IT & LAW CONSULTING GMBH

Die EU Datenschutzgrundverordnung – Was gilt es zu beachten?

IT-Expo vom 5. April 2017

Referentin: Maria Winkler

Agenda

- **Einführung**
- Anwendungsbereich
- Verarbeitung von Personendaten
- Aufsicht
- Betroffenenrechte
- Weitere Pflichten
- Rechtsschutz & Strafbestimmungen

Einführung

- Die EU Datenschutzgrundverordnung (DSGVO) wurde im April 2016 verabschiedet und ersetzt die nationalen Datenschutzgesetze und somit auch die EU-Datenschutzrichtlinie in der EU.
- Die Umsetzung muss bis Mai 2018 erfolgen.

Agenda

- Einführung
- **Anwendungsbereich**
- Verarbeitung von Personendaten
- Aufsicht
- Betroffenenrechte
- Weitere Pflichten
- Rechtsschutz & Strafbestimmungen

Personendaten (sachlicher Anwendungsbereich)

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. "personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Begriffliches

- **Verantwortliche**: Personen welche sowohl über die Zwecke als auch die Mittel der Verarbeitung von personenbezogenen Daten entscheiden
- **Auftragsverarbeiter**: Personen die im Auftrag des Verantwortlichen solche Daten verarbeiten

Persönlicher Anwendungsbereich

- Ein Schweizer Unternehmen ist nach dem sogenannten „**Marktortprinzip**“ erfasst, wenn:
  - es in der EU Dienstleistungen oder Produkte anbietet und dabei Personendaten von EU-Bürgern bearbeitet;
  - es das Verhalten von Betroffenen aus der EU beobachtet, soweit die Datenverarbeitung damit im Zusammenhang steht;
  - es Daten einer EU-Niederlassung bei sich im Auftrag bearbeitet.
- Ein Schweizer Unternehmen ist nicht erfasst, wenn:
  - es von Personen aus der Schweiz Daten in der Schweiz bearbeitet;
  - es zwar Daten von Kunden aus der EU bearbeitet, ihnen die Produkte und Dienstleistungen jedoch nur in der Schweiz anbietet.

Agenda

- Einführung
- Anwendungsbereich
- **Verarbeitung von Personendaten**
- Aufsicht
- Betroffenenrechte
- Weitere Pflichten
- Rechtsschutz & Strafbestimmungen

Verarbeitung von Personendaten

- In der EU wird für jede Verarbeitung von Personendaten ein Rechtfertigungsgrund gefordert (**Verbot mit Erlaubnisvorbehalt**). Mindestens eine der nachfolgenden Bedingungen muss erfüllt sein:
  - Einwilligung
  - Erforderlich für die Vertragserfüllung
  - Erforderlich für die Erfüllung einer rechtlichen Verpflichtung
  - Schutz lebenswichtiger Interessen
  - Wahrnehmung einer Aufgabe im öffentlichen Interesse
  - Wahrung der berechtigten Interessen

Anforderungen an die Einwilligung

- Einwilligung:
  - Freiwillig
  - Für konkrete Fälle
  - Nach Information über Zweck der Verarbeitung
  - Unmissverständlich
  - Ausdrücklich
  - Nachweisbar
  - Hinweis auf Widerrufsrecht

Auftragsverarbeiter (Art. 28 DSGVO)

- Bei einer Verarbeitung im Auftrag eines Verantwortlichen muss die Geeignetheit des Auftragsverarbeiters vorab geprüft werden.
- Es dürfen nur Auftragsverarbeiter eingesetzt werden, die hinreichende Garantien dafür bieten, dass geeignete technische und auch organisatorische Massnahmen für einen ausreichenden Datenschutz getroffen werden.
- Genehmigte Verhaltensregeln (Art. 40 DSGVO) oder Zertifizierungen (Art. 42 DSGVO) können solche Garantien belegen.
- Für die Verarbeitung durch einen Auftragsverarbeiter muss mit ihm ein Vertrag über die weisungsgebundene Tätigkeit abgeschlossen werden.

Datentransfer ins Ausland

- Zulässig sind Datentransfers an Drittländer, welche ein **angemessenes datenschutzrechtliches Schutzniveau** haben.
- Die Schweiz verfügt gemäss dem Angemessenheitsbeschluss der EU über einen angemessenen Datenschutz. Zurzeit wird das Datenschutzgesetz revidiert.
- Durch **vertragliche Garantien** oder **Binding Corporate Rules** ist ein Datentransfer in unsichere Drittländer trotzdem möglich.
- Neu können auch **Codes of Conduct** genehmigt oder **Zertifikate** ausgestellt werden.

