VISCHER

Das neue Schweizer Datenschutzgesetz: Ein Vergleich mit der EU-DSGVO

David Rosenthal
20. Oktober 2020

Die Schweiz macht es besser!

Text: bit.ly/34PmN9h
(Vergleich: datenrecht.ch)

- Das revidierte Schweizer Datenschutzgesetz ("DSG") tritt aller Wahrscheinlichkeit (Mitte) **2022 in Kraft**
- Prinzipienbasiert, viel weniger detailliert als die DSGVO
- Regelt Datenbearbeitungen durch die Privatwirtschaft und die Schweizer Bundesbehörden (wir behandeln hier nur Ersteres)
- **In Kürze:** Wer die Vorgaben der DSGVO bereits erfüllt, wird mit dem revidierten DSG keine allzugrosse Mühe haben
- Worüber ich sprechen werde:
 - Wichtige konzeptionelle Unterschiede zur DSGVO
 - Fälle, in denen das DSG strenger bzw. weniger streng ist
 - Fälle, in denen das DSG vergleichbar ist mit der DSGVO

Welche Bearbeitungen sind zulässig?

Keine
Anpassungen

DSGVO

- Bearbeitungsgrundsätze
 - Transparenz, Zweckbindung, Fairness, Datenminimierung, begrenzte Speicherfristen, Datenrichtigkeit, Datensicherheit
- Rechtsgrund erforderlich
 - Vertrag, gesetzliche Verpflichtung, Einwilligung, berechtigtes Interesse, etc.

Revidiertes DSG

- Dieselben Bearbeitungsgrundsätze
- Aber: Im Normalfall ist kein Rechtsgrund erforderlich
 - Nur dann, wenn Grundsätze *nicht* eingehalten werden, Dritten bes. schützenswerte Daten offenbart werden oder die betroffene Person der Bearbeitung widerspricht
 - DSG weniger eingeschränkt bei den Rechtfertigungsgründen für die Bearbeitung sensibler Daten

Wann ist eine Einwilligung gültig?

Keine
Anpassungen

DSGVO

- Einwilligung nur nach vorgängiger Information, für den bestimmten Fall, freiwillig und unmissverständlich
- Keine vorangekreuzten Kästchen
- Koppelungsverbot (mit Vertrag), ausser wo für Vertragserfüllung nötig
- Zwingender Hinweis auf das Recht auf Widerruf
- Widerruf ist jederzeit; i.d.R. keine Berufung auf berechnete Interessen

Revidiertes DSG

- Freiwillig auf informierter Basis
- vorangekreuzte Kästchen zulässig, sofern dem Formular als solchen mittels Knopfdruck zugestimmt wird
- Abgabe im Rahmen eines Vertrags zulässig, sofern sachlicher Bezug
- Hinweis auf Widerruf nicht nötig
- Widerruf kann eingeschränkt werden (z.B. bei geschäftlichen Nutzungen)

Geltungsbereich

Anwendbarkeit
prüfen

DSGVO

- Verarbeitung von Daten einer identifizierten oder identifizierbaren Person
- Automatische Verarbeitungen; manuelle nur bei Datensammlungen
- Haushaltsausnahme ($\neq$ beruflich)
- Anwendung ausserhalb EWR, wenn
 - Targeting von Personen im EWR betr. Waren/Dienstleistungen
 - Verhaltensbeobachtung im EWR

Revidiertes DSG

- Dieselbe Definition (Personendaten)
 - Nicht mehr: juristische Personen
- Sämtliche automatischen und manuellen Bearbeitungen erfasst
- Ausnahmen für persönliche Zwecke (privat und beruflich)
- Keine Anwendung in Rechtsverfahren
- Extraterritorialität sofern Aktivitäten, Verantwortliche, Auftragsbearbeiter oder betroffene Personen in Schweiz

