NIEDERER KRAFT FREY

Wie Daten nicht zur Straftat werden

Clara-Ann Gordon

Cyber Security Circle, Zürich, 17. Januar 2023

Übersicht

1. Revision des Schweizer Datenschutzgesetzes (revDSG)
2. Allgemeine Bestimmungen DSV
3. TOMs
4. Swiss Finishes
5. Kritikpunkte von Schweizer Unternehmen
6. Herausforderungen der Unternehmen
7. Chancen sehen und Denkanstösse

Revision des Schweizer Datenschutzgesetzes (revDSG)

Revision des Schweizer Datenschutzgesetzes (revDSG)

- Das aktuelle Datenschutzgesetz stammt aus dem Jahr 1992
- Technologische Entwicklungen und die DSGVO erforderten die Überarbeitung
- Parlamentarische Verabschiedung im Herbst 2020
- Verordnung zum DSG (DSV) am 23. Juni 2021 in die Vernehmlassung geschickt
- Bundesrat entschied das revDSG, DSV und Verordnung über Datenschutzzertifizierungen (VDSZ) per 1. September 2023 in Kraft zu setzen

Wichtige Erkenntnisse	
	– Keine Kopie der DSGVO: höherer Abstraktionsgrad, "Swiss approach" – Erneute Anerkennung der Datenschutzgleichwertigkeit durch die EU zu erwarten – Keine allgemeine Übergangsfrist: bis Inkrafttreten müssen Unternehmen bereit und im Einklang mit dem revidierten DSG sein

Übersicht über die wichtigsten Änderungen im revDSG I

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

- Einführung neuer Konzepte des "privacy by design" und des "privacy by default"
- TOMs zur Vermeidung von Datenschutzverletzungen
- Freiwillige Bestellung des DPO [*Datenschutzberater*]
- Verhaltenskodex
- Verzeichnis von Bearbeitungstätigkeiten
- Zertifizierung
- Vertreter

Übersicht über die wichtigsten Änderungen im revDSG II

- Verstärkte Informationspflicht bei Erhebung von personenbezogenen Daten
- Datenschutz-Folgenabschätzung
- Benachrichtigung bei Verletzung der Datensicherheit
- Recht auf Zugang

- Datenübertragbarkeit
- Ermittlungen
- Zuständigkeiten des EDÖB
- Strafrechtliche Sanktionen
- Zuständigkeit für strafrechtliche Sanktionen

Allgemeine Bestimmungen DSV

Allgemeine Bestimmungen DSV (I)

§

- Die revidierte DSV gilt ab **1. September 2023** – keine Übergangsfrist

- Geltungsbereich: Ist Ihr Unternehmen betroffen?

  Bearbeitung von Personendaten in der Schweiz oder ausserhalb der Schweiz aber mit Wirkung in der Schweiz (Art. 2 und 3 revDSG)

  → neu: extraterritoriale Wirkung

- Schutzziele (Art. 2 DSV): Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit

- Schutzbedarfsanalyse (Art. 1 DSV) → je höher der Schutzbedarf, desto strenger sind die Anforderungen an die Massnahmen

- Empfohlene Vorgehensweise: **GAP-Analyse** zwischen aktuellem ⇔ Zielzustand

Allgemeine Bestimmungen DSV (II)

- Allgemeine Massnahmen zur Gewährung der Datensicherheit
  - Anonymisierung, Pseudonymisierung und Verschlüsselung von Personendaten
  - Verfahren zur Identifikation, Bewertung und Evaluierung der Risiken und Überprüfung der Angemessenheit der getroffenen Massnahmen
  - Schulung und Beratung

- Risikobasierter Ansatz, d.h. keine starren Mindestanforderungen, sondern es muss im Einzelfall der Schutzbedarf festgelegt und Massnahmen anhand des Risikos definiert werden

➡ revDSV ist inhaltlich ähnlich, aber weniger detailliert als DSGVO (dafür technologieneutral)

TOMs

TOMs – Allgemeine Grundsätze (I)

- Leitplanke (Art. 8 Abs. 1 und 2 revDSG): Der Verantwortliche **und** der Auftragsbearbeiter gewährleisten durch geeignete technische **und** organisatorische Massnahme eine dem Risiko angemessene Datensicherheit. Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit **zu vermeiden**.
- Technische Massnahmen sind Massnahmen, die technisch implementiert werden (z.B. ein Passwortschutz, Zugangssperren oder eine Transportverschlüsselung)
- Organisatorische Massnahmen setzen beim Menschen an (z.B. durch ein Vieraugenprinzip, Kontrollen oder Schulungen)

→ Technische Massnahmen gelten tendenziell als stärker.