Agenda

- Einführung
- Anwendungsbereich
- Verarbeitung von Personendaten
- **Aufsicht**
- Betroffenenrechte
- Weitere Pflichten
- Rechtsschutz & Strafbestimmungen

Vertreter in der EU

- Schweizer Unternehmen, die unter die DSGVO fallen, müssen **schriftlich einen Vertreter in der EU** bezeichnen, der den Aufsichtsbehörden und den betroffenen Personen als Anlaufstelle für sämtliche Fragen im Zusammenhang mit der Gewährleistung der DSGVO dient.
- Der Vertreter muss **in einem der Mitgliedsstaaten niedergelassen** sein, in dem die betroffenen Personen, deren Daten bearbeitet werden, sich befinden.
- Es ist unklar, welche Funktion der Vertreter genau hat („Briefkasten“ oder „Verantwortlicher“).

Aufsichtsbehörden

- Schweizer Unternehmen, die unter die DSGVO fallen, unterstehen einer **doppelten Datenschutzaufsicht**:
  - dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB);
  - den zuständigen Aufsichtsbehörden der EU.
- Das Konzept der „federführenden Aufsichtsbehörde“ gilt für Nicht-EU-Staaten nicht (One-Stop-Shop).
- Allerdings ist umstritten, ob ein Tätigwerden einer EU-Aufsichtsbehörde in der Schweiz nach Schweizer Recht zulässig ist (Territorialprinzip).

Datenschutzbeauftragter

- **Private Unternehmen (Verantwortliche und Auftragsverarbeiter)** müssen einen Datenschutzbeauftragten benennen, wenn ihre **Kerntätigkeit:**
  - eine **umfangreiche regelmässige und systematische Überwachung** von Betroffenen erforderlich machen;
  - in der **umfangreichen Verarbeitung besonderer Kategorien von Daten** besteht (Art. 9 und Art. 10 DSGVO).
- Der Datenschutzbeauftragte muss über das erforderliche Fachwissen verfügen. Die **Kontaktdaten** des Datenschutzbeauftragten müssen veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.

Agenda

- Einführung
- Anwendungsbereich
- Verarbeitung von Personendaten
- Aufsicht
- **Betroffenenrechte**
- Weitere Pflichten
- Rechtsschutz & Strafbestimmungen

Betroffenenrechte

- Recht auf Löschung der Daten („Vergessenwerden“)
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht, nicht einer ausschliesslich auf automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden
- Auskunftsrecht
- Informationsrechte bei der Erhebung von personenbezogenen Daten

Recht auf Löschung (1) (Art 17 DSGVO)

- Voraussetzungen bei deren Vorliegen eine Löschung verlangt wird:
  - der Zweck für die Datenverarbeitung ist weggefallen (lit. a);
  - die Einwilligung wird widerrufen (lit. b);
  - es wird Widerspruch von der betroffenen Person eingelegt (lit. c);
  - die Daten wurden unrechtmässig verarbeitet (lit. d);
  - zur Erfüllung einer rechtlichen Verpflichtung ist die Löschung nötig (lit. e);
  - die Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben (lit. f).

Recht auf Löschung (2) (Art 17 DSGVO)

- Google Spain Entscheidung
  - Mario Costeja Gonzales reichte Beschwerde bei der spanischen Datenschutzaufsichtsbehörde ein, da Google zu seinem Namen Suchtreffer mit Links auf Tageszeitungsartikel anzeigte.
  - Die Artikel zeigten auf, dass das Grundstück von Gonzales aufgrund seiner Schulden versteigert wurde.
  - Die spanische Datenschutzaufsichtsbehörde verlangte von Google die Löschung der Suchtreffer. Google erhob ihrerseits Klage, weshalb der Fall an den EuGH ging.
  - Der EuGH entschied, dass wenn die **Betroffeneninteressen** diejenigen der Öffentlichkeit am Zugang der Information **überwiegen**, eine **Löschung** der Suchergebnisse **möglich** sein muss („**digitaler Radiergummi**“).

Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

- Betroffene dürfen verlangen, dass die personenbezogenen Daten, welche mithilfe automatisierten Verfahren verarbeitet werden, direkt von einem Verantwortlichen einem anderen Verantwortlichen **übermittelt** werden, soweit dies technisch machbar ist.
- Dies gilt, wenn die Betroffenen in die Verarbeitung der personenbezogenen Daten **eingewilligt** haben oder die Verarbeitung zur **Erfüllung eines Vertrags** erforderlich ist.

