IT & LAW | CONSULTING GMBH

EU-Datenschutzverordnung DSGVO

Seminar SVDS

mag. iur. Maria Winkler

09. November 2018

IT & LAW CONSULTING GMBH

Agenda

- **Einführung**
- Anwendungsbereich der DSGVO
- Auswirkungen der DSGVO auf die Organisation
- Neue Prozesse
- Strafbestimmungen
- Zusammenfassung

IT & LAW CONSULTING GMBH

Revisionen EU/EWR und Schweiz

- Die EU Datenschutzgrundverordnung (**DSGVO**) wurde im April 2016 verabschiedet und ersetzt die nationalen Datenschutzgesetze in der EU und die EU-Datenschutzrichtlinie.
- Die **DSGVO** ist seit dem **25. Mai 2018** in Kraft.
- Die **DSGVO** gilt seit dem **20. Juli 2018** auch im EWR.
- Auch das Schweizer DSG wird zurzeit revidiert. Der Entwurf (E-DSG) sowie die Botschaft des Bundesrates wurden am 15. September 2017 veröffentlicht. Das revidierte DSG ist **an die EU DSGVO angelehnt.**
- Es ist **ungewiss**, wann das revidierte DSG in Kraft treten wird, da der Entwurf zurzeit im Parlament in 2 Etappen behandelt wird.
- Bei der Umsetzung der DSGVO bestehen noch viele unbeantwortete Fragen, aufgrund der zur Zeit noch **fehlenden Praxis**.

IT & LAW | CONSULTING GMBH

Begriffe
(Art. 4 DSGVO)

- **Betroffene Person:** Natürliche Person, über die Daten bearbeitet werden.
- **Verarbeitung / Bearbeitung**: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten z.B. Erfassen, Ordnen, Speichern, Übermitteln, Löschen.

Wichtig

- Juristische Personen sind **nicht** von der DSGVO erfasst.
- Jeder Umgang mit Personendaten ist erfasst, auch wenn Daten beispielsweise „nur“ gespeichert werden.

IT & LAW CONSULTING GMBH

Rollen
(Art. 4 DSGVO)

- **Verantwortlicher**: Natürliche oder juristische Personen oder Behörden, die über die Zwecke und die Mittel der Verarbeitung von personenbezogenen Daten entscheiden.
- **Auftragsverarbeiter**: Natürliche oder juristische Personen oder Behörden, die im Auftrag des Verantwortlichen solche Daten verarbeiten (Dienstleister, Provider).
- **Gemeinsam Verantwortliche:** Zwei oder mehrere Verantwortliche bestimmen über Zwecke und Mittel der Verarbeitung.

Wichtig

- Der Grossteil der datenschutzrechtlichen Pflichten liegt beim Verantwortlichen.
- Hinweis: Die herrschende Meinung geht davon aus, dass Steuerberater die Rolle des Verantwortlichen ausüben (Bsp. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf).

IT & LAW CONSULTING GMBH

Agenda

- Einführung
- **Anwendungsbereich der DSGVO**
- Auswirkungen der DSGVO auf die Organisation
- Neue Prozesse
- Strafbestimmungen
- Zusammenfassung

IT & LAW CONSULTING GMBH

Räumlicher Anwendungsbereich (1/4)

Niederlassungsprinzip (Art. 3 Abs. 1 DSGVO)

- Die DSGVO gilt für alle Unternehmen, die **in der EU eine Niederlassung** haben und in diesem Zusammenhang Personendaten bearbeiten.
- Dies unabhängig davon, ob sie dabei als „Verantwortliche“ oder als „Auftragsverarbeiter“ tätig werden und unabhängig davon, ob die Verarbeitung in der Union stattfindet.
- Unklar ist, ob Vertriebspartner oder Tochtergesellschaften als „Niederlassungen“ gelten.
- Ein Schweizer Unternehmen, das eine rechtlich unselbständige Zweigniederlassung eines EU-Unternehmens ist, fällt unter die DSGVO.

IT & LAW | CONSULTING GMBH

Räumlicher Anwendungsbereich der DSGVO (2/4)

- Ein Schweizer Unternehmen ist nach dem sog. „**Marktortprinzip**“ (Art. 3 Abs. 2 DSGVO) erfasst, wenn:
  - es in der EU Dienstleistungen oder Waren anbietet und dabei Personendaten von natürlichen Personen bearbeitet, die sich in der EU befinden (B2C);
  - es das Verhalten von Betroffenen aus der EU beobachtet, soweit die Datenverarbeitung damit im Zusammenhang steht.

- Ein Schweizer Unternehmen ist **nicht** erfasst, wenn:
  - es Waren oder Dienstleistungen an Unternehmen in der EU anbietet (B2B);
  - es von Personen aus der Schweiz Daten in der Schweiz bearbeitet;
  - es Grenzgänger beschäftigt.

