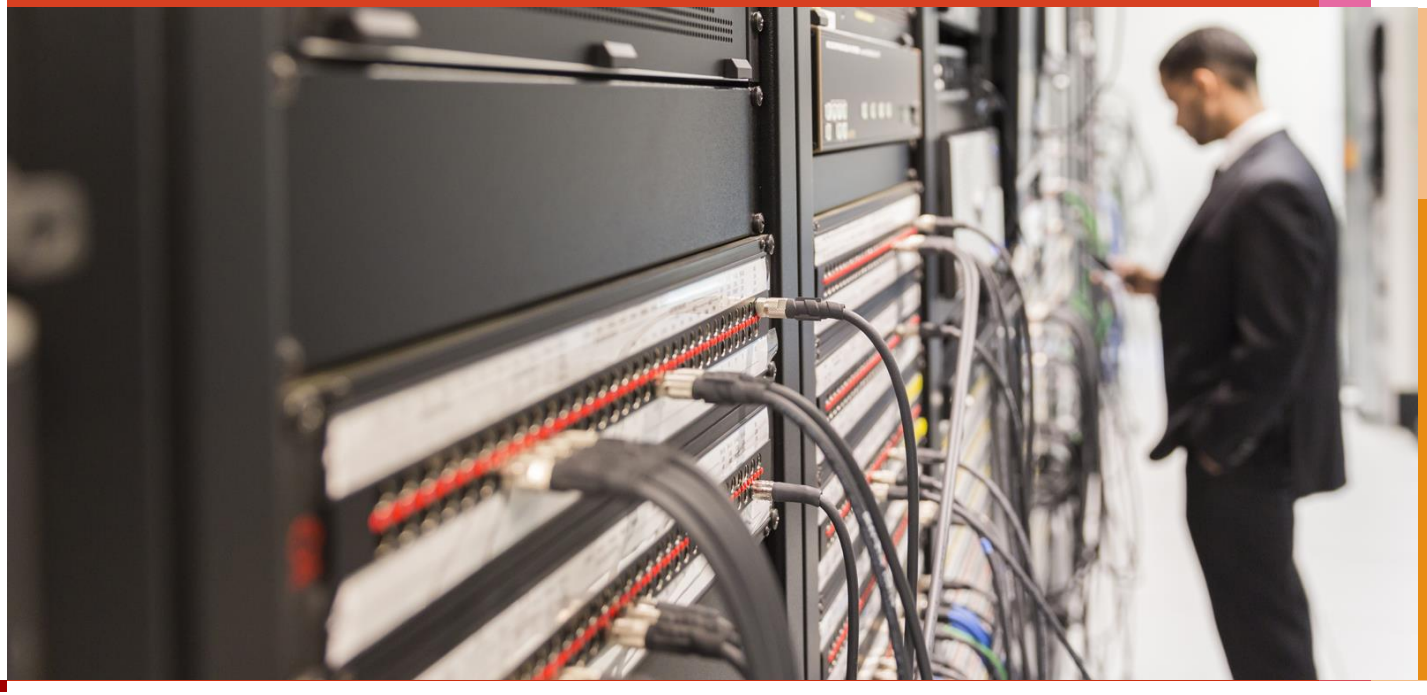
PwC Legal Switzerland

# *KMU Podium*
# EU-Datenschutz:Auswirkungen auf meine Firma?

*30 August 2018*



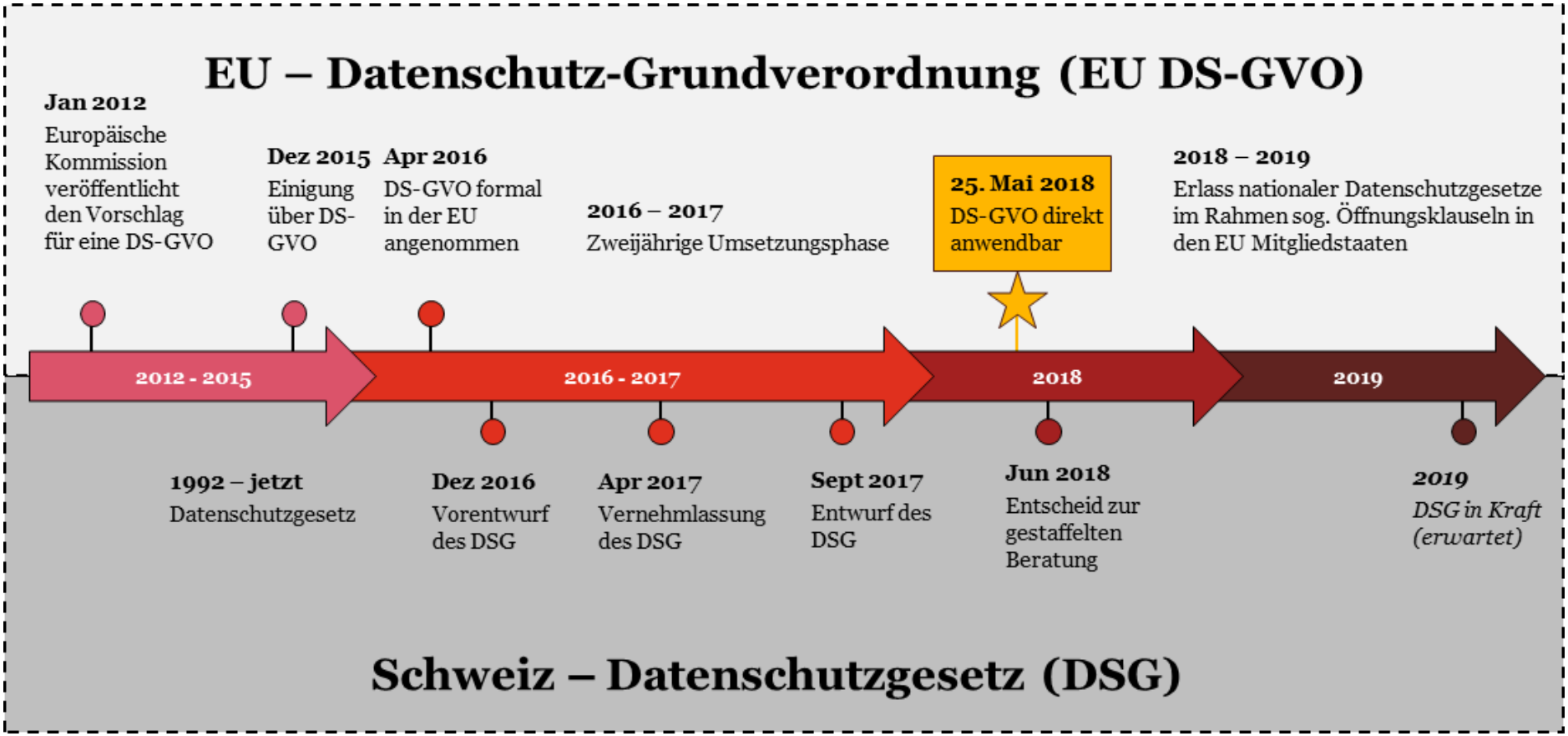
pwc

# *Agenda*

1. **Einführung**
2. **EU Datenschutz-Grundverordnung (DS-GVO)**
3. **Ausblick auf das revidierte Datenschutzgesetz in der Schweiz**

# 1 Einführung

# *Neuerungen im Datenschutz*
## *Zeitliche Entwicklung EU / Schweiz*



# *Neuerungen im Datenschutz*
## *Gegenüberstellung EU / Schweiz*

**EU-Datenschutz-Grundverordnung**
(DS-GVO)

- Weiterer Anwendungsbereich schliesst auch Schweizer Unternehmen möglicherweise mit ein.
- Neue Pflichten und Prinzipien
- Hohe Bussen im Falle der Nichteinhaltung der Verordnung (bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes, je nachdem welcher Betrag höher ist)
- In Kraft seit Mai 2016 – anwendbar ab Mai 2018

**Datenschutzgesetz**
(rev. DSG)

- Stärkung des Datenschutzes. Es soll der «Adäquanzentscheid» für Datentransfers EU-CH aufrecht erhalten werden.
- Anpassung an Datenschutzniveau der EU
- Bussen bis zu 250'000 CHF (auf Antrag)
- Tritt vermutlich in 2019 in Kraft (Verzögerung aufgrund gestaffelter Beratung)

# *Warum sollen Schweizer Unternehmen EU-Recht befolgen?*

Weiter und extraterritorialer Anwendungsbereich der DS-GVO!

