Factsheet: Europäische Datenschutzgrundverordnung (DSGVO/GDPR)

1. Name der Richtlinie

Verordnung (EU) Nr. 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG («Datenschutz-Grundverordnung»), ABL. EU vom 4. Mai 2016, Nr. L 119, S. 1.

2. Ausgangslage

Per 25. Mai 2018 tritt die **D**aten**s**chutz**g**rund**v**er**o**rdnung (DSGVO/GDPR) in Kraft. Obwohl es sich um eine Verordnung der EU handelt, können auch schweizerische Unternehmen und Organisationen von dieser Verordnung betroffen sein. Gegenüber den geltenden Datenschutzbestimmungen in der Schweiz erweitert die Verordnung insbesondere den Pflichtenkatalog und verschärft die Sanktionen bei Verfehlungen. Zusätzlich hat die Verordnung auch Einfluss auf die Revision des Schweizerischen Datenschutzgesetzes (DSG). Eine Vielzahl der Bestimmungen werden wohl in das sich in Revision befindende Gesetz einliessen (müssen), damit die Schweiz auch künftig von der EU als Land mit ebenbürtigem Schutz anerkannt wird. Auch wenn ein Unternehmen also nicht in den Anwendungsbereich der Datenschutzgrundverordnung fällt, können mit Anpassungen an die DSGVO wahrscheinliche innerstaatliche Auswirkungen und Entwicklungen antizipiert werden.

3. Anwendungsbereich

(Auf die in der DSGVO gemachte Unterscheidung zwischen «Verantwortlicher» und «Auftragsverarbeiter» wird nicht näher eingegangen wie auch allfällige Unterschiede bezüglich deren Pflichten. In der Folge wird der Einfachheit halber nur von «Daten-Verarbeiter» gesprochen. Es ist im Einzelfall abzuklären, ob sich nicht allenfalls die Anwendung der DSGVO aufgrund einer Tätigkeit als Auftragsverarbeiter ergibt.)

Was muss man tun, um unter die Verordnung zu fallen (sachlicher Anwendungsbereich)?
Personenbezogene Daten ganz oder teilweise automatisiert verarbeiten oder **nichtautomatisiert verarbeiten**, aber in einem **Dateisystem speichern** bzw. **zur Speicherung vorsehen**.

➔ Definition gemäss DSGVO:
*«**alle Informationen**, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie Namen, zu einer Kennnummer, zu Standorten, 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.»*

Für wen gilt diese Verordnung (räumlicher Anwendungsbereich)?
Werden personenbezogene Daten verarbeitet, ist die Anwendung der DSGVO davon **abhängig, wo die Verarbeitung stattfindet** (Territorialitätsprinzip) oder wo sich der **potenzielle Kunde aufhält** (Marktortprinzip) bzw. der **Aufenthalt einer Person ist, deren Verhalten beobachtet** wird (Profiling), d.h. folgende Kriterien sind massgebend:

1. Möglichkeit: Filiale, Zweigstelle oder Tochtergesellschaft **in der EU**;
2. Möglichkeit: Schweizer Unternehmen oder Organisation bearbeitet personenbezogene Daten **im Auftrag eines europäischen Unternehmens**;
3. Möglichkeit: **keine Niederlassung/Filiale in der EU**, aber **personenbezogene Daten von Personen, die sich in der EU befinden** (unklar, ob bspw. nur Personen mit Domizil in der EU oder auch Touristen erfasst werden etc.), werden verarbeitet, wobei die Datenverarbeitung zum Zweck erfolgt:
   (1) der **betroffenen Person Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob eine Zahlung geleistet wird oder;
   (2) das **Verhalten der betroffenen Person zu beobachten** für beispielsweise verhaltensbasierte Werbung (mittels Analyse von Kundendaten, Auswertung von Daten von Website-Besucher durch Tracking oder Cookies etc.).