IT & LAW | CONSULTING GMBH

Räumlicher Anwendungsbereich der DSGVO (3/4)

Angebot von Waren oder Dienstleistungen

- Erfasst sind Verantwortliche und Auftragsverarbeiter.
- die DSGVO gilt auch, wenn die Waren oder Dienstleistungen unentgeltlich angeboten werden.
- das Angebot muss auf die EU ausgerichtet sein (blosse Bestellmöglichkeit über den Webshop genügt nicht).

Verhaltensbeobachtung

- Erfasst ist nur die Beobachtung des Internetverhaltens (Tracking mit und ohne Profiling).
- Nur auf Dauer angelegtes Tracking von gewisser Intensität ist erfasst (da sonst keine „Beobachtung“).
- Beispiele: Cookies, die individuelle Rückverfolgbarkeit ermöglichen, Social-Plugins, etc. sofern diese einen Personenbezug haben.

IT & LAW | CONSULTING GMBH

Räumlicher Anwendungsbereich der DSGVO (4/4)

Anwendbarkeit der DSGVO auf Steuerberater/Treuhänder

- Steuerberater bearbeiten im Rahmen ihrer Dienstleistungen Personendaten (Art. 4 DSGVO), da sie mit Informationen arbeiten, welche die Identifikation einzelner Personen ermöglicht. Die Frage, ob die jeweilige Steuerberatung **territorial** unter die DSGVO fällt, ist im Einzelfall abzuklären.
- Wird die Steuerberatung für eine **natürliche Person** aus dem **EU-Raum/ EWR** erbracht, fällt sie unter die DSGVO.
- Die DSGVO kann **indirekt** zur Anwendung kommen, wenn eine Steuerberater für ein Unternehmen mit Sitz in der EU oder dem EWR als Auftragsdatenbearbeiter tätig wird, indem er beispielsweise für ein solches Unternehmen Daten archiviert.

IT & LAW | CONSULTING GMBH

Agenda

- Einführung
- Anwendungsbereich der DSGVO
- **Auswirkungen der DSGVO auf die Organisation**
- Neue Prozesse
- Strafbestimmungen
- Zusammenfassung

IT & LAW | CONSULTING GMBH

Vertreter in der EU

(Art. 27 DSGVO)

- Schweizer Unternehmen, die unter die DSGVO fallen, müssen **schriftlich einen Vertreter in der EU** bezeichnen.
- Eine **Ausnahme** besteht bei nur gelegentlicher Datenverarbeitung, sofern keine oder nur wenige sensitive Daten verarbeitet werden.
- Er dient als Anlaufstelle für sämtliche Fragen im Zusammenhang mit der Umsetzung der DSGVO.
- Der Vertreter muss **in einem Mitgliedstaat** niedergelassen sein, in dem sich die betroffenen Personen befinden.
- Es gibt keine Vorgaben betreffend die Qualifikation des Vertreters.
- Die **Haftung** des Vertreters ist unklar. Eine Haftungsbefreiung durch die Benennung eines Vertreters ist aber nicht möglich.

IT & LAW CONSULTING GMBH

Bezeichnung eines Datenschutzbeauftragten

(Art. 37 Abs. 1 und Abs. 4 DSGVO)

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

IT & LAW CONSULTING GMBH

Agenda

- Einführung
- Anwendungsbereich der DSGVO
- Auswirkungen der DSGVO auf die Organisation
- **Neue Prozesse**
- Strafbestimmungen
- Zusammenfassung

IT & LAW CONSULTING GMBH

Rechenschaftspflicht

(Art. 5 Abs. 2 DSGVO)

- Aufgrund der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) muss das Unternehmen die **Einhaltung der DSGVO nachweisen** können, sofern diese anwendbar ist.
- Dies führt zu einer Beweislastumkehr.
- Hieraus resultieren umfangreiche **Dokumentationspflichten**.

IT & LAW | CONSULTING GMBH

Rechtmässigkeit

(Art. 5 Abs. 1 a und Art. 6 DSGVO)

- Die Verarbeitung ist rechtmässig, wenn eine gesetzliche Grundlage vorliegt.
- Mindestens eine der folgenden Bedingungen muss erfüllt sein.
  - Bestimmte und informierte **Einwilligung**;
  - **Vertrag** mit der betroffenen Person;
  - **gesetzliche Verpflichtung**;
  - **Schutz von lebenswichtigen Interessen** der betroffenen Person oder einer anderen natürlichen Person;
  - **Wahrung von berechtigten Interessen** des Verantwortlichen oder eines Dritten
- **Hinweis:** Die gesetzliche Grundlage muss während der ganzen Dauer der Verarbeitung der Personendaten gegeben sein.

