Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Merkblatt

Europäische Datenschutz-Grundverordnung (DSGVO) – Merkblatt für den Umgang durch Gewerbebetriebe

1. Ausgangslage

Am 25. Mai 2018 tritt die neue Europäische Datenschutz-Grundverordnung (DSGVO) in Kraft. Sie löst die bisherige Richtlinie vom 24. Oktober 1995 ab. Mit der DSGVO soll in der Europäischen Union bzw. im Europäischen Wirtschaftraums (EWR) ein höheres und einheitliches Datenschutzniveau erreicht werden, das auch der Digitalisierung von Wirtschaft und Gesellschaft gerecht wird und damit das Vertrauen in den digitalen Binnenmarkt stärkt. Als Verordnung wird das neue Regelwerk innerhalb der EU-Staaten direkt zur Anwendung gelangen. Gleichwohl werden die einzelnen Mitgliedstaaten zusätzlich Vollzugsgesetze erlassen.

Die DSGVO wird auch für eine Vielzahl von Schweizer Unternehmen direkte Auswirkungen haben. Dies gilt unabhängig von der Tatsache, wie das revidierte Datenschutzgesetz (DSG), das aktuell im Eidgenössischen Parlament beraten wird, ausgestaltet sein wird (Inkrafttreten frühestens 2019). Bekanntlich will aber auch das DSG das europäische Datenschutzniveau soweit als nötig übernehmen, damit die EU unser Land weiterhin als Drittstaat mit angemessenem Datenschutzniveau anerkennt und damit die grenzüberschreitende Datenübermittlung auch künftig (einfach) möglich bleibt. In diesem Sinn werden auch Schweizer Unternehmen ohne «Europabezug» über kurz oder lang mit «europäischen» Datenschutzstandards konfrontiert sein.

Obschon das DSGVO auf den Grundsätzen der bisherigen Richtlinie (Rechtmässigkeit, Treu und Glauben, Transparenz, Zweckbindung, Richtigkeit etc.) aufbaut, werden die Rechte bzw. Pflichten der betroffenen Personen und Unternehmen doch erheblich ausgebaut. Während die sachliche Geltung[1] unverändert bleibt, wird der räumliche Anwendungsbereich gegenüber der Richtlinie erweitert und betrifft bei gegebenen Voraussetzungen auch die Datenbearbeitung ausserhalb der EU (Extraterritorialität).

2. Welche Schweizer Unternehmen sind betroffen?

In Einklang mit der bereits bestehenden Rechtsprechung des Europäischen Gerichtshofs zu Suchmaschinen (Google) erweitert die DSGVO den räumlichen Anwendungsbereich gemäss dem Kriterium des Zielmarktes (sog. Marktortprinzip), was im Ergebnis zu einer extraterritorialen Anwendung führen kann.

Damit ist das europäische Datenschutzrecht für Schweizer Unternehmen in folgenden Konstellationen anwendbar (vgl. Artikel 3 DSGVO):

- **Kriterium der Niederlassung:** Die Datenverarbeitung erfolgt durch ein Unternehmen (oder einen beauftragten Dritten) im Rahmen der Tätigkeit einer Niederlassung innerhalb der EU, unabhängig davon, ob die Verarbeitung tatsächlich in der EU stattfindet.

  Beispiele:

  - Schweizer Unternehmen hat Tochtergesellschaft in der EU. Sobald die Muttergesellschaft Zugriff auf die Personendaten hat, gilt die DSGVO auch für sie.

[1] Die Verordnung gilt gemäss Artikel 2 für jede Art der ganz oder teilweise automatisierten Verarbeitung (Erheben, Erfassen, Ordnen, Speichern, Verändern, Übermitteln etc.) personenbezogener Daten (identifizierter oder identifizierbarer natürlicher Personen) sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert werden (sollen). Ausgenommen sind namentlich persönliche und familiäre Tätigkeiten.

- Schweizer Unternehmen mit Filiale in der EU bearbeitet Personendaten in der zentralen IT-Organisation in der Schweiz.

