wenger & vieli
Rechtsanwälte

Datenschutzrecht - Schauen Sie genau hin!

Michael Tschudin / Claudia Keller

Programm

1. Einführung
2. EU-DSGVO – Inkrafttreten & Anwendungsbereich
3. 5 ausgewählte Themen
   a. Risikobasierter Ansatz
   b. Privacy by Design & Default
   c. Transparenz / Einwilligung
   d. Transfer in Drittländer
   e. Automatisierte Einzelentscheidung
4. Sanktionen
5. Q&A

Einführung (1)

Three-quarters of law firms "unprepared" for EU data regulation with six months to go

Alle drei Milliarden Yahoo-Konten wurden gehackt

Das grösste Datenleck der Geschichte ist noch weitreichender als bisher gedacht: Es wurden Daten von allen Yahoo-Accounts gestohlen.

Privatsphäre bei Postfinance nur begrenzt geschützt

GDPR **fines** may affect almost 80% of US firms, poll shows
ComputerWeekly.com - 08.11.2017

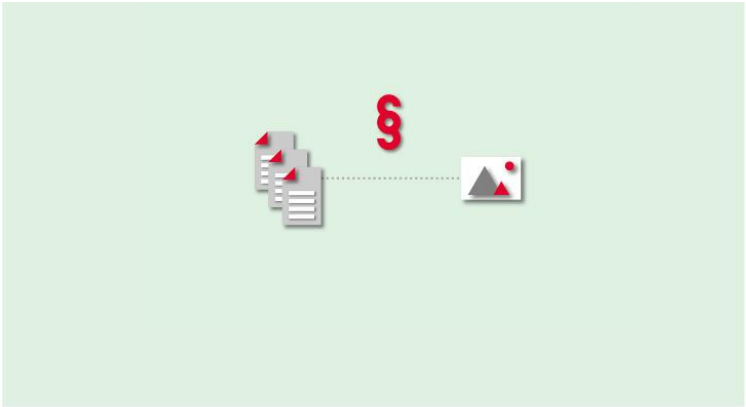
Einführung (2)

- Revision in der Schweiz
  - Vorentwurf für Vernehmlassung vom 21. Dezember 2016
  - Grosses und kritisches Echo: 222 (!) Stellungnahmen
  - Entwurf mit Botschaft vom 15. September 2017

- Leitlinien der Revision / und zugleich Kritik:
  - Verschärfung und Modernisierung
  - Kompatibilität mit europäischem Schutzniveau (Gewährleistung des Datenaustausches mit der EU)
  - Informationelle Selbstbestimmung

Einführung (3)

digitalswitzerland | challenge



Pictograms and Bot for Terms and Conditions

Legal

EU-Datenschutzgrundverordnung (1)

- DSGVO löst die vorhergehende EU-«Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr» ab.
- Anders als die vorhergehende Richtlinie gilt sie als Verordnung unmittelbar und muss nicht erst in den Mitgliedsstaaten durch nationales Recht umgesetzt werden.
- DSGVO tritt am 25. Mai 2018 in Kraft.

EU-Datenschutzgrundverordnung (2)

Auswirkungen auf Schweizer Unternehmen?

DSGVO von CH-Unternehmen einzuhalten, wenn Daten von in der EU ansässigen Personen bearbeitet werden und:

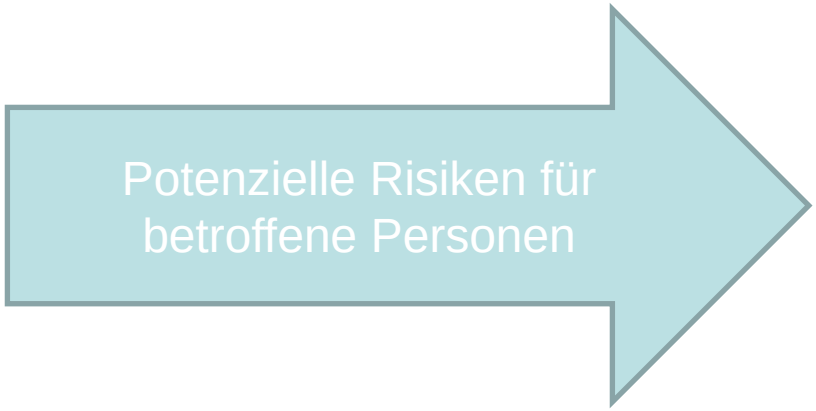
- Datenbearbeitung im Zusammenhang mit Angebot von Waren oder Dienstleistungen an Personen in der EU steht; oder
- bezweckt in der EU stattfindendes Verhalten von Personen zu beobachten.

EU-Datenschutzgrundverordnung (3)

Strafhöhe bei Verstössen kann beachtlich sein:
pro Verstoss bis zu 20 Millionen Euro oder vier Prozent des weltweiten (!) Umsatzes – je nachdem welche Grenze höher ist.

Thema I: Risikobasierter Ansatz (1)

Ausgangspunkt



Thema I: Risikobasierter Ansatz (2)

Hohes Risiko = strengere Pflichten

- Pflicht zur Erstellung einer Datenschutz-Folgeabschätzung (PIA)
- Meldepflicht für Verletzungen der Datensicherheit
- Strengere Anforderungen an Einwilligung

Thema I: Risikobasierter Ansatz (3)

Privacy Impact Assessment PIA

- Notwendig, wenn Bearbeitung hohes Risiko für Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringen kann.
- Hohes Risiko ergibt sich aus Art/Umfang/Umständen und Zweck der Bearbeitung.