**Art. 3 (1) DS-GVO:**
*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.*

**Art. 3 (2) DS-GVO:**
*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 steht mit:*

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

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

**Es muss in jedem Einzelfall geprüft werden, ob die DS-GVO Anwendung findet!**

# 2 *EU Datenschutz-Grundverordnung (DS-GVO)*

# *EU Datenschutz-Grundverordnung (DS-GVO)*

## *Personenbezogene Daten: Begriffsbestimmungen*


### Art. 4(1): personenbezogene Daten

„Personenbezogene Daten“ meint 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.

### Art. 9(1): besondere Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

### Art. 4(2): Verarbeitung

„Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

### Art. 4(4): Profiling

„Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

# Generelle Prinzipien der Datenbearbeitung


- *Datenschutz beschränkt sich nicht nur auf IT-Sicherheit.*
- *Jede Verletzung der Grundsätze stellt eine Datenschutzverletzung dar und gilt als Verletzung der persönlichen Rechte und Freiheiten der betroffenen Person.*
- *Die Rechenschaftspflicht bedeutet (i) eine Umkehrung der Beweislast und damit (ii) die Einrichtung einer Datenschutzrichtlinie, um die EU DS-GVO-Einhaltung zu gewährleisten.*

# *EU Datenschutz-Grundverordnung (DS-GVO)*
## *Rechte der betroffenen Personen (I/II) - Auswahl*

**Transparente Kommunikation, Art. 12(1) & (2) DS-GVO**

Um eine faire und rechtmässige Verarbeitung zu gewährleisten, müssen die Verantwortlichen den betroffenen Personen bestimmte Mindestangaben über die Erhebung und Weiterverarbeitung ihrer personenbezogener Daten machen. Diese Informationen müssen in einer prägnanten, transparenten, verständlichen und leicht zugänglicher Form in klarer und einfachen Sprache zur Verfügung gestellt werden. Alle Informationen, die Kindern zur Verfügung gestellt werden, sollten so klar und deutlich formuliert sein, dass ein Kind sie leicht versteht.

Die für die Verarbeitung Verantwortlichen sind gesetzlich verpflichtet, den Rechten der betroffenen Personen Geltung zu verschaffen.

**Recht auf Information, Art. 13 DS-GVO**

Die betroffenen Personen haben das Recht, Informationen über die Identität des für die Verarbeitung Verantwortlichen, die Gründe für die Verarbeitung ihrer personenbezogenen Daten und andere relevante Informationen zu erhalten, die für eine faire und transparente Verarbeitung personenbezogener Daten erforderlich sind.

**Auskunftsrecht, Art. 15 DS-GVO**

Eine Person hat folgende Rechte in Bezug auf den Inhaber der Datenverarbeitung:

- Eine Bestätigung darüber zu erhalten, ob persönlichen Daten über sie verarbeitet werden;
- Zugriff auf die Daten (d.h. auf eine Kopie); und
- das Recht mit zusätzlichen Informationen über die Verarbeitung versorgt zu werden.

# *EU Datenschutz-Grundverordnung (DS-GVO)*

## *Rechte der betroffenen Personen (II/II) - Auswahl*

### Recht auf Berichtigung, Art. 16 DS-GVO

Verantwortliche müssen sicherstellen, dass ungenaue oder unvollständige Daten gelöscht oder berichtigt werden. Die betroffenen Personen haben das Recht auf Berichtigung unrichtiger personenbezogener Daten.

### Recht auf Löschung ('Recht auf Vergessenwerden'), Art. 17 DS-GVO

Das Recht auf Löschung besagt, dass die betroffenen Personen das Recht haben, ihre personenbezogenen Daten aus den Systemen der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter unter bestimmten Umständen zu entfernen, z.B. indem sie ihre Einwilligung zur Verarbeitung widerrufen oder der Zweck für die Bearbeitung entfallen ist.

### Recht auf Datenübertragbarkeit, Art. 20 DS-GVO

Die betroffenen Personen haben das Recht, eine Kopie ihrer personenbezogenen Daten in einem allgemein gebräuchlichen, maschinenlesbaren Format zu erhalten und ihre personenbezogenen Daten von einem für die Verarbeitung Verantwortlichen zu einem anderen zu übertragen oder die Daten direkt zwischen den für die Verarbeitung Verantwortlichen übertragen zu lassen.