IT & LAW CONSULTING GMBH

Betroffenenrechte

- Informationspflichten Art. 12 bis 14 DSGVO;
- Auskunftsrecht Art. 15 DSGVO;
- Recht auf Berichtigung Art. 16 DSGVO;
- Recht auf Löschung Art. 17 DSGVO;
- Recht auf Datenübertragbarkeit Art. 20 DSGVO;
- Recht auf Einschränkung und Widerspruch Art. 18 und 21 DSGVO.

- **Empfehlung:**
  - Prüfen Sie die Datenschutzerklärungen auf Ihrer Website und in Ihren Verträgen.
  - Setzen Sie Prozesse auf, um die Betroffenenrechte systematisch zu gewährleisten.

IT & LAW CONSULTING GMBH

Verarbeitungsverzeichnis

(Art. 30 DSGVO)

- Das Verzeichnis dient dem **Nachweis, dass die datenschutzrechtlichen Vorschriften eingehalten** werden.
- Das Verzeichnis des Verantwortlichen hat einen Mindestinhalt:
  - Name und Kontaktangaben des Verantwortlichen;
  - Zweck der Verarbeitung (z.B. Personalaktenführung, Finanzbuchhaltung);
  - Kategorien der Daten (z.B. Lohndaten, Name, Adresse etc.);
  - Kategorien von Empfängern (z.B. Auftragsverarbeiter);
  - Übermittlung in Drittländer (sofern dies geschieht);
  - Speicherdauer.
- Das Verzeichnis des Auftragsverarbeiters hat einen reduzierten Mindestinhalt.
- **Empfehlung:** Prüfen Sie pro Verarbeitungsprozess die **Rolle Ihres Unternehmens** (Auftragsverarbeiter oder Verantwortlicher) und erstellen Sie das jeweilige Verzeichnis.

IT & LAW | CONSULTING GMBH

Datenschutz-Folgenabschätzung (DSFA)

(Art. 35 DSGVO)

- Bringt eine Verarbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich, muss der Verantwortliche eine **Datenschutz-Folgenabschätzung** (DSFA) erstellen.
- Die DSFA dient der systematischen Risikoeindämmung. Risiken müssen erkannt und anhand angemessener Mittel verringert werden.
- Um ihren Zweck zu erfüllen, muss die DSFA **vor der ersten Datenbearbeitung** erfolgen. Ähnliche Verarbeitungsvorgänge mit einem ähnlichen Risiko können gemeinsam beurteilt werden.
- Als hohes Risiko gilt beispielsweise:
  - Die systematische und umfassende Bewertung persönlicher Aspekte.
  - Umfangreiche Verarbeitung besonderer Kategorien von Personendaten.

IT & LAW | CONSULTING GMBH

Übersicht über die Durchführung einer DSFA

- **Stufe 1:** Klärung, ob die Bearbeitung ein **hohes Risiko** für die Persönlichkeit oder die Grundrechte **der betroffenen Personen** mit sich bringt **(Schwellwert-Analyse)**
- **Stufe 2:** Durchführung der DS-Folgenabschätzung
  - **Beschreibung der Datenbearbeitung** (Zweck, Kategorien der betroffenen Personen, Kategorien der Empfänger, Technologien, etc.)
  - Bewertung der Risiken für die betroffenen Personen (gemäss Stufe 1)
  - Massnahmen, die zur Reduktion der Risiken ergriffen werden
- **Stufe 3:** Konsultation der Aufsichtsbehörde, falls trotz der ergriffenen Massnahmen ein hohes Risiko bleibt.

IT & LAW CONSULTING GMBH

Technische und organisatorische Massnahmen

(Art. 5 (f) DSGVO und Art. 32 DSGVO)

- Der Verantwortliche und der Auftragsverarbeiter treffen **geeignete technische und organisatorische Massnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- Die Massnahmen gewährleisten insbesondere Schutz:
  - gegen unbefugte oder unrechtmässige Verarbeitung;
  - vor unbeabsichtigten Verlust;
  - vor Schädigung;
  - vor Zerstörung.
- Folgendes muss berücksichtigt werden:
  - die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen;
  - der Stand der Technik;
  - Implementierungskosten;
  - die Art, den Umfang, die Umstände und den Zweck der Verarbeitung.

IT & LAW | CONSULTING GMBH

Privacy by Design / by Default

Privacy by Design

➢ Der Verantwortliche muss:

- mit geeigneten technischen und organisatorischen Massnahmen die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umsetzen (z.B. Pseudonymisierung);
- die Datenverarbeitung so gestalten, dass die gesetzlichen Anforderungen erfüllt werden.