Thema II: Privacy by Design & Default (1)

Datenschutz durch Technik

Privacy by Design

Technische und organisatorische Ausgestaltung der Datenbearbeitung mit Blick auf Einhaltung der Datenschutzgrundsätze.

Thema II: Privacy by Design & Default (2)

Datenschutz durch Technik

Privacy by Design

Massgeblich sind:

- Stand der Technik;
- Art und Umfang der Datenbearbeitung;
- Risiken, welche Datenbearbeitung für Persönlichkeit und Grundrechte der Personen mit sich bringt.

Thema II: Privacy by Design & Default (3)

Datenschutzfreundliche Voreinstellungen

Privacy by Default

- Beschränkung der Bearbeitung der Personendaten auf das Mindestmass.
- Betroffene Person kann Erweiterung zustimmen.

Thema III: Transparenz / Einwilligung (1)

Umfassende, aktive Informationspflichten

- Beschaffung von Personendaten (auch wenn Daten nicht bei der betroffenen Person beschafft werden);
- Verantwortlichen der Datenbearbeitung;
- Bearbeitungszweck;
- Empfänger von Personendaten;
- Bekanntgabe ins Ausland (wohin? Garantien?).

Thema III: Transparenz / Einwilligung (2)

Anforderungen an Einwilligung

Die Einwilligung ist ein möglicher Rechtfertigungsgrund für die Datenbearbeitung.

Ist eine Einwilligung erforderlich, so gelten folgende Gültigkeitsvoraussetzungen:

- angemessene Information;
- freiwillig erteilt;
- eindeutig erteilt;
- bei besonders schützenswerten Daten/Profiling ausdrücklich erteilt.

Thema IV: Transfer in Drittländer (1)

- Datentransfer ins Ausland zulässig, wenn Empfängerland einen angemessenen Schutz gewährleistet; Bundesrat führt eine entsprechende Liste
- Wenn Empfängerland nicht auf der Liste, trotzdem zulässig wenn (Auswahl):
  - Völkerrechtlicher Vertrag
  - Vertragliche Absicherung (Klauseln müssen vom Beauftragten anerkannt sein)
  - Konzerninterne Datenschutzvorschriften (von zuständiger Behörde vorgängig genehmigt)
  - Weitere (z.B. Swiss-US Privacy Shield)

Thema IV: Transfer in Drittländer (2)

- Rechtfertigungsgründe (Auswahl):
  - Ausdrückliche Einwilligung
  - Unmittelbarer Zusammenhang mit der Abwicklung eines Vertrages mit der betroffenen Person bzw. in deren Interesse
  - Betroffene Person hat Daten allgemein zugänglich gemacht

- Trend:
  - Transfer zwischen Ländern mit gleichwertigem Datenschutz soll vereinfacht werden
  - Transfer in andere Länder nur bei vertraglicher Absicherung oder Einwilligung möglich

Thema V: Autom. Einzelentscheidung

- *Definition: «Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt»*
- Beispiele: Kreditwürdigkeit, Abschluss eines Versicherungsvertrag, automatisierte Steuerveranlagung?
- Allenfalls in Zusammenhang mit Profiling
- Rechtsfolge: Informationspflicht und «rechtliches» sowie «menschliches» Gehör

Sanktionen (1)

- Verfügungskompetenz (aktuell: Sachverhaltsabklärung, Empfehlung und Klage vor Bundesverwaltungsgericht)
- Aber: Keine Strafkompetenz, diese liegt bei den Kantonen
- Opportunitätsprinzip: *Keine Intervention wenn Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist*
- Keine Parteirechte der betroffenen Partei
- Mitwirkungspflicht: Bei Verweigerung: Hausdurchsuchung möglich
- Anzeigemöglichkeit des Beauftragten

Sanktionen (2)

- Bussen von bis zu CHF ¼ Mio. für:
  - Verletzung der Informationspflicht bei der Beschaffung von Personendaten
  - Verletzung der Informationspflicht bei einer automatisierten Einzelfallentscheidung
  - Verletzung der Informationspflicht bei Auskunftsrechten von betroffenen Personen
  - Unzulässige Bekanntgabe von Daten ins Ausland
  - Unzulässiges Outsourcing
  - Nichteinhalten der Mindestanforderung an die Datensicherheit
  - Missachtung von Verfügungen des Beauftragten

Sanktionen (3)

- Bestraft wird grundsätzlich nicht das Unternehmen, sondern die Leitungsperson
- Wenn die Ermittlung der verantwortlichen Leitungsperson unverhältnismässig wäre, können Bussen bis zu CHF 50’000.- dem Unternehmen auferlegt werden
- Keine fahrlässige Begehung möglich
- Datenschutzgrundverordnung: Bis zu 4% des weltweiten Umsatzes oder EUR 20 Mio.!

Was tun?

- Awareness für Datenschutz: Chefsache
- Abklären, ob DSGVO für Unternehmen anwendbar
- Datensicherheit gewährleisten
- Datenschutzcompliance anstossen:
  - Interne Datenschutzstelle
  - Bestandesaufnahme betr. aktuelle Datenbearbeitung erforderlich
  - Datenschutzerklärungen und Überprüfung von Verträgen
  - Dokumentation von Compliance-Bemühungen

wenger & vieli
Rechtsanwälte

Wenger & Vieli AG
Dufourstrasse 56, Postfach, CH-8034 Zürich
T +41 (0)58 958 58 58, www.wengervieli.ch