VISCHER

Datenschutzgesetz konkret.

Damit es mit der Umsetzung in der Praxis klappt

Sarah Bischof, VISCHER AG
29. März 2022

Die Ausgangslage

Kostenlose Kommentierung: https://bit.ly/3kUfzqu

- Am **1. September 2023** tritt das neue Datenschutzgesetz in Kraft (DSG)
  - Den Text finden Sie hier: https://bit.ly/34PmN9h
  - Noch fehlen die Verordnungen dazu
- Die Schweiz schliesst im Datenschutz zur EU auf
- Aber: Materiell **keine fundamentale Veränderung**
  - Bisher rechtmässige Bearbeitungen i.d.R. weiterhin erlaubt
  - Keine Kopie der EU-Datenschutz-Grundverordnung (DSGVO), aber Diverses übernommen
  - Ausgebaut werden vorwiegend die Governance und Betroffenenrechte
- Auch **kantonale Datenschutzgesetze** werden revidiert

Bundesrecht und kantonales Recht

Bundesgesetz über den Datenschutz

Private

Bundesorgane

Kantonale Datenschutzgesetze

Kantonale Organe

Damit wir vom Selben reden…

- **Personendaten** – nur Daten, die Rückschlüsse auf die Identität des Menschen erlaubt, um den es geht
  - Das DSG gilt nur für den, der Personendaten bearbeitet
- **Besonders schützenswerte Personendaten** – bestimmte Arten von Personendaten (z.B. Gesundheitsdaten oder Daten über soziale Hilfe)
- **Profiling** – Ein Computer bewertet einen Menschen
  - Profiling als solches wird (für Privatwirtschaft) kaum reguliert
- **Profiling mit hohem Risiko** – Profiling, welches zu einem Persönlichkeitsprofil führt (?)
  - Einwilligungen müssen ausdrücklich sein (falls erforderlich)

IP Adressen sind i.d.R. keine Personendaten! bit.ly/35TRzzC

z.B. Auswertung von Daten nach Affinität

ausdrücklich = beim Namen genannt

Was Sie tun müssen…

- … wenn Sie Personendaten **beschaffen**
  - Gegenüber der betroffenen Person klarmachen, wozu Sie dies tun (=bisher) und auf Datenschutzerklärung hinweisen (=neu)
  - Nur zwingend notwendige Daten erheben (z.B. Eingabemasken bereits so gestalten)
- … wenn Sie Personendaten **bearbeiten**
  - Nur für jene Zwecke verwenden, die Sie angegeben haben
  - Stoppen, wenn jemand widerspricht (z.B. «Ich will keine Werbung mehr»)
  - Daten berichtigen oder löschen, wenn nicht mehr aktuell bzw. nicht mehr benötigt

Betroffene Person kann Auskunft verlangen

Datenschutzerklärung

- **Informationspflicht -** jede direkte und indirekte Datenbeschaffung
- **Gesetzlicher Minimalinhalt** betreffend was geplant ist
  - Identität und Kontaktdaten des Verantwortlichen
  - Bearbeitungszweck
  - Kategorien von Empfängern (Dienstleister, Behörden etc.)
  - Beschaffte Daten (soweit aus Drittquellen)
  - Exportländer («Europa», «weltweit») und Grundlage für Export
- Weitere Informationen, wenn aus **Transparenzgründen notwendig**
- DSE muss mitgeteilt werden; Hinweis mit Link genügt i.d.R.
- **Keine Einwilligung** in die DSE!

Was Sie tun müssen…

- … wenn Sie Personendaten an Dritte **weitergeben**
- Eine Weitergabe an Dritte (für deren Zwecke) erfordert nur dann eine **Einwilligung**, falls…
  - sie nicht in der DSE oder sonst erwähnt war oder
  - sie als unverhältnismässig erscheint oder
  - es um besonders schützenswerte Personendaten geht
- **Information** in der DSE ist so oder so Pflicht
  - Kategorien von Empfängern (i.d.R. ohne Namensnennung)
  - Nutzung von Daten für Werbezwecke Dritter erwähnen
- Anvertraute geheime Daten: **Neues Berufsgeheimnis** beachten