Widerspruchsrecht (Art. 21 DSGVO)

- Betroffene dürfen trotz rechtmässiger Verarbeitung **Widerspruch** einlegen, wenn die Verarbeitung ihrer personenbezogenen Daten:
  - für die Wahrnehmung einer Aufgabe, im öffentlichen Interesse liegt;
  - oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
  - oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist.

Agenda

- Einführung
- Anwendungsbereich
- Verarbeitung von Personendaten
- Aufsicht
- Betroffenenrechte
- **Weitere Pflichten**
- Rechtsschutz & Strafbestimmungen

Verarbeitungsverzeichnisse (Art. 30 DSGVO)

- **Verantwortliche und Auftragsverarbeiter** führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen.
- Wesentliche Angaben über die Verarbeitung müssen gemacht werden z.B.:
  - Zweck der Verarbeitung
  - Kategorie der Daten
  - Kategorie der Betroffenen und der Empfänger
- Das Verzeichnis ist nicht öffentlich zugänglich.
- **Verstösse** dagegen werden mit **Geldbussen** bestraft.

Data Breach Notifications

- Bei Verstössen gegen Massnahmen zur Datensicherheit muss dies **verzeichnet** und der Datenschutzbehörde **gemeldet** werden.
- Bei einem voraussichtlich **hohen Risiko** von Auswirkungen für die persönlichen Freiheiten und Rechte der Betroffenen müssen zusätzlich die **Betroffenen informiert** werden.
- Unternehmen müssen Prozesse vorsehen um die Data Breaches zu erfassen und zu melden.

Datenschutz-Folgenabschätzung

(Art. 35 DSGVO)

- Mit der Datenschutz-Folgenabschätzung sollen **Risiken eingeschätzt und vermindert** werden.
- Eine Datenschutz-Folgenabschätzung muss durchgeführt werden, wenn die Verarbeitungsvorgänge ein **hohes Risiko** darstellt für die persönlichen Rechte und Freiheiten der Betroffenen (z.B. weitreichende Überwachung von öffentlichen Bereichen).
- Ergibt die Datenschutz-Folgenabschätzung, dass die geplante Datenverarbeitung ein hohes Risiko mit sich bringt, trifft den Verantwortlichen diesbezüglich eine **Informationspflicht** gegenüber der Aufsichtsbehörde.

Privacy by Design und by Default

(Art. 25 DSGVO)

- **Privacy by Design**

  Die Verantwortlichen müssen sicherstellen, dass geeignete technische und organisatorische Massnahmen getroffen werden um die Datenschutzgrundsätze umzusetzen (z.B. Datenminimierung oder Zugriffsberechtigungen).

- **Privacy by Default**

  Durch Voreinstellungen muss sichergestellt werden, dass nur die für einen bestimmten Zweck erforderlichen personenbezogenen Daten verarbeitet werden (z.B. Social Media auf „nicht öffentlich“ einstellen).

Agenda

- Einführung
- Anwendungsbereich
- Verarbeitung von Personendaten
- Aufsicht
- Betroffenenrechte
- Weitere Pflichten
- **Rechtsschutz & Strafbestimmungen**

Rechtsbehelfe

- Jede betroffene Person hat das Recht auf **Beschwerde bei einer Aufsichtsbehörde**, wenn sie glaubt, dass eine Verarbeitung der sie betreffenden Daten gegen die DSGVO verstösst (Art. 77 DSGVO).
- Jede natürliche oder juristische Person hat das Recht auf einen wirksamen **gerichtlichen Rechtsbehelf** (Art. 78, 79 DSGVO):
  - gegen eine Aufsichtsbehörde
  - gegen Verantwortliche oder Auftragsverarbeiter
- Ist einer Person wegen eines Verstosses gegen die DSGVO ein Schaden entstanden, kann sie **Schadenersatz** geltend machen.

Sanktionen

- Geldbussen sind bis zu **EUR 20 Mio**. oder bei Unternehmen bis zu **4%** des gesamten weltweit erzielten Jahresumsatzes möglich.

Was tun?

IT & LAW CONSULTING GMBH

Vielen Dank für Ihre Aufmerksamkeit!

Maria Winkler
IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug

Tel. +41 41 711 74 08
Fax +41 41 711 74 07
maria.winkler@itandlaw.ch
www.itandlaw.ch