EU-DSGVO & Datenschutz-Compliance für Schweizer Unternehmen

Workshop VSV, 21. Februar 2018

Lukas Bühlmann, LL.M. & Dr. Michael Reinle, LL.M.

EU DSGVO – Inkrafttreten am 25. Mai 2018

Agenda

- Anwendung auf CH-Unternehmen
- Überblick wichtige Themen
- Informationspflichten
- Einwilligung
- Berechtigtes Interesse
- Auftragsdatenbearbeitung
- Datentransfer in die USA
- Sanktionen
- Take Home

Anwendung auf CH-Unternehmen

Räumlicher Geltungsbereich

Art. 3 DSGVO: Anwendung auch auf Nicht-EU-Unternehmen

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

   - betroffenen Personen in der Union **Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
   - das **Verhalten betroffener Personen zu beobachten**, soweit ihr Verhalten in der Union erfolgt.

...

Konstellationen

- Bearbeitung von Daten durch **EU-Niederlassung** eines CH-Unternehmen oder Teilnahme an Datenbearbeitungen von EU-Unternehmen **(z.B. in Konzernverhältnissen)**
- Verkauf von **Waren oder Dienstleistungen** eines CH-Unternehmens an EU-Kunden oder **Überwachung des Verhaltens von Personen**, sofern sich das Verhalten in der EU abspielt – z.B. **Trackingtools** in Webshop, der auch auf EU-Kunden ausgerichtet ist
- CH-Unternehmen beauftragt EU-Unternehmen zur **Auftragsdatenverarbeitung** (z.B. Cloud-Anbieter) – auch bei Sub-Processing des EU-Verarbeiters an Unternehmen ausserhalb der EU oder Bearbeitung von Personendaten durch CH-Unternehmen **im Auftrag** eines EU-Unternehmens (z.B. einer EU-Niederlassung)

Gilt auch bei Weitergabe / Adresshandel

Überblick

Wichtige Themen #1

Räumlicher Anwendungsbereich, Art. 3 EU-DSGVO

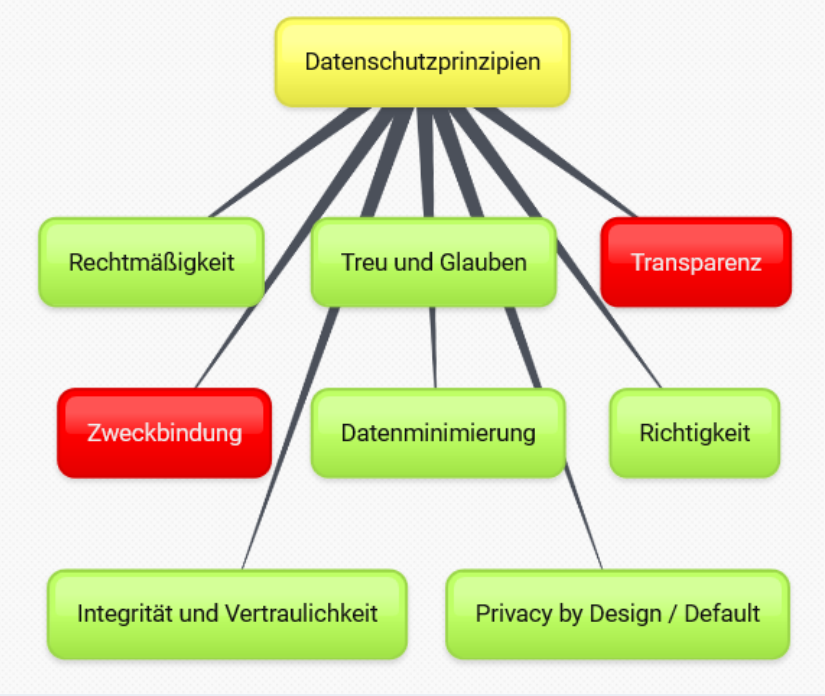
- Datenverarbeitung innerhalb der EU
- Marktortprinzip für Datenverarbeiter mit Sitz in Drittstaaten (z.B. CH)