Privacy by Default

➢ Der Verantwortliche muss:

- durch Voreinstellungen sicherstellen, dass nur Personendaten verarbeitet werden, die für den Verarbeitungszweck erforderlich sind;
- dies betrifft die Menge der erhobenen Personendaten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

IT & LAW | CONSULTING GMBH

Meldung von Datensicherheitsverletzungen

(Art. 33 and 34 DSGVO)

- Es handelt sich um eine Verletzung der Sicherheit, die **ungeachtet der Absicht oder der Widerrechtlichkeit** dazu führt, dass Personendaten **verlorengehen**, **gelöscht**, **vernichtet** oder **verändert** werden oder Unbefugten **offengelegt** oder **zugänglich** gemacht werden.
- Verstösse gegen **Massnahmen zur Datensicherheit** müssen durch Verantwortliche **dokumentiert** und der Aufsichtsbehörde (spätestens innerhalb von 72 Stunden) **gemeldet** werden.
- Wenn es zu ihrem Schutz erforderlich ist, bzw. wenn voraussichtlich ein **hohes Risiko** für die betroffenen Personen besteht, muss auch die betroffene Person informiert werden.
- **Auftragsverarbeiter** müssen alle Datensicherheitsverletzungen dem Verantwortlichen ohne Verzug melden.
- **Empfehlung:** Es muss ein Prozess eingeführt werden, um die Datensicherheitsverletzungen zu dokumentieren, zu bewerten und in den vorgesehenen Fällen zu melden.

IT & LAW | CONSULTING GMBH

Agenda

- Einführung
- Anwendungsbereich der DSGVO
- Auswirkungen der DSGVO auf die Organisation
- Neue Prozesse
- **Strafbestimmungen**
- Zusammenfassung

IT & LAW CONSULTING GMBH

Sanktionierung nach DSGVO

- Im Falle einer Nicht-Befolgung der DSGVO hat die Aufsichtsbehörde mehrere Rechte, z.B.:
  - Das Recht **Warnungen** auszusprechen;
  - Den Verantwortlichen oder Auftragsverarbeiter u.a. anzuweisen:
    - den Anträgen der betroffenen Person zu entsprechen;
    - Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen;
    - die betroffenen Personen bei einer Datenschutzverletzung zu benachrichtigen;
    - eine Beschränkung der Verarbeitung.
- Zusätzlich oder an Stelle dieser Massnahmen hat die Aufsichtsbehörde das Recht, **Geldbussen** gemäss Art. 83 DSGVO zu verhängen.
- Bei Verstössen gegen die DSGVO sind **Sanktionen** vorgesehen: Geldbussen bis zu 10 Mio. € resp. 20 Mio. € oder im Falle eines Unternehmens bis zu 2% resp. 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, **welcher der Beträge höher** ist.

IT & LAW CONSULTING GMBH

Agenda

- Einführung
- Anwendungsbereich der DSGVO
- Auswirkungen der DSGVO auf die Organisation
- Neue Prozesse
- Strafbestimmungen
- **Zusammenfassung**

IT & LAW CONSULTING GMBH

Zusammenfassung

- Unternehmen, die ihre Geschäftstätigkeit auf die EU oder den EWR ausrichten, sollten dringend prüfen, ob sie unter die DSGVO fallen.
- Die DSGVO ist in der gesamten EU und im EWR-Raum direkt anwendbares Recht. Dennoch gibt es in jedem EU-Staat und im EWR-Raum noch eigene Datenschutzgesetze (Umsetzung der sog. Öffnungsklauseln).
- Die DSGVO bringt für Unternehmen neue Pflichten.
- Die Einhaltung der DSGVO muss bewiesen werden.

Nützliche Links

- Bayrisches Landesamt für Datenschutzaufsicht; Kurzpapiere der Konferenz der Datenschutzbehörden zur DSGVO

  https://www.lda.bayern.de/de/datenschutz_eu.html
- Gesellschaft für Datenschutz und Datensicherheit; Praxishilfen

  https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- Verein Privacy Officers Österreich; Checkliste zur Umsetzung der DSGVO

  https://www.privacyofficers.at/privacyofficers-at-veroeffentlicht-aktualisierte-version-2-0-der-checkliste-zur-umsetzung-der-dsgvo/
- Herausgeber: CNIL, Commission Nationale de l'Informatique et des Libertés

  Tool für die Durchführung einer Datenschutz-Folgenabschätzung (Open Source) in englischer und französischer Sprache

  https://www.cnil.fr/en/tag/Privacy+Impact+Assessment+(PIA)

IT & LAW CONSULTING GMBH

Vielen Dank für Ihre Aufmerksamkeit

mag. iur. Maria Winkler
IT & Law Consulting GmbH
Sternenstrasse 18
8002 Zürich
maria.winkler@itandlaw.ch