VISCHER

Datenschutzreform in der EU und der Schweiz: Neuer Fokus Datensicherheit (Schutzmassnahmen und «Data Breach Response»)

simsa Provider Day 2016

Zürich, 8. Juni 2016

Dr. Thomas Steiner, LL.M. (Berkeley)

Rechtsanwalt, VISCHER AG

Übersicht

1. EU Datenschutzgrundverordnung (wichtige Neuerungen)
2. Revision des Schweizer Datenschutzgesetzes (vorgeschlagene Neuerungen soweit bekannt)
3. Neuer Fokus Datensicherheit: Schutzmassnahmen, Compliance-Nachweise und «Data Breach Notice»
4. «Data Breach Response»: Vorbild Kalifornien und Best Practice für die Schweiz

EU Datenschutzgrundverordnung (DS-GVO) – anwendbar auf Schweizer Provider

- 99 Artikel, 88 Seiten
- Gilt ab 25. Mai 2018 in allen EU-Mitgliedstaaten
- Persönlichkeitsschutz im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Anwendbar auf Schweizer Provider: Datenverarbeitung «im Zusammenhang mit» Angebot von Dienstleistungen für (oder Überwachung von) Kunden in der EU

EU DS-GVO – wichtige Neuerungen

- Erweiterte Informationspflichten, freiwillige und eindeutige Einwilligung, Recht auf Vergessenwerden, Datenportabilität
- *Privacy by Design* und *Privacy by Default*
- Risiko-/Folgenabschätzung und neuer Fokus auf Sicherheit der (automatisierten) Datenverarbeitung: Risikobasierter Ansatz
- ***Data Breach Notice***
- Nachweis über Compliance («Accountability»)
- Hohe Geldbussen: Bis zu EUR 10 Mio. bzw. 20 Mio. oder (wenn höher) 2% bzw. 4% des im vorangegangenen Geschäftsjahrs weltweit erzielten Umsatzes

Revision des Schweizer DSG – Aktueller Stand der Revision und Hintergrund

- Endkonsultation EJPD intern: Ende Juni 2016
- Vernehmlassung: 3 Monate ab Ende August 2016
- Sicherung des Adäquanz-Status: Anpassung an EU DS-GVO
- Anpassungen an EU Richtlinie zum Datenschutz in der Strafverfolgung (Schengen-Besitzstand)
- Umsetzung des revidierten Übereinkommens 108 des Europarats (insb. Transparenz, Stärkung des Auskunftsrechts, Nachweis der Compliance, Risikoabschätzung, Datensicherheit; Befugnisse der Aufsichtsbehörde – ggf. Sanktionen)

Revision des Schweizer DSG – wichtige Neuerungen (Vorschläge Stand 3. Juni 2016)

- Aufhebung des Schutzes für juristische Personen
- Erweiterte Informationspflichten (Transparenz)
- «Herrschaft» über Daten stärken (Recht auf Vergessenwerden, erweitertes Auskunftsrecht, Datenportabilität)
- Risiko-/Folgenabschätzung, *Privacy by Design* und *Privacy by Default*; neuer Fokus Datensicherheit: Risikobasierter Ansatz
- ***Data Breach Notice***
- Nachweis der Compliance («Accountability»)
- Verschärfung der (bestehenden/allenfalls neue?) Strafnormen/ Bussen, Strafbarkeit des Unternehmens

Fokus Datensicherheit: Schutzmassnahmen (gemäss EU DSG-GVO)

- «technische und organisatorische Schutzmassnahmen»: Risikobasierter Ansatz (abhängig von Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der Eintrittswahr-scheinlichkeit und der Schwere des Risikos für Betroffene)
- Sicherheitsmassnahmen: (a) Pseudonymisierung und Verschlüsselung, (b) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherstellen, (c) Verfügbarkeit und Zugang bei physischem oder technischem Zwischenfall rasch wiederherstellen können, (d) Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Massnahmen
- Nachweis der Compliance («Accountability»)

Fokus Datensicherheit: «Data Breach» Melde- / Benachrichtigungspflicht (gemäss EU DS-GVO)

- «Data Breach» : Unbefugter Zugang («access») zu personenbezogenen Daten genügt als Auslöser
- Meldung an Datenschutz-Aufsichtsbehörde unverzüglich, «möglichst binnen 72 Stunden»
- Benachrichtigung der betroffenen Personen wenn: «voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen» besteht
- Hohes Risiko wahrscheinlicher bei Aneignung bzw. Verlust oder Offenlegung (ggf. bei Vernichtung, Veränderung)
- Hosting Provider als Auftragsdatenbearbeiter: Pflicht zur Meldung an Kunden («unverzüglich»)