Grundsatz: Verbot mit Erlaubnisvorbehalt

- Durch die Verordnung selbst
- Durch Einwilligung (hohe Anforderungen an Gültigkeit)
- „überwiegendes Interesse“ (spielt künftig größere Rolle)
- Durch Gesetz

Stärkung der Datenschutzprinzipien, z.B. Transparenz

- Aktive Informationspflicht mit klaren Inhaltsvorgaben
- Aktive Informationspflicht auch bei Datenbeschaffung aus Drittquellen
  → Problem bei Datenanreicherung



Wichtige Themen #2

Verschärfte Sorgfaltspflichten

- Datenschutz-Folgenabschätzung („Impact Assessment“),
- Dokumentations- und Nachweispflichten („Accountability“)
- Data Privacy by Design, Data Privacy by Default

Ausbau der Betroffenenrechte

- Auskunftsrecht und Zugriffsrecht
- Recht auf Berichtigung
- Recht auf Löschung einschließlich eines Rechtes auf „Vergessenwerden“
- Recht auf Datenübertragbarkeit (Datenportabilität)
- Widerspruchsrecht und Widerrufsrecht

Deutlich schärfere Sanktionen

- bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes

Regelungen im Überblick

- Extraterritoriale Anwendung (Art. 3 DSGVO)
- Definitionen (z.B. Profiling und Pseudonymisierung; Art. 4 DSGVO)
- Datenbearbeitungsgrundsätze (Art. 5 DSGVO)
- Rechtmässigkeit der Datenbearbeitung (Art. 6 DSGVO)
- Einwilligung (Art. 7 DSGVO)
- Spezialkategorien von Personendaten (Art. 9 DSGVO, „besonders schützenswerte Daten“)
- Informationspflicht bei direkter Datenbeschaffung (Art. 13 DSGVO)
- Informationspflicht bei indirekter Datenbeschaffung (Art. 14 DSGVO)
- Auskunftsrecht (Art. 15 DSGVO)
- Berichtigungsrecht (Art. 16 DSGVO)
- Löschungsrecht (Art. 17 DSGVO)
- Recht einer Datenbearbeitung zu widersprechen (Art. 21 DSGVO)
- Verantwortung der verantwortlichen Stelle (Art. 24 DSGVO)
- Data Protection by Design / Default (Art. 25 DSGVO)
- Benennung eines Vertreters durch Nicht-EU-Unternehmen, falls DSGVO auf diese anwendbar (Art. 27 DSGVO)
- Auftragsdatenbearbeitung (Art. 28 f. DSGVO)
- Pflicht, alle Datenbearbeitungen zu dokumentieren (Art. 30 DSGVO)
- Notifikation von Datenschutzpannen an die Aufsichtsbehörden (Art. 33 DSGVO)
- Notifikation von Datenschutzpannen an betroffene Personen (Art. 34 DSGVO)
- Datenschutzfolgeabschätzung (Art. 35 DSGVO)
- Benennung eines Datenschutzverantwortlichen (Art. 37 DSGVO)
- Auslandsdatentransfer (Art. 44 ff. DSGVO)
- Administrativbussen (Art. 83 DSGVO)

Informationspflichten

Direkte Datenbeschaffung

Informationspflichten, Art. 13 DSGVO

1. Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
2. Kontaktdaten des Datenschutzbeauftragten
3. Zwecke und Rechtsgrundlage
4. **Ggf. die berechtigten Interessen an einer Datenverarbeitung**
5. Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
6. Ggf. die Absicht einer Übermittlung in Drittstaaten oder an eine internationale Organisation
7. **Weitere Informationen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten**
8. Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer
9. Bestehen von Betroffenenrechten wie Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht oder Datenübertragbarkeit
10. Widerrufsrecht bei einwilligungsbasierter Datenverarbeitung
11. Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
12. Ggf., ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist oder für den Vertragsschluss erforderlich ist
13. **Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling sowie aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person**

Indirekte Datenbeschaffung

Aktive Informationspflicht (Art. 14 DSGVO)

