VISCHER

DSG Revision: Welchen Datenschutz braucht die Schweiz in Zukunft?

Sessionsanlass ePower, Bellevue Bern

28. Februar 2017

Dr. Rolf Auf der Maur, Rechtsanwalt, VISCHER AG

Übersicht

- Ausgangslage und Treiber der DSG Revision
- Ziele der Revisionsvorlage (VE-DSG vom 21.12.2016)
- Grundsätzliche Unterschiede zwischen Schweiz und EU
- Gemeinsame Herausforderungen ./. USA
- Revisionspunkte mit Handlungsbedarf aus Sicht ICT
- Fazit und Anliegen

Regelungsinteresse beim DSG 1992: Schutz vor dem Fichenstaat

Treiber der DSG Revision 2017: Angst vor Kontrollverlust bei Big Data Analytics

Ziele und Leitlinien der Revisionsvorlage

Notwendig:

- Umsetzen der rev. SEV 108 des Europarates (mit Ratifikation)
- Aufrechterhaltung des Status der Gleichwertigkeit gegenüber der DSGVO der EU (ab Mai 2018)
- [Schengen relevante RL als Acquis Communautaire per 1.8.2018]

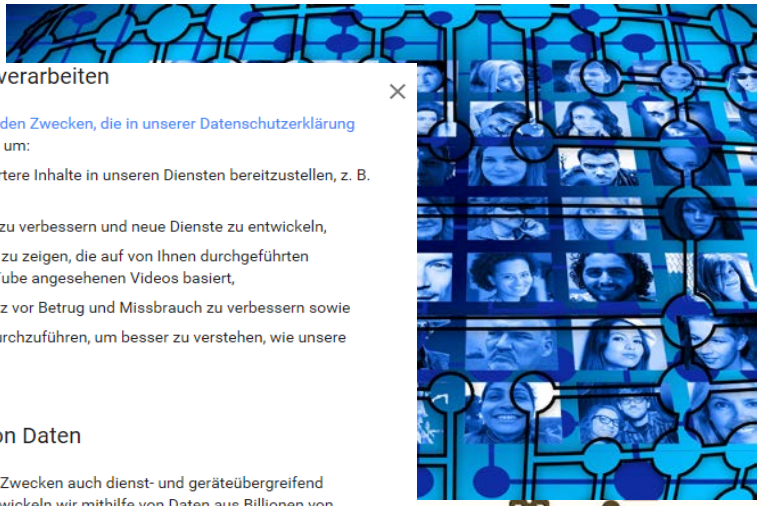
Erwünscht (gemäss Begleitbericht BJ):

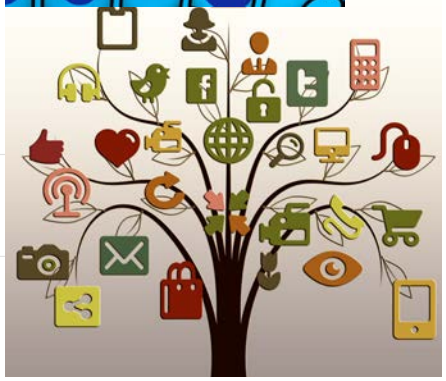
- Stärkung des Datenschutzes mit risikobasiertem Ansatz
- Technologieneutralität
- Modernisierung der Terminologie
- Verbesserung des grenzüberschreitenden Datenverkehrs
- Stärkung der Rechte der betroffenen Personen
- Verbesserung der Wettbewerbsfähigkeit der Schweiz
- Förderung der Selbstregulierung
- Stärkung der Kontrolle durch Verfügungskompetenz des EDÖB und Ausbau der strafrechtlichen Sanktionen

Grundsätzliche Unterschiede Schweiz vs. EU

Schweiz	EU
• Datenbearbeitung erlaubt unter Einhaltung bestimmter Voraussetzungen (Zweckbindung, Verhältnismässigkeit, Rechtmässigkeit) • EDÖB heute ohne Verfügungs-kompetenz, soll diese aber neu erhalten (Sanktionskompetenz soll bei kanto-nalen Strafverfolgungsbehörden bleiben) • Nationale Wirkung für Bund und Private • DSG 39 Artikel / VE-DSG 60 Artikel auf 24 Seiten	• Verbotsgesetz mit Erlaubnisvorbehalt (Einwilligung, gesetzliche Pflicht oder überwiegendes Interesse – als Resultat einer Interessenabwägung) • Sanktionen bis 4% des weltweiten Jahresumsatzes oder EUR 20 Mio. bei Verletzungen gegen DSGVO Pflichten. Ausgestaltet als Verwaltungssanktionen. • Extraterritoriale Wirkung • 99 Artikel plus 173 Erwägungen auf 88 Seiten