Informationspflichten

DSE
anpassen

DSGVO

- Erhebung von Personendaten löst Informationspflicht gegenüber betroffenen Person aus (Mitteilung der Datenschutzerklärung, "DSE")
- DSGVO 13 ff. definiert Mindestinhalt der Datenschutzerklärung
- Gilt auch, wenn Personendaten via Dritte erhoben werden
- Nur sehr wenige Ausnahmen

Revidiertes DSG

- Ähnliche Pflichten bei der Sammlung von Personendaten
- Liste des Mindestinhalts einer DSE ist kürzer; Informationen gem. DSGVO 13(2) nur ausnahmsweise nötig
- Mehr Ausnahmen (z.B. für gesetzlich geregelte Datenbearbeitungen)
- **Aber:** Anzugeben sind alle Länder, in welche Personendaten übertragen werden (inkl. Grundlage für Exporte in unsichere Länder)

Auskunftsrecht

Eigene Richtlinien erstellen

DSGVO

- Verantwortlicher gibt der betroffenen Person auf Nachfrage:
 - Kopie ihrer Personendaten
 - gewisse Zusatzinformationen
- Betroffene Person kann eine Kopie ihrer Daten verlangen
- Verweigerung offensichtlich unbegründeter/exzessiver Anfragen oder Verlangen einer Gebühr
- Ausnahmen zum Schutz von Dritten und Geschäftsgeheimnissen

Revidiertes DSG

- Gleiches Konzept, aber
 - kürzere Liste der einforderbaren Zusatzinformationen
 - zusätzlich Angaben zu Exporten (Länderliste, Rechtsgrundlagen)
 - Recht, weitere nützliche Informationen zu verlangen
- Gebühren? Noch unklar
- Schwacher Schutz von Geschäftsgeheimnissen

Andere Betroffenenrechte

Keine
Anpassungen

DSGVO

- Recht auf Berichtigung
- Recht auf Löschung/Vergessen
- Recht auf Einschränkung
- Recht auf Widerspruch
- Recht auf Datenübertragbarkeit
- Pflicht, Dritte über die erfolgte Ausübung dieser Rechte zu informieren

Revidiertes DSG

- Vergleichbare Betroffenenrechte
- Schweizer Version des Rechts auf Widerspruch umfasst bereits das Recht auf Löschung/Einschränkung
 - Kann von überwiegenden privaten Interessen verdrängt werden
- Nur wenige Ausnahmen vom Recht auf Berichtigung (Rechtspflicht, Archiv im öffentlichen Interesse)
- Keine Pflicht Dritte zu informieren

Verantwortliche, Auftragsverarbeiter

Verträge
anpassen

DSGVO

- DSGVO 28(3) legt den Mindestinhalt von Auftragsdatenverarbeitungs-Verträgen ("ADV") fest
- Beizug von Unterauftragsverarbeiter nur mit Genehmigung des Verantwortlichen
- DSGVO 26 verlangt vertragliche Festlegung der Verantwortlichkeiten von gemeinsamen Verantwortlichen
- Auftragsverarbeiter haften beschränkt

Revidiertes DSG

- Übernahme der Begrifflichkeit Verantwortlicher/Auftragsbearbeiter
- Weniger detaillierte Inhaltvorgaben für ADV; sollten angepasst werden
 - Verweise auf DSG und Länder-Liste (Datenexporte) hinzufügen
- Keine explizite Vertragspflicht von gemeinsamen Verantwortlichen
- Haftung aller die "mitwirken" an einer Persönlichkeitsverletzung

Datenschutzbeauftragter, Vertreter

Keine
Anpassungen

DSGVO

- Datenschutzbeauftragter ("DSB") bestellen für Verarbeitungen mit
 - regelmässiger/systematischer Überwachung oder
 - vielen sensitiven Daten
- DSGVO definiert die Unabhängigkeit, den Status, die Aufgaben und andere Voraussetzungen eines DSB
- Ausländische Verantwortliche/ Auftragsverarbeiter müssen unter gewissen Voraussetzungen einen Vertreter in der EU bestellen