- Informationspflicht gilt auch bei der Beschaffung von Daten aus Drittquellen
- Information muss spätestens einen Monat nach Datenerhebung aus Drittquelle erfolgen
- Ausnahme: Information ist unmöglich, unverhältnismässig oder würde den verfolgten Zweck vereiteln

Inhalt der Information

a. den **Namen und die Kontaktdaten** des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b. zusätzlich die Kontaktdaten des **Datenschutzbeauftragten**;

c. Die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung;

d. die **Kategorien** personenbezogener Daten, die verarbeitet werden;

e. Gegebenenfalls die **Empfänger** oder Kategorien von Empfängern der personenbezogenen Daten;

f. gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem **Drittland** oder einer internationalen Organisation zu **übermitteln**,…

Einwilligung

Einwilligung

Definition (Art. 4 Nr. 11 DSGVO):

- freiwillig
- für den bestimmten Fall
- in informierter Weise und
- unmissverständlich abgegebene Willensbekundung
- in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung

Form

- eindeutige bestätigende Handlung
- schriftliche Erklärung, die auch elektronisch erfolgen kann
- „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.“ (EG 32) → kein Opt-Out

Alteinwilligungen gelten nur dann, wenn die Anforderungen der DSGVO eingehalten wurden (EG 171)

Einwilligungsgrundsätze

- ART. 7 DSGVO
- Informiertheit (Art. 7 Abs. 2 DSGVO)
  - „Für den konkreten Fall und in Kenntnis der Sachlage“
  - Hervorhebungspflicht bei Verbindung mit anderen Texten (AGB?, DSE?)
  - Klare und einfache Sprache
  - In verständlicher und leicht zugänglicher Form
- Widerruflichkeit (Art. 7 Abs. 3 DSGVO)
  - jederzeit mit Wirkung für die Zukunft widerruflich
  - hierauf ist vor Abgabe hinzuweisen
- Freiwilligkeit: (Art. 7 Abs. 4 DSGVO)
  - nicht gegeben bei „klarem Ungleichgewicht“
  - z.B. Zwangssituationen und rechtl. Abhängigkeitsverhältnisse
- Jederzeitige Abrufbarkeit (§ § 13 Abs. 2 TMG, 28 Abs. 3a BDSG)
  - Nach DSGVO **nicht** mehr erforderlich

Kopplungsverbot

Bedrohlich für Werbung, konkrete Bedeutung umstritten!

- ART. 7 Abs. 4 DSGVO

- Kopplungsverbot: Die Erfüllung eines Vertrages darf nicht von der Einwilligung in weitere Datenverarbeitungen abhängig gemacht werden
  - „Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, **von der Einwilligung** zu einer Verarbeitung von personenbezogenen Daten **abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind**.“
- Relevant z.B. bei Gewinnspielen

Einwilligung in Weitergabe von Daten

- OLG Frankfurt vom 28. Juli 2016
  - Einwilligungserklärung in Telefon- und E-Mail-Werbung im Rahmen eines Gewinnspieles unwirksam
  - Grund: Einwilligung für Weitergabe an eine Vielzahl von werbenden Unternehmen zu unbestimmt!
  - Link auf Liste mit 50 werbenden Unternehmen, aber: Geschäftsbereiche der Unternehmen zu wenig spezifisch

- Rechtslage Schweiz
  - Anforderungen an Einwilligung zur Weitergabe von Daten an Dritte liberaler
  - Aber: Nutzer muss eine Vorstellung über den Kreis der Datenempfänger erhalten!
  - Geschäftsbereiche der werbenden Unternehmen auch nach schweizerischem Recht relevant – Kategorisierung genügt!