- ➔ Betrachtung jeweils im Einzelfall, ob der Daten-Verarbeiter beabsichtigte, Waren und Dienstleistungen an Personen im EU-Raum anzubieten oder das Verhalten von Personen im EU-Raum zu beobachten. Beispielsweise können Angebot in englischer Sprache unter Angabe von EU-Preisen oder Referenzen von EU-Kunden als Indizien für ein Angebot an EU-Kunden gesehen werden. Die blosse Zugänglichkeit zu einer Website, einer E-Mail-Adresse oder anderer Kontaktdaten wie auch der Gebrauch einer im Drittland (also die Schweiz) üblichen Sprache sind für sich alleine noch keine ausreichenden Anhaltspunkte.
- ➔ Noch keine Praxis zur konkreten Anwendung der Bestimmung, womit zahlreiche Interpretationsmöglichkeiten mit entsprechend unterschiedlichen Folgen denkbar sind.
- ➔ Nicht erfasst: Daten von Personen aus der Schweiz in der Schweiz bearbeiten.
- ➔ Wohl nicht erfasst: Daten von EU-Kunden bearbeiten, ihnen aber die Waren und Dienstleistungen nur in der Schweiz anbieten.

4. Grundsätze der Bearbeitung

Jede Bearbeitung von Personendaten ist **verboten**, ausser sie wird durch einen der folgenden, **gesetzlich vorgesehenen Gründe erlaubt**:

1. Einwilligung
2. Erforderlich für die Vertragserfüllung
3. Erforderlich für die Erfüllung einer rechtlichen Verpflichtung
4. Schutz lebenswichtiger Interessen
5. Wahrnehmung einer Aufgabe im öffentlichen Interesse
6. Wahrung der berechtigten Interessen

Zur **Einwilligung**:
Eine Person muss in eine Datenverarbeitung **freiwillig** und für **konkrete Fälle** einwilligen. Dies nachdem sie über den **Zweck der Datenverarbeitung informiert** worden ist. Ein schriftliches Ersuchen um Einwilligung (Einwilligungserklärung) ist in **verständlicher** und **leicht zugänglicher Form** an die betroffene Person zu richten (auch bezüglich der Sprache). Zudem muss die Person **darauf hingewiesen** werden, dass sie ihre **Einwilligung jederzeit widerrufen** kann, wobei der Widerruf der Einwilligung **so einfach wie deren Erteilung** sein muss. Der **Daten-Verarbeiter** ist bezüglich der erfolgten Einwilligung **nachweispflichtig** (auch für Einwilligungen, die bereits vor dem 25. Mai 2018 erfolgten).
Zudem ist es nicht zulässig, die Erbringung von Dienstleistungen von der Einwilligung zur Bearbeitung für solche Daten abhängig zu machen, die **zur Vertragserfüllung nicht erforderlich** sind.

5. Pflichten Daten-Verarbeiter bzw. Rechte der betroffenen Person

- Auskunftsrecht und Informationsrecht bei der Erhebung von personenbezogenen Daten sowie Recht, nicht einer ausschliesslich auf automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden (Art. 13–15 DSGVO)
- Recht auf Löschung der Daten („Vergessenwerden"; Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSG)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)
- Privacy by Design und by Default (Art. 25 DSGVO)
- Dokumentationspflicht und Führung eines Verarbeitungsverzeichnisses (Art. 30 DSGVO)
- Sicherheit der Bearbeitungsvorgänge (Art. 32 DSGVO)
- Data Breach Notifications (Benachrichtigung über Datenschutzverletzung; Art. 33 f. DSGVO)
- Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

6. Datenschutzbeauftragter und Vertreter in der Europäischen Union

Datenschutzbeauftragter (Art. 37 ff. DSGVO):

- Private Unternehmen (Verantwortliche und Auftragsverarbeiter) müssen einen Datenschutzbeauftragten benennen, wenn ihre Kerntätigkeit:

(1) eine umfangreiche regelmässige und systematische Überwachung von Betroffenen erforderlich macht;
(2) 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.
- Ein solcher (Unternehmens-) Datenschutzbeauftragter kann intern im Unternehmen oder extern angesiedelt sein.