Revidiertes DSG

- Keine Pflicht zur Bestellung DSB
- DSG kennt die ähnliche Rolle des "Datenschutzberaters"
 - Voraussetzungen vergleichbar
 - kann DSFAs anstelle der Aufsichtsbehörde beurteilen
- Pflicht zur Bestellung eines lokalen Vertreters, wo Verantwortliche sich auf Personen in der Schweiz ausrichten oder diese beobachten und umfang- und hochrisikoreiche Bearbeitungen haben

Datensicherheit, Privacy by Design

Keine
Anpassungen

DSGVO

- Technische und organisatorische Massnahmen für ein dem Risiko angemessenes Datenschutzniveau
- Massnahmen zur Einhaltung anderer Vorschriften ("Privacy by Design")
- "Privacy by Default"
 - Standardmässige Beschränkung der Verarbeitung auf ein Minimum
 - Keine Veröffentlichung ohne Zustimmung der betroffenen Person

Revidiertes DSG

- Das DSG verlangt dasselbe Datenschutzniveau
- Ähnliche Pflichten bezüglich "Privacy by Design"
- "Privacy by Default"
 - Pflicht, dass Voreinstellungen die am wenigsten invasive Einstellung bezüglich Privatsphäre aufweisen
 - Es kann mit dem Endbenutzer etwas anderes vereinbart werden

Automatisierte Einzelentscheide

Keine
Anpassungen

DSGVO

- Anspruch, keiner automatisierten Entscheidung/Profiling mit negativen rechtlichen oder tatsächlichen Folgen ausgesetzt zu sein
- Solche Entscheidungen sind aber erlaubt für den Abschluss oder die Erfüllung eines Vertrags, sofern per Gesetz erlaubt oder mit Einwilligung
 - Recht auf "menschliches Gehör"
 - Informationspflicht

Revidiertes DSG

- Gleiche Definition automatisierter Einzelentscheide, jedoch ohne die Erwähnung von "Profiling"
- Kein Verbot oder dergleichen
- Ähnliches Recht auf menschliches Gehör und Information, es sei denn die Entscheidung erfolgt
 - so wie von der betroffenen Person gewünscht (z.B. im Online-Shop) oder
 - mit ihrer Einwilligung

Data Breach Notifications

**Abläufe
anpassen**

DSGVO

- Verletzung des Schutzes von Personendaten = ungeplanter Bruch der Vertraulichkeit, Integrität oder Verfügbarkeit persönlicher Daten
- Meldung von Verletzungen mit dem Risiko negativer Folgen für die Betroffenen an die Datenschutz-Behörde innerhalb von 72 Stunden
- Meldung an betroffene Person bei Vorliegen hohen Risikos
- Auftragsverarbeiter muss jede Verletzung dem Verantwortlichen mitteilen

Revidiertes DSG

- Verletzung der Datensicherheit gleich definiert wie in der DSGVO
- Auftragsverarbeiter: Wie DSGVO
- Verantwortliche: Meldung an Behörde nur bei hohem Risiko
- Keine 72-Stunden-Frist, keine Pflicht zur Protokollierung der Verletzungen
- Meldung an betroffene Person, falls es "zu ihrem Schutz erforderlich" ist
- Ausnahme bei übermässigem Aufwand

Regeln für Datenexporte

*Andere, aber
ähnliche Abläufe*

DSGVO

- Keine Übermittlung in Länder ohne angemessenes Datenschutzniveau (ausser Vorliegen einer Ausnahme oder einer Schutzmassnahme)
- EK entscheidet über Angemessenheit
- Übliche Schutzmassnahmen: Standard-Vertragsklauseln ("SCC"), Binding Corporate Rules ("BCR")
- Ausnahmen u.A. bei Einwilligung oder für Vertragserfüllung oder im Rahmen von Behörden- und Gerichtsverfahren

