische Massnahmen für die Datensicherheit bereits bei der Planung eines Bearbeitungsvorgangs (Privacy by Design) und bei der Programmierung/beim Entwurf der Grundeinstellungen (Privacy by Default) berücksichtigt werden.
Auftragsbearbeitung *Werden die Daten von einem Auftragsbearbeiter bearbeitet?*	Art. 9	☐ Übertragung der Bearbeitung von personenbezogenen Daten an einen Auftragsbearbeiter weiterhin möglich (ausser eine gesetzliche oder vertragliche Geheimhaltungspflicht verbietet dies) ☐ Auftrags-Datenbearbeitungsvertrag muss sicherstellen, dass die Daten durch den Auftragsbearbeiter nur so bearbeitet werden, wie es der Verantwortliche selbst tun dürfte	Keine Änderungen: Wie nach geltendem Recht (Art. 10a) kann die Bearbeitung einem Auftragsbearbeiter übertragen werden, wenn der Verantwortliche sicherstellt, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten und, dass die Personendaten nur in der für den Verantwortlichen selbst zulässigen Weise bearbeitet werden.
Verantwortung *Wer ist innerhalb des Unternehmens für die Einhaltung des Datenschutzes verantwortlich?*	Art. 10	Für die Einhaltung der anwendbaren Datenschutzgesetze ist grundsätzlich der Verwaltungsrat zuständig, da er die Oberleitung einer Gesellschaft innehat. Er kann dies aber an die Geschäftsleitung oder einen betriebsinternen oder -externen Datenschutzverantwortlichen delegieren (welcher unabhängig von der Geschäftsleitung agieren können muss): ☐ Hat das Unternehmen einen Datenschutzberater ernannt? ☐ Wurde eine Person innerhalb des Managements bestimmt, welche die Einhaltung des DSG unterstützt? ☐ Wurde eine Person in jeder jeweiligen lokalen Geschäftseinheit mit der Einhaltung des Datenschutzes beauftragt? ☐ Ist die Unabhängigkeit des Datenschutzberaters sichergestellt und besteht ein klares Pflichtenheft?	Die Verantwortung für die Einhaltung des Datenschutzes verbleibt beim Verantwortlichen. Der interne Datenschutzverantwortliche wird neu als Datenschutzberater bezeichnet. Unternehmen können (müssen aber nicht) einen Datenschutzberater ernennen, der als Kontaktstelle für die betroffenen Personen und für die in der Schweiz für Datenschutzfragen zuständigen Datenschutzbehörden dient.

NKF Compliance Checkliste III

Thema	Artikel im revDSG	Kriterien	Was ist neu?
Verzeichnis *Müssen Sie ein Verzeichnis der Bearbeitungstätigkeiten führen?*	Art. 12	☐ Auflistung aller Bearbeitungstätigkeiten, inklusive des Bearbeitungszwecks, der Datenkategorien, einer Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit, der Angabe der Staaten bei Auslandtransfers von Daten sowie der entsprechenden Garantien etc. ☐ Data Retention Schedule, welcher die Aufbewahrungsdauer der einzelnen Datenkategorien auflistet	Neue Pflicht für den Verantwortlichen und den Auftragsbearbeiter. Der Bundesrat kann Ausnahmen für Unternehmen mit weniger als 250 Mitarbeiter vorsehen, falls deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.
Vertreter *Wer muss einen Vertreter ernennen?*	Art. 14	Verantwortliche mit Wohnsitz/Sitz ausserhalb der Schweiz benennen einen Vertreter in der Schweiz, wenn sie Personendaten von Personen in der Schweiz bearbeiten und die Datenbearbeitung die folgenden Voraussetzungen erfüllt (kumulativ): ☐ die Datenbearbeitung steht im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz; ☐ die Datenbearbeitung erfolgt umfassend und regelmässig und bringt ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich	Neue Pflicht für den Verantwortlichen mit Sitz/Wohnsitz im Ausland.

NKF Compliance Checkliste IV

Thema	Artikel im revDSG	Kriterien	Was ist neu?
Übermittlung von Daten *Was gilt, wenn Personendaten ins Ausland bekanntgegeben werden?*	Art. 16	Rechtliche Grundlagen für den Datentransfer ins Ausland: ☐ Vom Bundesrat anerkannt, dass im betreffenden Staat ein gleichwertiges Datenschutzniveau beseht; sonst ☐ gruppeninterne Datenübertragungsvereinbarungen/Datenschutzvorschriften (sogenannte Binding Corporate Rules) ☐ Anerkannte Standardvertragsklauseln (EU-Musterklauseln oder EDÖB-Mustervertrag)	Keine Änderungen der Grundprinzipien für Datenexporte. Neu erlässt der Bundesrat Angemessenheitsentscheide über das Datenschutzniveau anderer Staaten (bisherige "Staatenliste" des EDÖB entfällt). Die Notifikationspflicht bei Verwendung von genehmigten Standardvertragsklauseln entfällt. Hinweis: Nach dem Schrems-II-Entscheid des EuGH ist der Privacy Shield gemäss EDÖB keine ausreichende Rechtsgrundlage mehr für den Datentransfer in die USA (→ andere Datenschutzmassnahmen umsetzen). Gemäss EDÖB muss für jeden Drittstaat geprüft werden, ob das lokale öffentliche Recht die verwendeten vertraglichen Regelungen (z.B. Standardvertragsklauseln) respektiert.
Informationspflicht *Welche Massnahmen müssen Sie treffen?*	Art. 19	☐ Datenschutzbestimmungen, die der betroffenen Person alle Informationen zur Verfügung stellen, die sie benötigt, um ihre Rechte gemäss dem DSG geltend zu machen; mindestens mitzuteilen sind: (i) die Identität und die Kontaktdaten des Verantwortlichen, (ii) der Bearbeitungszweck, (iii) gegebenenfalls die Empfänger denen Personendaten bekanntgegeben werden, (iv) bei Bekanntgabe ins Ausland den Staat und gegebenenfalls die Garantien (bspw. Binding Corporate Rules), (v) gegebenenfalls die Kategorien der bearbeiteten Personendaten ☐ Cookie-Richtlinie (inkl. Zustimmungspflicht für nicht-technische Cookies)	Im Vergleich zum geltenden Recht bestehen konkrete und erweiterte Informationspflichten mit Bezug auf die Bearbeitung aller Arten von Personendaten.