Gemeinsame Herausforderungen ./. USA: "The Privacy Paradox" und Cybersecurity





Warum wir die Daten verarbeiten

Wir verarbeiten diese Daten zu den Zwecken, die in unserer Datenschutzerklärung aufgeführt sind, beispielsweise um:

- nützlichere und personalisiertere Inhalte in unseren Diensten bereitzustellen, z. B. relevantere Suchergebnisse,
- die Qualität unserer Dienste zu verbessern und neue Dienste zu entwickeln,
- interessenbasierte Werbung zu zeigen, die auf von Ihnen durchgeführten Suchanfragen oder auf YouTube angesehenen Videos basiert,
- die Sicherheit und den Schutz vor Betrug und Missbrauch zu verbessern sowie
- Analysen und Messungen durchzuführen, um besser zu verstehen, wie unsere Dienste genutzt werden.

Zusammenführung von Daten

Wir führen die Daten zu diesen Zwecken auch dienst- und geräteübergreifend zusammen. Beispielsweise entwickeln wir mithilfe von Daten aus Billionen von Suchanfragen Modelle zur Rechtschreibkorrektur, die in allen unseren Diensten zum Einsatz kommen. Außerdem können wir Sie und andere Nutzer mithilfe kombinierter Daten vor potenziellen Sicherheitsrisiken warnen.

Wie verwendet Google Daten zur Verbesserung der Nutzerfreundlichkeit?

Tipp: Wenn Sie sich mit einem Google-Konto anmelden, bevor Sie zustimmen, wird Ihre Auswahl auf allen Geräten und in allen Browsern gespeichert, bei denen Sie angemeldet sind.

WEITERE OPTIONEN ICH STIMME ZU

Revisionspunkte mit Handlungsbedarf aus Sicht ICT

- Sanktionen: was muss guter Datenschutz kosten?
- Auftragsdatenbearbeitung: neue Hürden für ICT Dienstleister
- Verschärfung der Informationspflichten und Einwilligungspflichten: Mehr Aufwand oder mehr Privacy?
- Auslandtransfer: möglich, aber komplizierter und langwieriger
- Ausbau des Auskunftsrechts: Einladung zu Missbrauch
- Profiling: auch bei manueller Bearbeitung und nur mit ausdrücklicher Zustimmung?
- Permanente Überprüfungspflicht – kaum erfüllbar
- Geheimnisschutz: Sind Online / Social Network Daten mit Daten von Ärzten und Anwälten gleichzustellen?
- Privacy by Design / Privacy by Default: rechtlich redundante Duftnoten
- Selbstregulierung: ja – aber von “oben” verordnet?
- Data Breach Regulierung: Import aus den USA mit Swiss Finish
- Datenschutz für juristische Personen: Abschaffung richtig?

Sanktionen: was muss guter Datenschutz kosten?

Sanktionen: VE-DSG kriminalisiert die Verletzung administrativer Nebenpflichten

- DSGVO fordert "abschreckende Sanktionen" mit Busse von EUR 20 Mio oder 4% des weltweiten Jahresumsatzes
- SEV 108 fordert "geeignete Sanktionen"
- VE-DSG verzichtet auf Sanktionskompetenz der Behörde und setzt stattdessen auf einen Ausbau der Straftatbestände bei Verletzung administrativer Nebenpflichten mit Busse bis 500’000.—
- Diese Straftatbestände genügen dem Legalitätsprinzip nicht
- Die Verletzung der Persönlichkeit durch Bearbeitung von Personendaten (Kernbereich des Datenschutzes) bleibt dagegen straffrei

Wirkung der Sanktionen: Behinderung von Schweizer Unternehmen

- Verantwortliche (natürliche) Personen riskieren Strafeintrag und Busse
- Unternehmen werden "nur" gebüsst (bis CHF 100’000.--) sofern der Verantwortliche nicht feststellbar ist
- Resultat: Globale Online Plattformen haben in der Schweiz wenig zu befürchten
- Verantwortliche in Schweizer Unternehmen werden sich absichern wollen und Compliance Kosten in die Höhe treiben
- Kantonale Strafverfolgungsbehörden würden sich mit unterschiedlichem Eifer an die Arbeit machen. Eine einheitliche Rechtspraxis könnte lange auf sich warten lassen
- Die neu vorgeschlagene Verfügungskompetenz des EDÖB genügt. Bei einem Verstoss gegen rechtskräftige Verfügungen greifen strafrechtliche Sanktionen gemäss Art. 292 StGB