Vertreter in der EU (Art. 27 DSGVO):

- Verfügt der Verantwortliche über keine Niederlassung in der EU, muss ein Vertreter mit Niederlassung in einem der von der Datenverarbeitung betroffenen EU-Land schriftlich benannt werden.
- Vertreter soll als Kontaktstelle zu der Aufsichtsbehörde und von der Datenverarbeitung betroffenen Personen fungieren -> Der Unternehmensvertreter gilt als Anlaufstelle für die EU-Aufsichtsbehörden und bietet eine faktische Zugriffsmöglichkeit.
- Ausnahme von der Benennungspflicht, falls Datenverarbeitung nur gelegentlich erfolgt, keine umfangreiche Verarbeitung besonderen Daten oder keine Verarbeitung personenbezogener Daten über Straftaten oder Verurteilungen einschliesst, wobei Art, Umstände, Umfang und Zweck der Verarbeitung wohl nicht zu einem Risiko für die Rechte und Pflichten natürlicher Personen führen.

7. Sanktionen (Art. 83 f. DSGVO)

Rechtsverletzungen können strenger als bisher bestraft werden, indem die Höhe der Bussen bis zu 20 Millionen Euro oder 4% des weltweiten Gesamtumsatzes betragen wird. Zusätzlich können die Aufsichtsbehörden weitere Massnahmen gegen fehlbare Daten-Verarbeiter vorsehen, beispielsweise eine Gewinnabschöpfung oder Anordnungen zur Beendigung des sanktionierten Verstosses. Zusätzlich zu diesen Sanktionen drohen den Verantwortlichen oder deren Auftragsverarbeitern künftig Schadenersatzforderungen für materielle und neu auch für immaterielle Schäden (Art. 82 DSGVO).

8. Empfehlungen

Ernsthafte Anstrengungen zur Umsetzung der Anforderungen unternehmen und dokumentieren.

Abschluss schriftlicher Auftragsvereinbarungen bezüglich Bestimmungen Datenschutz mit Dienstleistern.

Verträge betreffend Datenschutz bei der Übermittlung von Daten ausserhalb Europas.

Erfassung und Dokumentation bestehender Datenverarbeitungen -> Analyse, ob datenschutzrechtliche Anforderungen eingehalten werden -> Gap-Analyse, Definition Massnahmen zur Umsetzung.

9. Links

<http://dsat.ch/>
<http://datenrecht.ch/>
<https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/rechtliche-grundlagen/Datenschutz%20-%20International/DSGVO.html>
<http://www.netzwoche.ch/eu-dsgvo>

(bei Verwendung allfällige Lizenzbestimmungen beachten und Quellenangaben respektieren)

Im Detail: Pflichten Daten-Verarbeiter bzw. Rechte der betroffenen Person

Auskunftsrecht und **Informationsrecht** bei der Erhebung von personenbezogenen Daten sowie **Recht, nicht einer ausschliesslich auf automatisierten Verarbeitung beruhenden Entscheidung unterworfen** zu werden (Art. 13–15 DSGVO):

- aktive Informationspflicht, auch bei nicht sensiblen Personendaten oder wenn Daten nicht bei einer Person selbst erhoben wurden.
- Transparenz (ebenso Recht auf Mitteilung gem. Art. 19 DSGVO).
- Information über automatische Einzelfallentscheidungen und über Profiling.
- Auskunft, ob Daten von einer Person erhoben wurden oder nicht.
- Kopie von erhobenen Daten auf Verlangen herausgeben.

Recht auf Löschung der Daten („Vergessenwerden"; Art. 17 DSGVO):

- Betroffener erhält neu umfassenden Löschungsanspruch für seine personenbezogenen Daten, sofern diese nicht mehr notwendig sind.
- Daten müssen so schnell wie möglich gelöscht werden können.
- Falls Datenübermittlung an einen Dritten erfolgte, muss der Daten-Verarbeiter angemessene Massnahmen treffen, um jene Stellen zu informieren, dass Löschung (Pseudoanonymisierung) verlangt wurde.