Revidiertes DSG

- Dasselbe Konzept
- Knüpft an Übermittlung über die Schweizer Grenzen hinaus an
- Angemessenheit bestimmt durch Bundesrat (folgt der EU)
- Verwendung von EU SCC und BCR im Rahmen des DSG grundsätzlich möglich
- Ähnliche Ausnahmen

Dokumentationspflichten

**Kleine
Anpassungen**

DSGVO

- Verzeichnis der Verarbeitungstätigkeiten
 - für Verantwortliche/Auftragsver.
 - definierter Inhalt
- Rechenschaftspflicht (DSGVO 5(2))
- Datenschutz-Folgenabschätzung
 - für Verarbeitungen mit vermutungsweise hohem Risiko
 - Pflicht, die Aufsichtsbehörde zu konsultieren bei hohem Risiko trotz getroffener Massnahmen

Revidiertes DSG

- Selbes Verzeichnis verwenden
 - Auflistung der Exportländer und Rechtsgrundlagen
- Vergleichbare Pflicht zur Vornahme Datenschutz-Folgenabschätzung
 - Rechtsgrundlage muss darin nicht genannt werden
 - Konsultation eines DSB andstelle des EDÖB möglich
- Keine Rechenschaftspflicht

Berufsgeheimnis

**persönliche
Strafbarkeit**

DSGVO

- Gibt es in der DSGVO so nicht

Revidiertes DSG

- Schweigepflicht für alle Berufsleute
 - für in Ausübung des Berufes erfasste geheimer Personendaten
 - sofern deren Kenntnis für die Ausübung des Berufes nötig ist
- Nur vorsätzliches Handeln erfasst
- Schutz der Kunden; Verzicht ist möglich, aber nicht immer nötig
- Persönliche Busse bis CHF 250'000

Busse!

Durchsetzung und Bussen

**persönliche
Strafbarkeit**

DSGVO

- Datenschutz-Aufsichtsbehörden können
 - Verarbeitungsvorgänge untersuchen
 - Verfügungen zur Einstellung, Einschränkung oder Anpassung einer Verarbeitung erlassen
 - Für die meisten Verstösse: Bussen bis EUR 10/20 Mio. oder 2/4% des weltweit erzielten Jahresumsatzes
- Ev. weitere Bussen gemäss lokalem Recht

Revidiertes DSG

- Die Datenschutz-Aufsichtsbehörde (EDÖB) kann
 - Bearbeitungsvorgänge untersuchen
 - Verfügungen zur Einstellung, Einschränkung oder Anpassung der Verarbeitung erlassen
- Kantonale Strafbehörden können
 - Persönliche Bussen bis CHF 250'000 verfügen für Verletzung gewisser DSG-Bestimmungen und mangelnde Kooperation mit dem EDÖB
 - Bussen sind nicht versicherbar

Busse!

Schlussbemerkungen

- Einhaltung des Datenschutzes in der Schweiz wird mit dem revidierten Gesetz **aufwändiger** (mehr Governance)
- Risiko der persönlichen Strafbarkeit wird die mit dem Datenschutz betrauten Einzelpersonen (und ihre Berater) **vorsichtiger** machen als bisher
- Die Vorgaben sind vergleichbar mit jenen der DSGVO, doch hat die Schweiz **einen pragmatischeren Ansatz** gewählt, was sich im Tagesgeschäft auszahlt
- Differenzen zwischen der DSGVO und dem DSG werden oft erst im Umgang mit **Einzelfällen** (z.B. bei Streitigkeiten über das Auskunftsrecht) von Relevanz sein
- Keiner kann das DSG vollständig einhalten – das bleibt so

VISCHER

Anmeldung zu Updates unseres
Data & Privacy Blogs auf
www.vischer.com

Vielen Dank für die Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Zürich

Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

www.vischer.com

Basel

Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf

Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

Kontaktieren Sie mich per E-Mail, falls Sie eine Kopie meines ausführlichen Kommentars zu den neuen Bestimmungen erhalten möchten (erscheint im November).

Übersicht: <https://bit.ly/2SYo2xv>