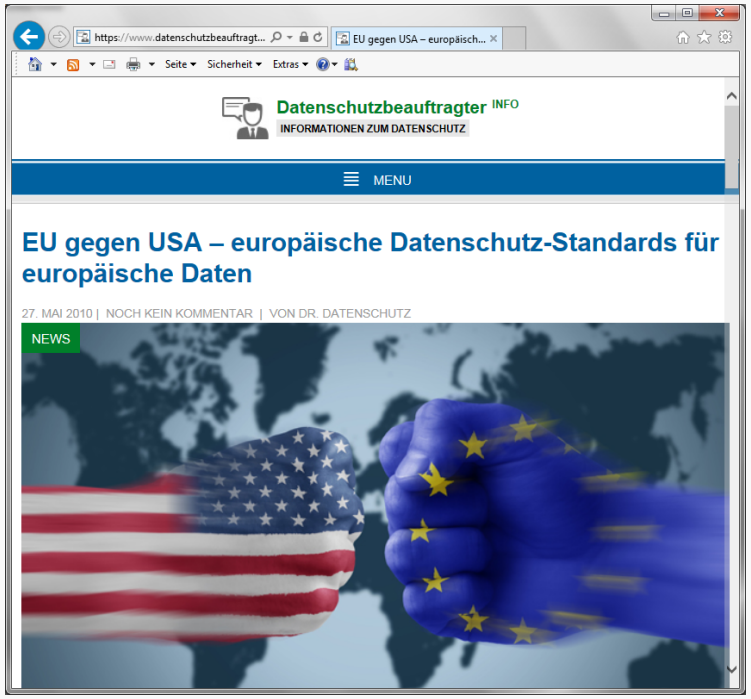
Modul 1, 13. September 2016

Webinar@Weblaw: DSGVO – Geltungsbereich, Bearbeitungsgrundsätze, Informationspflichten.

David Rosenthal

Geltungsbereich: Für wen in der Schweiz gilt die DSGVO und inwieweit?



facebook

EU-Recht

«Gegen» die USA

«Gegen» Online-Anbieter

Was geht das ein Unternehmen in der Schweiz an?

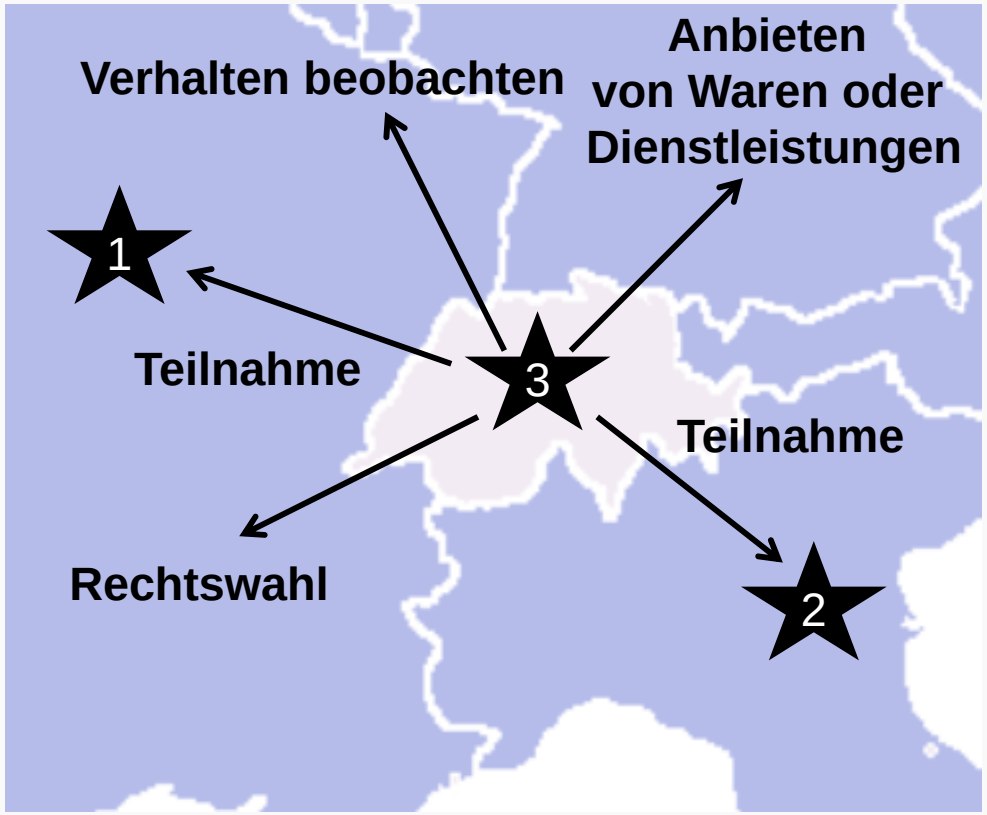
4%

(des weltweiten Jahresumsatzes oder 20 Mio. EUR)