# *Wirkung der DS-GVO auf Unternehmen*

## *Pflichten auf Unternehmensseite… (eine Auswahl)*

| | |
|---|---|
| **Verzeichnis** | Unternehmen, die personenbezogene Daten verarbeiten, sind für die Einhaltung der Verarbeitungsgrundsätze verantwortlich (Rechenschaftspflicht) und müssen ein **Verzeichnis von Verarbeitungstätigkeiten** führen. |
| **DPIA** | Ein Datenschutzfolgenabschätzung (Data Protection Impact Assessment, kurz DPIA) ist notwendig, wenn eine Form der Verarbeitung, **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten** natürlicher Personen zur Folge hat (zum Beispiel Profiling). |
| **Meldepflicht** | Im Falle einer "Verletzung des Schutzes personenbezogener Daten" muss der Verantwortliche ohne Verzögerung und **nicht später als 72 Stunden** die zuständige Datenschutzbehörde informieren, wenn die Verletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Liegt ein hohes Risiko vor, muss die betroffene Person informiert werden. |
| **Governance** | Rechenschaftspflicht Art.5(2) DS-GVO<br>- Nachweispflicht der Compliance mit den Bearbeitungsprinzipien bzw. der DS-GVO<br>- U.a. Datenschutz-Reglement, Weisungen, Verantwortlichkeiten, Erklärungen<br>- **Beweis-Umkehr! (nicht so im DSG!)** |
| **Privacy by design & by default** | Unternehmen müssen **technische und organisatorische Massnahmen** treffen, die darauf ausgerichtet sind, die Datenschutzgrundsätze (wie z.B. Datenminimierung) bereits bei der Planung interner Prozesse sowie von Produkten und Dienstleistungen wirksam umzusetzen. Mittels Voreinstellungen sollen nur diejenigen personenbezogenen Daten bearbeitet werden, welche für den Zweck erforderlich sind. |

**DPO falls nötig**

# *Sanktionen aus der DS-GVO*
## *Geldbussen und Haftung/Schadenersatz…*

**Übersicht: Fälle und Bussenhöhe**

***10 Mio. €** oder **2%** des globalen Jahresumsatzes (was immer höher ist)*

- Verletzung: **Datenschutz durch Technik**, **Joint Controllers**, **Vertreter** in der EU, **Auftragsverarbeiter**, **Verzeichnis der Verarbeitungstätigkeiten**, **Zusammenarbeit mit der Aufsichtsbehörde**, **Sicherheit der Verarbeitung (TOMs)**, **Meldepflicht** gegenüber Aufsichtsbehörde oder betroffener Person, **DPIA**, **Datenschutzbeauftragter** (DPO), **Zertifizierung**
- Verletzung: Bedingungen für die **Einwilligung eines Kindes** werden nicht eingehalten
- Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

***20 Mio. €** oder **4%** des globalen Jahresumsatzes (was immer höher ist)*

- Verletzung: **Grundsätze der Verarbeitung**
- Verletzung: Bestimmungen über die **Rechte der betroffenen Personen**,
- Verletzung: Bestimmungen betreffend **Übermittlung von personenbezogenen Daten in das Ausland**
- Verletzung gewisser **Pflichten gemäss Rechtsvorschriften der Mitgliedstaaten**
- **Nichtbefolgung einer Anweisung** oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde oder Nichtgewährung des Zustands

**Wichtig:** Erleidet eine betroffene Person aufgrund eines Verstosses gegen die DS-GVO einen materiellen oder immateriellen Schaden, hat er einen **Anspruch auf Schadenersatz.**

# 3 *Ausblick auf das revidierte Datenschutzgesetz in der Schweiz*

# *Revision des Datenschutzgesetzes in der Schweiz*
## *Zusammenfassung zum Entwurf DSG*

- **Kein “Swiss finish”**
- Erhöhte Transparenz, verschärfte Sanktionen
- **Risikobasierter Ansatz**
- **Weniger Melde- und Konsultationspflichten als in der EU**
- Stärkere Rolle und Position des EDÖB
- **Keine Umkehr der Beweislast**
- Kein spezifischer Schutz von Kinder
- Fehlendes Prinzip der Datenübertragbarkeit
- **Schwächere Strafbestimmungen als in der EU (max. CHF 250’000)**

## *Ihr Kontakt…*

**Susanne Hofmann**
Legal Compliance Lead
PwC Legal Services
+41 58 792 17 12
susanne.hofmann@ch.pwc.com

***Besten Dank für die Aufmerksamkeit!***