Recht auf Einschränkung der Verarbeitung (Art. 18 DSG):

- Verantwortlicher darf nicht mehr jede Bearbeitung vornehmen, z.B. nur noch Aufbewahrung.

Recht auf Datenübertragbarkeit (Art. 20 DSGVO):

- Anbieter elektronischer Dienstleistungen müssen eine reibungslose Daten Portabilität gewährleisten, um einen leichten Wechsel des Diensteanbieters zu ermöglichen. Ein solcher Wechsel muss vom Anbieter direkt angeboten werden und – soweit technisch machbar – ohne Umweg mittels Down- und Upload der entsprechenden personenbezogenen Daten umsetzbar sein.

Widerspruchsrecht (Art. 21 DSGVO):

- Betroffene dürfen trotz rechtmässiger Verarbeitung, welche sich aus öffentlichem oder berechtigtem Interesse ergibt, aufgrund ihrer besonderen Situation Widerspruch gegen eine sie betreffende Datenverarbeitung einlegen.

Privacy by Design und by Default (Art. 25 DSGVO):

- Privacy by Design: Die Daten-Verarbeiter 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).

  ➔ Umsetzung des Datenschutzes wird durch IT-Hard- und Softwaresysteme unter Anwendung verschiedener Prinzipien (Minimize, Hide, Separate, Aggregate, Inform, Control, Enforce, Demonstrate etc.) datenschutzfreundlich gestaltet. Der Nutzer solcher Systeme kann seinen Willen mit datenschutzfreundlichen Voreinstellungen, wie beispielsweise stets erforderlichem Opting-In, bewusster äussern (vs. bisheriger Regelfall des Opting-Out).

Dokumentationspflicht und Führung eines Verarbeitungsverzeichnisses (Art. 30 DSGVO):

- Daten-Verarbeiter führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen.
- Wesentliche Angaben über die Verarbeitung müssen gemacht werden wie Zweck der Verarbeitung, Kategorie der Daten, Kategorie der Betroffenen und der Empfänger.
- Verzeichnis ist nicht öffentlich zugänglich.
- Daten-Verarbeiter müssen die Einhaltung des Gesetzes jederzeit nachweisen können. Fehler- oder Lückenhaftigkeit gilt als Rechtsverletzung und kann sanktioniert werden.
  - ➔ Hinweis: Unternehmen mit weniger als 250 Beschäftigten sind wiederum mit einigen Gegenausnahmen von dieser Pflicht ausgenommen.

Sicherheit der Bearbeitungsvorgänge (Art. 32 DSGVO):

- Angemessene organisatorische und technische Massnahmen unter Beachtung von: Stand der Technik, Implementierungskosten, Art und Umfang wie auch Umstände und Zweck der Bearbeitung, Risiken etc.
- Spezielle Erwähnung von Verschlüsselung und Pseudoanonymisierung.

Data Breach Notifications (Benachrichtigung über Datenschutzverletzung; Art. 33 f. DSGVO):

- Verstösse gegen Massnahmen zur Datensicherheit müssen verzeichnet und der Datenschutzbehörde gemeldet werden (innerhalb 72 Stunden -> Prozess für Erfassung und Meldung muss vorgesehen sein).
- Bei voraussichtlich hohem Risiko von Auswirkungen für die persönlichen Freiheiten und Rechte der Betroffenen müssen diese zusätzlich ebenfalls informiert werden.

Datenschutz-Folgenabschätzung (Art. 35 DSGVO):

- Dient Risikoeinschätzung und -verminderung.
- Falls Datenverarbeitung ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen darstellen könnte (z.B. weitreichende Überwachung von öffentlichen Bereichen), muss eine Datenschutz-Folgenabschätzung durchgeführt werden.
- Werden im Rahmen dieser Analyse spezifische Risiken erkannt, trifft den Verantwortlichen diesbezüglich eine Informationspflicht gegenüber der Aufsichtsbehörde resp. falls vorhanden gegenüber dem Datenschutzbeauftragten.
- Zwingend beim Profiling (häufig im Rahmen Onlinehandel).