Wesentliche Punkte

- **Grundkonzept** (was ist erlaubt, was nicht) ist ähnlich wie in der Schweiz
  - EU verlangt für jede Datenbearbeitung eine Rechtfertigung (z.B. Einwilligung, Erfüllung einer Rechtspflicht, berechtigte Interessen) (im DSG ist das anders)
- **Räumlicher Geltungsbereich:** DSGVO gilt auch für viele Schweizer Firmen
- **Personendaten:** Werden unter der DSGVO breiter verstanden als im DSG
- **Einwilligung:** Anforderungen an ihre Gültigkeit sind strenger als im DSG
- **Informationspflichten:** Es muss wesentlich umfassender informiert werden
- **Betroffenenrechte:** Betroffene erhalten weitere Eingriffs- und Auskunftsrechte
- **Governance:** Aufwand insbesondere bzgl. der Dokumentation steigt stark
- **Buzzwords:** Privacy by Design & Co. – meist alter Wein in neuen Schläuchen
- **Auslandsdatentransfer:** Hier wird es nicht wirklich strenger als im DSG
- **Sanktionen:** Scharfe Sanktionen … aber ob sie durchgesetzt werden können?
- **Frist zur Umsetzung:** 25. Mai 2018

Wer fällt unter die DSGVO?



1 **Controller***

2 **Processor****

3 **Controller oder Processor**

* "Verantwortlicher"

** "Auftragsverarbeiter"

Article 3

Territorial scope

(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

(3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Consid. 22, 23, 24, 25

Artikel 3

Räumlicher Anwendungsbereich

(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

(a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

(b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Erw. 22, 23, 24, 25

Wer fällt unter die DSGVO?

- **Erfasst ist eine Schweizer Firma …**
  - die Kunden aus der EU hat und diesen dort Dienstleistungen oder Produkte anbietet – soweit sie im Zusammenhang damit auch ihre Daten bearbeitet
  - die auswertet, was die einzelnen Benutzer aus der EU auf ihrer Website oder App damit tun, soweit es um die diesbezüglichen Daten geht
  - soweit sie Daten an einen Provider in der EU (z.B. Cloud) ausgelagert hat
  - soweit sie Daten einer EU-Niederlassung bei sich im Auftrag bearbeitet
  - wenn eine Person aus der EU in der Schweiz klagt und sich darauf beruft
- **Nicht erfasst ist eine Schweizer Firma …**
  - soweit sie Daten von Personen aus der Schweiz in der Schweiz bearbeitet
  - soweit sie Daten von Kunden aus der EU bearbeitet, denen sie ihre Produkte und Dienstleistungen aber nur in der Schweiz anbietet
  - soweit sie HR-Daten von in der Schweiz tätigen Arbeitnehmern bearbeitet (mit Ausnahmen: Verhaltensüberwachung von EU-Arbeitnehmer in der EU)

Anwendungsbeispiele

Quelle: Airportsineurope.com

Firma in CH, Bearbeitung in F und CH, Dienstleistung in F an Personen mit Wohnsitz auch in EU

Quelle: Universitätsspital Zürich

Betrieb und Bearbeitung in CH, Anbieten von Dienstleistung (meist) in CH an Personen mit Wohnsitz auch in EU

Bild: Thies Wachter, Zürich

Firma und Bearbeitung in CH, Anbieten von Dienstleistung an Personen mit Wohnsitz auch in EU

Was sind die Folgen?

- **Risiko 1: Klage einer betroffenen Person wegen DSGVO-Verletzung**
  - Risiko von Schadenersatz, Genugtuung, Bearbeitungsverbot betr. Daten der klagenden Person, Lösch-, Widerspruchs-, und Auskunftsansprüche, etc.
  - Solche Klagen waren in der Schweiz schon bisher möglich (gab es fast nie)

- **Risiko 2: Unterstellung unter die EU-Datenschutzaufsichtsbehörden**
  - Risiko von Meldepflichten, Untersuchungen und Sanktionen|Massnahmen
  - DSGVO sieht eine nationale Aufsicht vor, d.h. jedes Land muss selbst für die Durchsetzung der DSGVO auf ihrem Hoheitsgebiet sorgen
  - Sie ist aber auch für Schweizer Firmen zuständig, soweit deren Bearbeitung "Auswirkungen auf betroffene Personen in ihrem Hoheitsgebiet" hat oder auf "Personen mit Wohnsitz in ihrem Hoheitsgebiet ausgerichtet" ist (Erw. 122)
  - Ausländische Behörden dürfen ohne Bewilligung nicht einfach auf Schweizer Boden tätig werden (Art. 271 StGB) …

Was sind die Folgen?