«Data Breach»: Ausnahmen von der Benachrichtigungspflicht (gemäss EU DS-GVO)

Meldung an Aufsichtsbehörde, aber keine Benachrichtigung der betroffenen Personen wenn:

- «technische und organisatorische Sicherheits-vorkehrungen» auf die vom *Data Breach* betroffenen Personendaten angewandt; oder
- nach Entdeckung des *Data Breach* durch Massnahmen sicher gestellt, dass für die betroffenen Personen «aller Wahrscheinlichkeit nach» kein hohes Risiko mehr besteht

«Data Breach» Melde-/Benachrichtigungspflicht gemäss DSG (Vorschlag Stand 3. Juni 2016)

- «Data Breach» Definition weit gefasst – unberechtigter Zugang genügt (vgl. EU DS-GVO und Übereinkunft 108)
- (zumindest) Meldung an EDÖB («unverzüglich»)
- Benachrichtigung der betroffenen Personen bei hohem Risiko für Persönlichkeit und Grundrechte
- Keine generellen Ausnahmen analog EU DS-GVO vorgesehen
- Entscheid über Benachrichtigung der betroffenen Personen in Absprache und in Kooperation mit EDÖB

Datensicherheit und «Data Breach»: Risikobasierter Ansatz als Chance

- Bedürfnis und Pflicht der Kunden: Verschlüsselung, Systemintegrität, Back-up Systeme, Incident Response-Prozesse, Beratung, Kooperation mit Provider und EDÖB
- Chance für Hosting Provider / IT-Infrastrukturanbieter: Verschlüsselung, Zugangskontrollen (Data Center und Systeme), Beratung, Mitarbeiter-Schulung, Systeme und Prozess für Verarbeitungs-Logs

California Data Security Breach Notification – aus Erfahrung lernen (1|2)

- *California Data Security Breach Notification Statute* (2002): Modell für andere U.S. Gliedstaaten (und für die Schweiz?)
- Benachrichtigung der betroffenen Personen *ausnahmslos*, aber nur bei begründetem *Verdacht auf unberechtigte Aneignung* («acquisition») von «unencrypted personal information»
- (seit 2012) Meldung an CA-Staatsanwaltschaft wenn mehr als 500 Kalifornier betroffen sind
- 2012–2015 wurden 657 *Data Breaches* gemeldet

California Data Security Breach Notification – aus Erfahrung lernen (2|2)

California Data Breach Report 2016 (2012–2015)

- *Malware* und *Hacking* (unerlaubtes Eindringen in IT-System)
  - 54% der Fälle, 90% der betroffenen Datensätze
  - Beispiele (2015): Anthem, UCLA Health, T-Mobile USA
- Verlust oder Diebstahl (physisch)
  - 22% der Fälle, 6% der betroffenen Datensätze
- Fehler von Mitarbeitern (Falscher E-Mail-Empfänger oder unbeabsichtigte Veröffentlichung auf Website)
  - 17% der Fälle, 4% der betroffenen Datensätze
- Missbrauch bzw. unautorisierte Nutzung von Zugangsrechten (intern)
  - 7% der Fälle, <1% der betroffenen Datensätze

«Data Breach Response» - Best Practice (1|3)

- Art des *Data Breach* und der betroffenen Datenkategorien ermitteln
- Sofortmassnahmen: Weitere unerlaubte Zugriffe auf bzw. Offenlegung von Daten verhindern
- (ungefähre) Zahl betroffener Personen und personen-bezogener Datensätze ermitteln
- Risikoabschätzung / Beschreibung der wahrscheinlichen Folgen des *Data Breach*

«Data Breach Response» - Best Practice (2|3)

- Meldung an EDÖB (bei Auftragsverarbeitung an Kunden)
- Entscheid über Benachrichtigung der betroffenen Personen in Kooperation mit EDÖB
- Beweismaterial sichern (Dokumentation/Nachweis der getroffenen Schutzmassnahmen; eventuell Strafanzeige)
- Interne Untersuchung des *Data Breach*
- Anpassung und regelmässige Kontrolle der organisatorischen und technischen Schutzmassnahmen

«Data Breach Response» - Best Practice (3|3)

Musterformular *(California Data Breach Notification)*

- *Company Name – Notice of Data Breach*
- *What happened?*
- *What information was involved?*
- *What we are doing*
- *What you can do*
- *For more information*

(vgl. auch Mindestinformationen gemäss EU DS-GVO)

Ihr Kontakt bei VISCHER

Dr. Thomas Steiner, LL.M.

Rechtsanwalt, Senior Associate

tsteiner@vischer.com

+41 58 211 34 00

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