Berechtigtes Interesse

Zentraler Erlaubnistatbestand

- Berechtigtes Interesse als wichtiger Rechtfertigungsgrund für Datenbearbeitungen (Art. 6 Abs. 1 Satz 1 lit. f DSGVO)
  - Interessenabwägung im Einzelfall: Interesse des Datenbearbeiters gegenüber Persönlichkeitsrechtsinteressen der betroffenen Person
  - Berechtigtes Interesse z.B. wenn Datenbearbeitung für Durchführung eines Online-Einkaufes notwendig (z.B. Beschaffung derjenigen Daten, welche für die Bestellung und Lieferung einer Ware erforderlich; Daten, welche für Zahlungsabwicklung notwendig)
- Im Zweifel: „Reasonable Expectations“
  - Mit welchen Datenbearbeitungen musste die betroffene Person im Zeitpunkt der Datenbeschaffung aufgrund der Umstände rechnen!
- Widerspruchsrecht (Art. 21 DSGVO)
  - Voraussetzungsloses unentgeltliches Widerspruchsrecht
  - Information der betroffenen Person

Auftragsdatenbearbeitung

Auftragsdatenbearbeitung

- Anforderungen an die Auftragsdatenbearbeitung
  - Art. 28 EU-DSGVO
  - Schriftlicher Vertrag
  - Genehmigung von Subunternehmern
  - Instruktions- und Kontrollrechte des Verantwortlichen
  - Unterstützungs- und Kooperationspflichten des Auftragsverarbeiters
  - Sorgfältige Auswahl: Zusammenarbeit nur mit Auftragsverarbeitern, die durch die Implementierung von technischen und organisatorischen Massnahmen die Verarbeitung im Einklang mit der EU-DSGVO sicherstellen können
  - Sicherstellung der Implementierung von technischen und organisatorischen Massnahmen zur Datensicherheit – Nachweispflicht des Auftragsverarbeiters

Datentransfer in die USA

Datentransfer in die USA

- Anforderungen an den Datentransfer in die USA
  - USA kein genügendes Datenschutzniveau – Sicherheitsgarantien notwendig
  - Standard Contract Clauses (Data Controller – Data Processor)
  - Privacy Shield Principles - Zertifizierung ab 1. August 2016 möglich