- Schweizer Unternehmen unterstehen **mehreren Aufsichtsbehörden parallel**
  - Dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gem. DSG
  - Den nationalen Aufsichtsbehörden jener EU-Staaten, von deren Einwohner Daten bearbeitet werden
- Konzept des **One-Stop-Shop** gilt nur für Unternehmen mit Sitz in der EU, nicht für Schweizer Unternehmen, d.h. jede EU-Aufsichtsbehörde agiert konkurrierend
  - Folge: Parallele Meldepflichten, parallele Verfahren, etc. möglich
- Werden sich die **Schweiz und EU absprechen** und eine Lösung gegen diese Mehrfachbelastung finden? → Art. 50 DSGVO böte eine Handhabe …
  - EU-Behörden werden vom EDÖB Amtshilfe erhalten können, aber wie weit?
  - Art. 271 StGB: Schweizer Unternehmen dürfen nicht einfach kooperieren
- Pflicht Schweizer Unternehmen zur Benennung eines **Vertreters in der EU**, der sie "in Bezug auf ihre Pflichten" unter der DSGVO "vertritt"

Den Esel meinen, den Sack schlagen?

- Welche **persönliche Verantwortlichkeit** kommt dem "Vertreter" zu?

(17) „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

- **Variante 1:** Rechtsvertreter und Zustelldomizil (Beispiel: Anwalt)
- **Variante 2:** Stellvertretender Verantwortlicher (Beispiel: Prüfperson gem. KlinV)
- Frage bisher ungeklärt; Argument der Durchsetzbarkeit spricht für Variante 2
- Im Falle von Variante 2 bietet sich Gründung eines **Special Purpose Vehicle** in der EU an, das im Bedarfsfall geopfert werden kann (oder Art. 27 wird ignoriert)

Wer braucht *keinen* "Vertreter" in der EU?

(2) Die Pflicht gemäß Absatz 1 des vorliegenden Artikels gilt nicht für

(a) eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder

(b) Behörden oder öffentliche Stellen.

= besonders schützenswerte Personendaten

Kriterien müssen kumulativ erfüllt sein, jedoch nur in Bezug auf die Bearbeitung von Daten von Personen, die sich in der EU befinden

Was von der DSGVO gilt?

- **Sicher:** Regeln zur Bearbeitung von Personendaten (Zweckbindung, Pflicht zur Transparenz, Verhältnismässigkeit, Anforderungen an Einwilligung, etc.)
- **Vermutlich:** Betroffenenrechte (Informationspflichten, Auskunftsrecht, Recht auf Vergessen und Widerspruch, Datenportabilität, etc.), Exportbestimmungen
- **Umstritten:** Organisationsvorschriften (Regeln zum Datenschutzbeauftragten, Meldepflicht bei "Data Breaches", Pflicht zu Dateninventar und PIAs, etc.)

- Revidiertes Schweizer DSG wird zwar vergleichbare Bestimmungen haben, die aber eben nicht deckungsgleich bzw. weniger detailliert sein werden

- DSGVO verweist für viele **Ausnahmen und Rechtfertigungen** auf sonstiges EU-Recht (z.B. Art. 6(1)(c), 22(2) und 23), doch es ist unklar, ob und inwieweit sich Schweizer Firmen darauf berufen können (Risiko der Diskriminierung)
  - Antwort wird je nach EU-Mitgliedsstaat (bzw. Kollisionsrecht) unterschiedlich sein

Was tun?

- **Zuerst die Lageanalyse**
  - Erheben, welche Daten bearbeitet werden
  - Beurteilen, ob und inwieweit die DSGVO darauf Anwendung findet
  - Beurteilen, ob ein Vertreter in der EU bezeichnet werden muss
  - Konzernverhältnisse einbeziehen (z.B. Outsourcing, Joint-Controllership)
  - Datenschutzrisiken bewerten (bei B2B-Firmen anders als bei B2C-Firmen)
- **Falls die DSGVO anwendbar ist, Entscheid fällen**
  - DSGVO als genereller Standard anwenden oder nur dort, wo sie wirklich gilt?
  - DSGVO voll umsetzen, die Organisationsvorschriften ignorieren oder alles ignorieren? Vertreter in der EU benennen oder ignorieren?
  - Meldungen nur an eine nationale EU-Datenschutzbehörde oder an alle 28 Behörden? EWR?
- **Weitere Klärung der offenen Fragen wird noch einige Jahre beanspruchen**
  - Immerhin: DSG wird vergleichbare Anforderungen aufstellen

Besten Dank für Ihre Aufmerksamkeit!

Homburger AG
lic. iur. David Rosenthal
Prime Tower
Hardstrasse 201
8005 Zürich
Tel. +41 43 222 1000
Fax +41 43 222 1500
david.rosenthal@homburger.ch
www.homburger.ch