TOMs – Allgemeine Grundsätze (II)

- Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg zu überprüfen und nötigenfalls anzupassen (Art. 1 Abs. 5 DSV). **Je höher das Risiko, desto häufiger ist eine Überprüfung notwendig.**

→ In der DSGVO wird ein Verfahren zur regelmässigen Überprüfung verlangt.

- Massnahmen müssen dem Schutzbedarf entsprechen (vgl. Ziele Art. 2 revDSV)
- Kriterien zur Festlegung (Art. 1 Abs. 4 DSV):
  - Stand der Technik (lit. a): es ist ausreichend Massnahmen zu haben, die sich bereits bewährt haben;
  - Implementierungskosten (lit. b): "Kosten" ist weit zu verstehen und meint (personelle, finanzielle und zeitliche) Ressourcen
- Strafnorm: mit Busse bis zu 250'000 wird bestraft, wer die Mindestanforderungen an die Datensicherheit vorsätzlich nicht einhält (Art. 61 lit. c revDSG)
- In der DSGVO wird bezüglich TOMs dasselbe Datenschutzniveau verlangt

TOMs (I) - Beispiele

Ziel	Massnahme gemäss Art. 3 revDSV	Bedeutung	Praktisches Beispiel
Vertraulichkeit	Zugriffskontrolle	Zugriffsberechtigungen sowie Art und Umfang des Zugriffs bestimmen und beschränken	individuelle Vergabe von Nutzungsrechten, Passwortabfrage nach Inaktivität
	Zugangskontrolle	kein Zugang zu Räumlichkeiten/Anlagen für unbefugte Personen	ständig verschlossene Türen/Fenster, Codeschlösser an Türen, Sicherheitspersonal, Alarmsystem
	Benutzerkontrolle	die Daten sollen nicht in unbefugter Weise benutzt oder weitergegeben werden	regelmässige Kontrollen von Berechtigungen (Sperrung bei Personalwechsel), "Spyware" (insoweit zulässig), Virenschutz/Firewall, VPN

TOMs (II) – Beispiele

Ziel	Massnahme gemäss Art. 3 revDSV	Bedeutung	Praktisches Beispiel
Verfügbarkeit & Integrität	Datenträgerkontrolle	unbefugten Personen das Lesen, Kopieren, Verändern, Verschieben, Löschen oder Vernichten von Datenträgern verunmöglichen; verhindern, dass Personendaten unkontrolliert auf Datenträger übertragen werden können	Verschlüsselung oder Vernichtung von Daten, gesicherte Speicherung von Datenträger, Sperre von USB-Datenträgern
	Speicherkontrolle	unbefugten Personen Zugriff, Einsicht, Veränderung und Löschung von Inhalt des Datenspeichers verunmöglichen	differenzierte Zugriffsberechtigung für Daten, Protokollierung von Zugriffen
	Transportkontrolle	designierter Empfänger erhält Daten in ihrer ursprünglichen Form; unbefugte Dritte können Daten nicht abfangen	Verschlüsselung, sichere Transportbehälter bei physischen Transporten
	Wiederherstellung	Möglichkeit der Wiederherstellung der Verfügbarkeit der Daten und des Zugangs zu den Daten nach einem Zwischenfall	Redundante Datenspeicherung und Backup-Konzept, Sicherungs- und Wiederherstellungssysteme (wie RAID)
	Datenintegrität	Gewährleistung der Stabilität der Systeme; Fehlfunktion soll das System selbst melden; gespeicherte Personendaten sollen nicht durch Fehlfunktionen des Systems beschädigt werden	VPN-Tunnel, Firewall, Erkennung von Feuer und Rauch
	Systemsicherheit	Prozess für die Aktualisierung von Systemen bzw. proaktive Behebung von Schwachstellen	Automatische Aktivierung von verfügbaren Software- und Firmware-Updates

TOMs (III) - Beispiele

Ziel	Massnahme gemäss Art. 3 revDSV	Bedeutung	Praktisches Beispiel
Nachvollziehbarkeit	Eingabekontrolle	nachträglich muss überprüft werden können, welche Daten zu welcher Zeit von welcher Person eingegeben oder verändert wurden	Protokollierung
	Bekanntgabekontrolle	Identifizierung von Datenempfänger	Protokollierung
	Erkennung und Beseitigung	reaktive Massnahme, dass Verletzungen rasch erkannt werden und Massnahmen zur Minderung bzw. Beseitigung der Folgen ergriffen werden können	

Swiss Finishes

Swiss Finishes – revDSG vs. DSGVO (I)

- Extraterritorialer Geltungsbereich:
  - anwendbar z.B. auf Unternehmen mit Sitz im Ausland
  - wenn Auswirkung der Datenbearbeitung auf die Schweiz