- Wichtig: Zugriff durch Bearbeiter in den USA gilt auch als Datentransfer

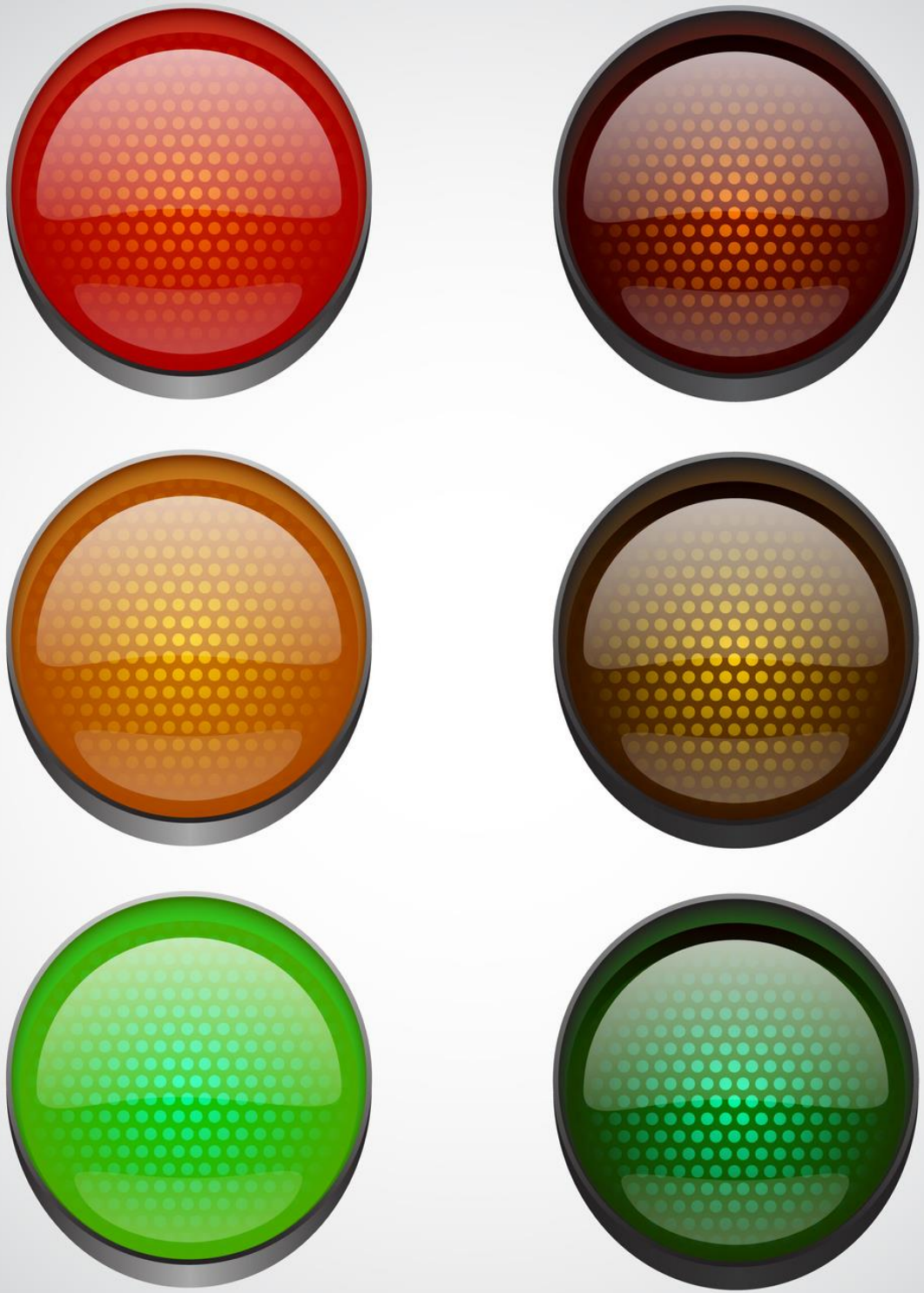
Tracking-Tools

Einbezug von Google Analytics

- LG Hamburg vom 9. August 2016
  - LG Hamburg untersagt einem Online-Händler weitere Nutzung von Google Analytics
  - Grund: Keine Information über die Nutzung von Google Analytics und keine Anonymisierung der IP-Adressen
  - Vorgaben deutsche Datenschutzbehörden (2011)
  - Auftragsdatenverarbeitung: schriftlicher Vertrag mit Google
  - Widerspruchsmöglichkeit: Information in Datenschutzerklärung
  - IP-Anonymisierung
  - Löschung bestehender Analytics-Accounts, falls Anforderungen bisher nicht erfüllt!

Sanktionen

- Verwaltungssanktionen:
- Bis zu 20 Mio. oder 4% des weltweiten Jahresumsatzes
- Wettbewerbsverfahren (Abmahnungen) aufgrund Nichtbeachten der datenschutzrechtlichen Vorgaben, auch Verbandsklagerecht.



Take Home Message

Take Home

- DSGVO wird auf zahlreiche CH-Unternehmen anwendbar sein
- Informationspflichten machen Anpassungen an Privacy Notices und Datenschutzerklärungen notwendig
- Im Gegensatz zur Schweiz für jede Datenbearbeitung Rechtfertigungsgrund
- Hohe Anforderungen an die Einwilligung – Hat insbesondere Auswirkungen auf das digitale Marketing von Unternehmen
- Berechtigtes Interesse erfordert schwierige Interessenabwägung
- Auftragsdatenbearbeitung zukünftig immer wichtiger (Cloud Computing, Einbezug von Applikationen von Drittanbietern, Hosting von Webseiten im Ausland)
- Spezielle Vorsichtsmassnahmen bei Datentransfers in die USA (oder Zugriff auf Daten aus den USA)
- Sanktionierung von DSGVO-Verletzungen – Investitionen in Datenschutz-Compliance notwendig

Typisches Projekt zur Umsetzung der DSGVO - Ablauf

Projektablauf - Übersicht

Lukas Bühlmann, LL.M.
Partner, Zürich
lukas.buehlmann@mll-legal.com
www.mll-legal.com | www.mll-news.com

Dr. Michael Reinle, LL.M.
Senior Associate, Zürich
michael.reinle@mll-legal.com
www.mll-legal.com | www.mll-news.com

Besten Dank

Wir danken für Ihre Zeit und Ihr Interesse