Kooperation mit Dritten

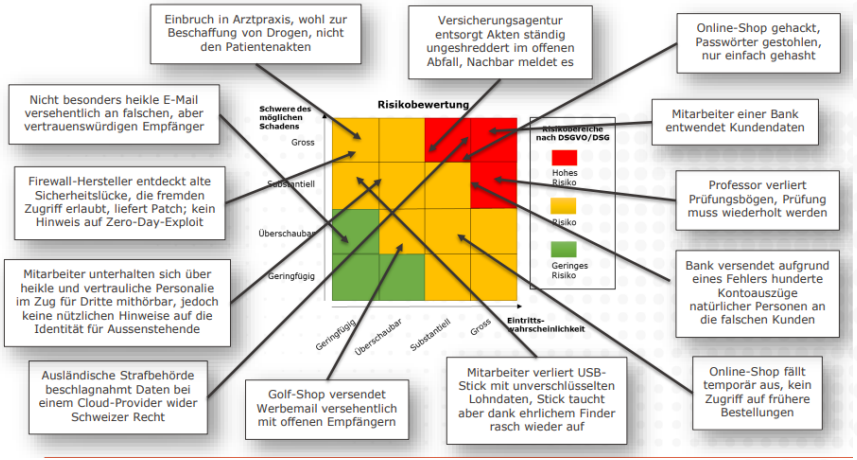
- Revidiertes DSG übernimmt Konzept vom «**Controller**» und «**Processor**» aus der DSGVO
  - Verantwortlicher bestimmt Zweck und Mittel der Datenbearbeitung
  - Wer zusammen mit anderen den Zweck und Mittel einer Datenbearbeitung bestimmt, ist gemeinsam verantwortlich («Joint Controller»)
  - Auftragsbearbeiter bearbeitet Daten nur für Zwecke des Verantwortlichen und gemäss dessen Weisungen (= Cloud Provider mit CRM-Lösung)
- Braucht es einen **Vertrag**?
  - Ja, im Falle eines Auftragsbearbeiters oder Export ins Ausland
  - Im Falle einer gemeinsamen Verantwortung rechtlich nicht, aber Regelung der Datenverwendung wird empfohlen
- Information in DSE über Kooperation mit Dritten

Neue Dokumentationspflichten

- Führung eines **Verzeichnisses aller Bearbeitungstätigkeiten**
  - Pflicht von Verantwortlichen (umfassend) und Auftragsbearbeiter (reduziert)
  - «Bearbeitungstätigkeit» im Gesetz nicht definiert
  - Basis für die gesamte Datenschutz-Compliance
- Erstellung von **Datenschutz-Folgenabschätzungen**
  - Bei allen heiklen Datenbearbeitungs-Vorhaben
  - Dokumentation der (i) Datenbearbeitung und Massnahmen zum Schutz der Daten, (ii) der Risiken (d.h. Nachteile) für betroffene Personen, (iii) etwaiger noch nötiger Massnahmen, (iv) Beurteilung, ob trotz Massnahmen ein «hohes Risiko» vorliegt (wenn ja → Konsultation EDÖB)
  - **Keine einmalige** Aufgabe

Neue Meldepflicht bei Datensicherheitsverletzung

- Unplanmässige Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit der Daten (d.h. nicht jede Daten**schutz**verletzung)
- Meldung an EDÖB, falls hohes Risiko für die betroffenen Personen



Die Sanktionen

- Neu drohen Bussen bis zu **CHF 250’000**
- Bestraft werden in erster Linie die **natürlichen Personen** («private Personen»), nicht das Unternehmen / die Organisation
  - Ausnahme: Busse von max. CHF 50’000 und Ermittlung der verantwortlichen natürlichen Person wäre unverhältnismässig
- Sanktioniert wird nur, wer die Taten **vorsätzlich** (bzw. grobfahrlässig) begeht

Wie mit dem neuen DSG umgehen?

vgl. Checkliste «Minimalprogramm»

- Gibt es ein «**Minimalprogramm**»?
  - Inventar – keine Doktorarbeit daraus machen (Excel-Liste reicht)
  - Datenschutzerklärung – weil sie Ihr Aushängeschild ist
  - Korrekte Verträge mit Dritten – weil Sie gebüsst werden könnten
  - Sich vorbereiten auf: Anfragen von Betroffenen, Data Breaches
- Aktivitäten **risikobasiert** auf DSG-Compliance prüfen
- Datenschutz-Compliance ist eine **Sisyphus-Arbeit** – niemand hält das DSG vollständig und jederzeit ein!
- Beginnen Sie **bereits jetzt** mit den Umsetzungsarbeiten
  - Umsetzung dauert – Zusatzbelastung zum normalen Tagesgeschäft
  - Manche Anforderungen werden bereits heute erwartet

Einige praktische Links

Allgemein

http://www.rosenthal.ch/

https://datenrecht.ch/

http://dsat.ch/

EDÖB

https://www.edoeb.admin.ch/

Aufsichtsstelle Datenschutz Baselland

https://www.baselland.ch/politik-und-behorden/besondere-behorden/datenschutz

Datenschutzbeauftragter Basel-Stadt

https://www.dsb.bs.ch/

VISCHER

Danke für Ihre Aufmerksamkeit! Fragen?

sbischof@vischer.com

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

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

www.vischer.com