NKF Compliance Checkliste V

Thema	Artikel im revDSG	Kriterien	Was ist neu?
Datenschutz-Folgenabschätzung (DSFA) *Wann müssen Sie eine DSFA durchführen?*	Art. 22	Wenn die beabsichtigte Bearbeitung zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen kann, muss eine DSFA durchgeführt werden: ☐ Besteht eine Dokumentation zur Durchführung einer DSFA (inkl. Methodik)? ☐ Ist ein Register von durchgeführten DSFA vorhanden?	Neue Pflicht für den Verantwortlichen. Ein hohes Risiko ist insbesondere bei der Verwendung neuer Technologien oder bei umfangreicher Bearbeitung von besonders schützenswerten Personendaten gegeben. Die DSFA muss 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 enthalten.
Verletzung der Datensicherheit *Haben Sie eine Meldepflicht?*	Art. 24	Verfahren zur Benachrichtigung des EDÖB im Falle einer Verletzung der Datensicherheit ("so rasch als möglich"): ☐ Reaktions- und Benachrichtigungsplan (inkl. Benachrichtigungsformular) für mögliche zukünftige Fälle von Verletzungen der Datensicherheit ☐ Ist ein Register vorhanden, in welchem Verletzungen der Datensicherheit dokumentiert werden?	Neue Meldepflicht für den Verantwortlichen, sofern die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Die betroffene Person muss informiert werden, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

NKF Compliance Checkliste VI

Thema	Artikel im revDSG	Kriterien	Was ist neu?
Rechte der betroffenen Person *Welche Rechte müssen Sie beachten?*	Art. 25, 32	Vorsehen interner Verfahren, um auf folgende Rechte der betroffenen Personen zu reagieren: ☐ Auskunftsrechte ☐ Berichtigung von Daten ☐ Löschung von Daten ☐ Entscheidungen auf der Grundlage automatisierter Bearbeitung	Die Rechte der betroffenen Personen werden unter dem revidierten DSG leicht erweitert bzw. spezifiziert. Dies gilt insbesondere für die Rechte betroffener Person in Zusammenhang mit Entscheidungen, welche ausschliesslich auf einer automatisierten Bearbeitung beruhen.
Recht auf Datenportabilität *Müssen Sie Daten an die betroffenen Personen herausgeben?*	Art. 28	☐ Auf Anfrage der betroffenen Person muss der Verantwortliche in der Lage sein, personenbezogene Daten in einem elektronischen Standardformat herauszugeben (sofern der Verantwortliche die Daten automatisiert bearbeitet und die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden)	Neue Pflicht für den Verantwortlichen. Die Daten sind grundsätzlich kostenlos herauszugeben, der Bundesrat kann aber Ausnahmen vorsehen, namentlich wenn der Aufwand unverhältnismässig ist.
Neue Befugnisse des EDÖB/Sanktionen *Welche Massnahmen gewärtigt ein Unternehmen bei einem Verstoss gegen das DSG?*	Art. 51 ff.	Nach dem revidierten DSG kann der EDÖB (von Amtes wegen oder nach Meldung) die Datenbearbeitungstätigkeiten untersuchen und bei Verstössen administrative Massnahmen anordnen (bspw. Einstellung der Bearbeitung). Bei Verletzung von DSG-Pflichten sind die Bussen **persönlich** (bis zu CHF 250'000). Entsprechend sollte geprüft werden: ☐ Umfang der D&O-Versicherung ☐ Spezifische Datenschutzversicherung (Neuabschluss oder Prüfung Umfang)	Prüfen Sie den Versicherungsschutz auf Bussgelder für Datenschutz- und Sicherheitsverletzungen.

Q&A

Ihre Kontakte

Clara-Ann Gordon
clara-ann.gordon@nkf.ch
D +41 58 800 84 26

Dr. András Gurovits
andras.gurovits@nkf.ch
D +41 58 800 83 77

Janine Reudt-Demont
janine.reudt-demont@nkf.ch
D +41 58 800 83 95

Niederer Kraft Frey AG Bahnhofstrasse 53 CH-8001 Zürich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch