NIEDERER KRAFT FREY

asut

Data Center und Datensicherheit

Die neue Datenschutzverordnung (DSV)

Clara-Ann Gordon

Zürich – 20. Juni 2023

1. Einleitung
2. Die Rolle des Data Centers bei der Datenbearbeitung
3. TOMs
4. Meldepflicht gegenüber dem EDÖB
5. Bussen
6. Fazit

Einleitung

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)

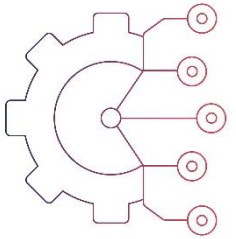
  → neu: extraterritoriale Wirkung

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

- Schutzbedarfsanalyse (Art. 1 revDSV) → 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

→ DSV ist inhaltlich ähnlich, aber weniger detailliert als die DSGVO (dafür technologieneutral)

Die Rolle des Data Centers bei der Datenbearbeitung

Rolle des Data Centers bei der Datenbearbeitung

- Ausgangspunkt: Welches sind die Dienstleistungen des Data Centers?
  - Webhosting? E-Mail Hosting? Back-up? Dedicated Server? SLA? Etc.
- Meistens ein Auftrag oder auftragsähnlicher Vertrag (AGB)
- Zugriff auf Kundendaten ausgeschlossen? Möglich? Aus technischen Gründen notwendig?
- Auftragsdatenbearbeiter? Verantwortlicher?
- Data Center wird verpflichtet, Datensicherheit zu gewährleisten
- TOMs des Data Centers entscheidend
- DSG auf Data Center anwendbar, aber auch sektorspezifische Bestimmungen (FINMA), Straftatbestände sowie Geheimhaltungspflichten

TOMs

TOMs – Allgemeine Grundsätze (I)

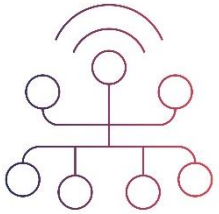
- Leitplanke (Art. 8 Abs. 1 und 2 revDSG): Der Verantwortliche **und** der Auftragsbearbeiter gewährleisten durch geeignete technische **und** organisatorische Massnahme eine dem Risiko angemessene Datensicherheit. Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit **zu vermeiden**
- 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.

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

→ In der DSGVO wird ein Verfahren zur regelmässigen Überprüfung verlangt

TOMs – Allgemeine Grundsätze (II)



- Massnahmen müssen dem Schutzbedarf entsprechen (vgl. Ziele Art. 2 revDSV)
- Kriterien zur Festlegung (Art. 1 Abs. 4 revDSV):
  - 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 – Vertraulichkeit

- **Zugriffskontrolle**: die Zugriffsberechtigungen und die Art wie auch der Umfang des Zugriffs wird bestimmt
  - z.B. individuelle Vergabe von Nutzungsrechten, Passwortabfrage nach Inaktivität
- **Zugangskontrolle**: kein Zugang für unbefugte Personen zu den Räumlichkeiten bzw. Anlagen
  - z.B. ständig verschlossene Türen/Fenster, Codeschlösser an Türen, Sicherheitspersonal
- **Benutzerkontrolle**: die Daten sollen nicht in unbefugter Weise benutzt oder weitergegeben werden
  - z.B. regelmässige Kontrollen von Berechtigungen (Sperrung bei Personalwechsel), "Spyware" (insoweit zulässig), Virenschutz/Firewall

TOMs – Verfügbarkeit und Integrität (I)

- **Datenträgerkontrolle**: unbefugten Personen das Lesen, Kopieren, Verändern, Verschieben, Löschen oder Vernichten von Datenträgern verunmöglichen; verhindern, dass Personendaten unkontrolliert auf Datenträger übertragen werden können
  - z.B. Verschlüsselung oder Vernichtung von Daten, gesicherte Speicherung von Datenträgern
- **Speicherkontrolle**: verunmöglichen, dass unbefugte Personen auf den Inhalt des Datenspeichers Zugriff haben, diesen einsehen, verändern oder löschen können
  - z.B. differenzierte Zugriffsberechtigung für Daten, Protokollierung von Zugriffen
- **Transportkontrolle**: designierter Empfänger muss Daten in ihrer ursprünglichen Form erhalten und keine Dritte sollen die Daten unbefugt abfangen können
  - z.B. Verschlüsselung, sichere Transportbehälter bei physischen Transporten

TOMs – Verfügbarkeit und Integrität (II)

- **Data Recovery**: Möglichkeit der Wiederherstellung der Verfügbarkeit der Daten und des Zugangs zu den Daten nach einem Zwischenfall
  - z.B. Backup-Konzept, Sicherungs- und Wiederherstellungssysteme (wie RAID)

- **Zuverlässigkeit**: Gewährleistung der Stabilität der Systeme; Fehlfunktion soll das System selber melden; gespeicherte Personendaten sollen nicht durch Fehlfunktionen des Systems beschädigt werden
  - z.B. VPN-Tunnel, Firewall, Erkennung von Feuer und Rauch

- **Systemsicherheit**: Prozess für die Aktualisierung von Systemen bzw. proaktive Behebung von Schwachstellen
  - z.B. Aktivierung von verfügbaren Software- und Firmware-Updates

TOMs – Nachvollziehbarkeit

- **Eingabekontrolle**: nachträglich muss überprüft werden können, welche Daten zu welcher Zeit von welcher Person eingegeben oder verändert wurden
  - z.B. Protokollierung
- **Bekanntgabekontrolle**: Identifizierung von Datenempfänger
  - z.B. Protokollierung
- **Erkennung/Beseitigung**: reaktive Massnahme, dass Verletzungen rasch erkannt werden und Massnahmen zur Minderung bzw. Beseitigung der Folgen ergriffen werden können

TOMs – Beispiele (I)

Ziel	Massnahme gemäss Art. 3 DSV	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 – Beispiele (II)

Ziel	Massnahme gemäss Art. 3 DSV	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 – Beispiele (III)

Ziel	Massnahme gemäss Art. 3 DSV	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	

Meldepflicht gegenüber dem EDÖB

Meldung Datensicherheitsverletzung (I)

- Der Verantwortliche meldet dem EDÖB (und der Auftragsbearbeiter = Data Center dem Verantwortlichen) so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt (Art. 24 Abs. 1 und 3 revDSG)

- Eine Verletzung der Datensicherheit liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 5 lit. h revDSG)

- Bezüglich dem hohen Risiko erfolgt eine Einzelfallbeurteilung
  - Ist eine schwere negative Folge mindestens wahrscheinlich oder eine mittelmässige negative Folge sehr wahrscheinlich, ist das Risiko hoch
  - Methodik der Risikoberechnung = Eintrittswahrscheinlichkeit x Schadenshöhe

Meldung Datensicherheitsverletzung (II)

— Der Verantwortliche muss die Verletzungen dokumentieren

— Die Dokumentation muss die mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten (Art. 15 Abs. 4 revDSV)

— Die Dokumentation ist ab dem Zeitpunkt der Meldung mindestens zwei Jahre aufzubewahren (Art. 15 Abs. 4 revDSV)

— Der EDÖB arbeitet derzeit an der Entwicklung einer webbasierten Meldeoberfläche, voraussichtlich in Form eines **interaktiven Formulars**

Meldepflicht – Unterschiede zur DSGVO

Notifikation	DSGVO (Art. 33/34)	revDSG (Art. 24) / revDSV (Art. 15)
Datenschutzbehörde	- Unverzüglich und möglichst binnen 72 Stunden - Ausser falls voraussichtlich kein Risiko	- So rasch als möglich - Falls voraussichtlich hohes Risiko
Betroffene Person	- Unverzüglich - Falls voraussichtlich hohes Risiko	- Falls zum Schutz der betroffenen Person notwendig - Falls vom EDÖB verlangt
Sanktion bei Unterlassung	- Busse bis zu EUR 10 Mio. bzw. 2% Jahresumsatz	N/A

Bussen

Bussgelder

Strengere Sanktionen ab 1. September 2023:

– 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

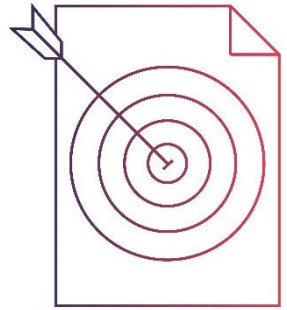
– Strafnorm: mit einer Busse bis zu CHF 250'000 wird bestraft, wer die Mindestanforderungen an die Datensicherheit vorsätzlich nicht einhält

Fazit

Fazit

Data Center spielen zentrale Rolle bei der Einhaltung der Eckpfeiler des Datenschutzes:

Vertraulichkeit – Integrität – Verfügbarkeit



- Ohne physische Sicherheit gibt es keine Integrität
- Data Center tragen Verantwortung
- Sicherheit mit Prozessen gewährleisten
- Data Center haben auch Meldepflichten

Unsere Newsletter

Checkliste NKF zum revDSG:
https://drive.google.com/file/d/1e7ABHuUWl9KpLpVz1YjFLSz2vsivKLbu/view

Newsletter NKF zu einer risiko-basierten Umsetzung des revDSG:

https://drive.google.com/file/d/1Zas79OyTkw5e2p-HmLnEYSfIv9v6LYnu/view

Vielen Dank für Ihre Aufmerksamkeit! Fragen?

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