Auftragsdatenbearbeitung: neue Hürden für ICT Dienstleister

- Zulässig, aber mit neuen Pflichten für Auftraggeber und Auftragnehmer (plus Verordnungskompetenz des BR)
- unnötige und wenig praktikable Informationspflicht des Verantwortlichen gegenüber dem Betroffenen bei der Weitergabe an Auftragsbearbeiter (Art. 13 Abs. 4 VE-DSG) über EU-Anforderungen hinausgehend
- unnötiges Erfordernis schriftlicher Zustimmung für Unteraufträge (Art. 7 Abs. 3 VE-DSG)
- Mitteilung jeder Berichtigung oder Löschung von Personendaten an den Empfänger (=Auftragsbearbeiter) (Art. 19 lit. b VE-DSG)
- strafrechtlich sanktionierte Pflicht zur Information des Verantwortlichen bei Data Breach (Art. 17 Abs. 4, Art. 50 Abs. 3 lit. b VE-DSG)
- Pflicht zur Vornahme von Datenschutz-Folgeabschätzungen und zur Meldung an den EDÖB (dieser hat eine 3-monatige Einsprachefrist)
- Pflicht zur Information des EDÖB bei Auslandtransfer (Art. 6 Abs. 3 VE-DSG)

Informations- und Einwilligungspflichten: Mehr Aufwand oder mehr Privacy?

- Ausbau der Informations- und Einwilligungspflichten
- Einschränkung nur auf **einen** und **klar** erkennbaren Zweck (Art. 4 Abs. 3 und 4 VE-DSG) Verschärfung zu Art. 5 Abs. 1 lit. b DSGVO
- Bei Datenbeschaffung von Dritten muss der Betroffene bereits bei der Beschaffung (= 1. Speicherung?) informiert werden und nicht erst bei der ersten Kontaktaufnahme (Art. 13 Abs. 2 VE-DSG)
- Wirkung: Vorteil für globale Log-in Giganten und Nachteil für kleinere nationale online Plattformen

Auslandtransfer: möglich, aber komplizierter und langwieriger

- Nur zulässig wenn:
  - in ein vom Bundesrat anerkanntes Land mit gleichwertigem Schutz, oder
  - spezifische vom EDÖB genehmigte Garantien vorliegen
- Andernfalls (u.a.):
  - Einwilligung des Betroffenen in jedem einzelnen Fall
  - Zwecks Vertragserfüllung
  - Rechtfertigungsgrund der Feststellung, Durchsetzung oder Ausübung von Rechtsansprüchen im Ausland soll auf Verwaltungsverfahren ausgedehnt werden (bisher nur Gerichtsverfahren).
- Meldepflicht an den EDÖB auch im Falle der Bearbeitung zwecks Vertragserfüllung (sogar für Auftragsbearbeiter).

Ausbau des Auskunftsrechts: Einladung zu Missbrauch

- Jede natürliche oder juristische Person kann vom Verantwortlichen **kostenlos Auskunft** verlangen, ob Daten über sie bearbeitet werden.
- Zu liefern ist ein im Gesetz definierter **Mindestkatalog an Daten**
- Bei automatisierten Entscheiden: Information über Ergebnis, Zustandekommen und Auswirkungen
- Hat der Verantwortliche seinen Sitz im Ausland, ist der Auftragsbearbeiter in der Schweiz auskunftspflichtig

Profiling: auch bei manueller Bearbeitung und nur mit ausdrücklicher Zustimmung?

- Das dynamische "Profiling" ersetzt das statische "Persönlichkeitsprofil"
- Ausgangspunkt sind alle Daten (nicht nur Personendaten wie in der DSGVO)
- Ausdrückliche Zustimmung des Betroffenen nötig (Art. 4 Abs. 6 VE-DSG) – gemäss DSGVO nur, wenn Profiling Teil einer automatisierten Entscheidung mit rechtlicher Wirkung ist
- Profiling mit oder ohne Automatisierung (DSGVO nur bei automatisierter Bearbeitung)
- Credit Scoring nur ab 18 zulässig (DSGVO ab 16) (Art. 24 Abs. 2 lit. c Ziff. 3 VE-DSG)

Permanente Überprüfungspflicht: kaum erfüllbar

Art. 4 Abs. 5 VE-DSG:

Der Verantwortliche muss (laufend) überprüfen, *"ob die Daten richtig sind und wenn nötig nachgeführt wurden. Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden."*

Folge: enormer Aufwand beim Verantwortlichen, Informationsschwemme beim Betroffenen.