- Erweiterte Informationspflichten:
  - bei Datenübermittlung ins Ausland → zwingend anzugeben sind:
    - der Staat oder die internationale Einrichtung
    - ggf. Garantien

Swiss Finishes - revDSG vs. DSGVO (II)

- Meldepflicht bei Verletzung der Datensicherheit:
  - Verletzung führt voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person
  - Meldefrist: keine im Gesetz («so rasch als möglich»)
  - Meldung grds. nur an EDÖB; Meldung zusätzlich an betroffene Person(en), wenn es zu ihrem Schutz erforderlich ist oder es der EDÖB verlangt

Swiss Finishes - revDSG vs. DSGVO (III)

- Strengere Sanktionen:
  - ad personam Busse von bis zu CHF 250'000
  - sanktionierte Delikte: z.B. Nichtnennung des Landes, in das die personenbezogenen Daten bekanntgegeben werden; Verletzung des Rechts auf Auskunft; Verstoss gegen die Pflicht zur Gewährleistung ausreichender Datensicherheit

Kritikpunkte von Schweizer Unternehmen

Kritikpunkte von Schweizer Unternehmen

- Wieso ist eine Revision des DSG überhaupt notwendig?
- Swiss Finish – über die Anforderungen der DSGVO hinausgeschossen. Schweizer Unternehmen schon genug schwer belastet mit Parallelanwendung DSGVO und DSG
- Abschieben der Datenschutzaufsicht und Verantwortung auf Unternehmen
- Mehrarbeit für Schweizer Unternehmen auf diversen Ebenen:
  - Datenschutz-Governance – interner und externer Beratungsaufwand und Arbeit
  - Betriebsinterne Massnahmen zur Sicherstellung des Datenschutzes
  - Erhöhung der Interaktionen mit Datensubjekten (stark erweiterte Informations- und Auskunftspflichten) – vor allem für KMU eine starke Belastung
  - Verfügungskompetenz und Untersuchungsmöglichkeiten des EDÖB führt zu Mehrarbeit für Unternehmen

Herausforderungen der Unternehmen

Welche Herausforderungen bei der Umsetzung?

- Management der persönlichen Daten und die Bildung eines Verzeichnisses von Bearbeitungstätigkeiten (Data Mapping)
- Umgang mit unstrukturierten Daten
- Wie geht Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellung?
- Compliance mit Anfragen zur Datenlöschung (right to be forgotten)
- Ausbau der Löschungskapazitäten und Prinzipien der Speicherbegrenzung
- Wie Datenschutz-Rechte für Datensubjekte umsetzen?
- Daten- und Cybersicherheit erhöhen
- Etc.

Chancen sehen und Denkanstösse

Herausforderungen… aber auch Chancen

- Aufmerksamkeit (Awareness) des Managements: Datenschutz ist Compliance!
- Internes «Aufräumen» und sich bewusst werden der internen Datenbearbeitungen und Datensammlungen
- Optimierung der internen Datenverwaltung
- Einführung von neuen Softwareprogrammen
- Durch notwendige IT-Umstellungen bessere Organisation der Kundendaten und 360-Grad-Sicht auf Mitarbeiter, Kunden oder Bürger
- Bessere Interaktion und Kommunikation mit Kunden - Vertrauensgewinn
- Mehr Sicherheit in Sachen digitaler und physischer Zutritt zu Daten
- Neue Marketing-Möglichkeiten mit verbesserter Datenverwaltung

Denkanstösse für Unternehmen

- Seriöse Auseinandersetzung mit der Implementierung der neuen Bestimmungen hat Einfluss auf Arbeitsabläufe, internen und externen Prozesse und die Kultur im Unternehmen generell
- Anpassungen, die im Laufe der Übernahme des revDSG gemacht werden müssen, sind eine Investition in die Zukunft
- Transformationsprozesse führen zu Raum für die wirklich wichtigen Tätigkeiten: nämlich weniger Ablage und Archivierung, mehr Kundenkontakt, mehr Wertschöpfung
- Vorteile beim Aufbruch in die Digitalisierung generieren
- … und schliesslich Reputation stärken: Datenschutz im Markenkern=Wettbewerbsvorteil! Konsumenten wollen Schutz der Privatsphäre!

Weitere Hinweise

Checkliste NKF zum revDSG, abrufbar unter:

de-nkf-client-news-revidiertes-bundesgesetz-uber-den-datenschutz-02122020.pdf

Newsletter NKF zu einer risiko-basierten Umsetzung des revDSG, abrufbar unter:

de-client-news-anpassungen-und-massnahmen-unter-dem-neuen-dsg-final.pdf

Vielen Dank für Ihre Aufmerksamkeit!

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

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