Verletzung der beruflichen Schweigepflicht (erweiterter Geheimnisschutz)

- **Tatbestand:** Bekanntgabe von "geheimen Personendaten" (Bisher nur besonders schützenswerte Personendaten und Persönlichkeitsprofile - Art. 35 DSG)
- **Geheimnisträger**: (i) Kenntnis im Rahmen der beruflichen Tätigkeit, welche die Kenntnis solcher Daten erfordert **oder** (ii) Bearbeitung zu kommerziellen Zwecken. Im Fokus gemäss Begleitbericht: **"Onlinehändler und Soziale Netzwerke**"
- **Sanktion:** Gefängnis bis 3 Jahre oder Busse bis über 1 Mio.

Privacy by Design / Privacy by Default: rechtlich redundante Duftnoten

- Verpflichtet sind Verantwortlicher und Auftragsbearbeiter
- Massnahmen zum Datenschutz sind ab dem "Zeitpunkt der Planung" zu treffen
- Standardmässig dürfen nur jene Personendaten bearbeitet werden, die für den Verwendungszweck erforderlich sind (Redundanz zu den schon heute geltenden Grundsätzen der Datenbearbeitung)

Selbstregulierung: ja – aber von "oben" verordnet?

- EDÖB soll "Empfehlungen der guten Praxis" (unter Beizug der interessierten Kreise) erlassen
- Interessierte Kreise können eigene Empfehlungen ausarbeiten und diese vom EDÖB genehmigen lassen
- Die Befolgung durch den Verantwortlichen soll Einhaltung der Anforderungen implizieren (der Auftragsbearbeiter ging vermutlich irrtümlich vergessen)
- Rechtsmittel gegen den Erlass von (oder die Verweigerung der Zustimmung zu) Regeln der guten Praxis sind nicht vorgesehen

Data Breach Regulierung: Import aus den USA mit Swiss Finish

- Regelungszweck in den USA: Erfahrungen sammeln über Gründe für Data Leaks zwecks Entwicklung von besseren Sicherheitsmassnahmen
- Umsetzung VE-DSG: Pflicht des Verantwortlichen zur Meldung faktisch **jedes Datenschutzverstosses** (einschliesslich Datenverlust) an den EDÖB. Frist: **unverzüglich**
- DSGVO sieht Meldepflicht "nur" vor, sofern die Verletzung des Datenschutzes ein Risiko für den Betroffenen beinhaltet und dieses nicht durch andere Massnahmen beseitigt wurde. Die Frist beträgt 72 Stunden

Abschaffung Datenschutz für juristische Personen: konsequent und richtig?

- Kern des Persönlichkeitsschutzes ist Art. 28 ZGB
- Persönlichkeit haben sowohl natürliche wie juristische Personen
- Datenschutz für Mitarbeitende und natürliche Hilfspersonen bleibt
- Verletzung der Persönlichkeit juristischer Personen wird auch künftig möglich bleiben (Verletzung von Art. 28 ZGB), aber die Rechtssicherheit leidet

DSGVO Übertreibungen ohne Aufnahme in den VE-DSG

- "Recht auf Vergessen" (Implizit schon im DSG enthalten)
- Anspruch auf Portabilität der Daten (Konsumentenschutz)
- Hohe Verwaltungsbussen (dafür aber Ausbau der Straftatbestände)
- Informationskatalog (teilweise)

Fazit und Anliegen

- Erklärte Ziele der Revision sind sinnvoll (wären aber auch mit einer **Teilrevision des DSG** zu erreichen)
- **Positiv:** Verzicht auf einzelne Übertreibungen der DSGVO und Beibehaltung des Erlaubnisprinzips
- **Negativ**: Übertreibungen ("Swiss Finish") gegenüber DSGVO (ev. diente als Vorlage die Parlamentsfassung). **Sämtliche Verschärfungen gegenüber DSGVO sind zu streichen**.
- Missglückt: Sanktionsregelung. Verfügungskompetenz des EDÖB und **Sanktionen bei Verstössen gegen rechtskräftige Verfügungen genügt (Art. 292 StGB)**.
- Insgesamt: VE-DSG bringt mehr Aufwand für Compliance und eine Informationsflut – nicht unbedingt mehr Privacy

Ihr Kontakt bei VISCHER

Dr. Rolf Auf der Maur

Rechtsanwalt, Partner

ram@vischer.com

+41 58 211 34 00

VISCHER: Your Team for Swiss Law

VISCHER

Herzlichen Dank.

Zürich
Schützengasse 1
CH-8021 Zürich
Tel +41 58 211 34 00
Fax +41 58 211 34 10

Basel
Aeschenvorstadt 4
CH-4010 Basel
Tel +41 58 211 33 00
Fax +41 58 211 33 10