- **Kriterium des Zielmarktes:** Die Datenverarbeitung durch ein Unternehmen (oder einen beauftragten Dritten) ohne Niederlassung in der EU bezieht sich auf Personen, die sich in der EU befinden und sofern:

  a) diesen Personen in der EU Waren oder Dienstleistungen entgeltlich oder unentgeltlich angeboten werden oder

  b) das Verhalten dieser Personen in der EU beobachtet wird.

  Beispiele:

  - Schweizer Online Shop bearbeitet Personendaten von Kunden in der EU.
  - Hotel in der Schweiz bietet über Website Buchungssystem auch Gästen in der EU an.

Nicht unter die DSGVO fallen also Schweizer Unternehmen, welche weder über eine Niederlassung in der EU verfügen, noch Waren oder Dienstleistungen an Personen mit Niederlassung in der EU anbieten bzw. deren Verhalten auch nicht beobachten.

Die blosse Zugänglichkeit einer Webseite eines Schweizer Unternehmens ist kein Indiz für die Absicht des Unternehmens, in der EU seine Dienstleistungen und Waren anzubieten. Werden hingegen z.B. Angebote in Euro gemacht oder richtet sich das Angebot offensichtlich an Personen in der EU, untersteht das Unternehmen der DSGVO.

Damit eine Schweizer Firma abschätzen kann, ob sie vom Anwendungsbereich der DSGVO betroffen ist, kann namentlich die Beantwortung folgender Fragen aufschlussreich sein:

- Verfügt das Unternehmen über eine Niederlassung oder eine Tochtergesellschaft innerhalb der EU?
- Bearbeitet das Unternehmen Daten von Personen aus der EU (Kundendaten aller Art, auch Daten, die von Besuchern der Website oder einer App verwendet werden)?
- Bietet das Unternehmen Personen in der EU Dienstleistungen oder Waren an?
- Betreibt das Unternehmen eine Plattform für online Bestellungen für Personen in der EU?
- Bearbeitet das eigene Unternehmen Daten für ein Unternehmen der EU?

Wer eine oder mehrere Fragen mit Ja beantwortet, fällt mit grosser Wahrscheinlichkeit unter den Geltungsbereich der DSGVO.

3. Welche Regeln haben betroffene Unternehmen zu berücksichtigen?

Schweizer Unternehmen, welche unter die DSGVO fallen, haben namentlich folgende Regeln zu berücksichtigen:

Als **Grundsätze der Datenverarbeitung** werden in Artikel 5 definiert:

- **Rechtmässigkeit:** Es liegt eine Einwilligung der betroffenen Person oder eine sonstige zulässige Rechtsgrundlage vor.
- **Treu und Glauben:** Die Datenverarbeitung erfolgt auf redliche und vertrauenswürdige Weise.
- **Transparenz:** Die Datenverarbeitung ist für die betroffene Person umfassend erkennbar.
- **Zweckbindung:** Die Datenverarbeitung erfolgt einzig zu einem eindeutig festgelegten und legitimen Zweck.

- **Datenminimierung:** Personenbezogene Daten müssen dem Zweck angemessen auf das notwendige Mass beschränkt werden.
- **Richtigkeit:** Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein.
- **Speicherbegrenzung:** Identifizierbare Personendaten werden nur solange gespeichert, wie es der Zweck erfordert.
- **Integrität und Vertraulichkeit:** Bei der Verarbeitung von Personendaten ist eine angemessene Sicherheit zu gewährleisten.
- **Rechenschaftspflicht**: Unternehmen sind für die Einhaltung dieser Grundsätze und deren Nachweis verantwortlich.

Diese Grundsätze werden in zahlreichen Artikeln und zughörigen Erläuterungen konkretisiert.

Zunächst gilt es das Prinzip der **Rechtmässigkeit** zu beachten: Eine Datenverarbeitung gilt gemäss Artikel 6 ff. insbesondere dann als rechtmässig, wenn

a) eine ausdrückliche Einwilligung der betroffenen Person vorliegt,

b) sie für den Abschluss oder die Erfüllung eines Vertrages erforderlich ist,

c) sie für die Erfüllung einer gesetzlichen Pflicht erforderlich ist oder

d) sie zur Wahrung berechtigter Interessen dient und die Interessen der betroffenen Person nicht überwiegen (Interessenwahrung).

Eine Einwilligung muss eindeutig gegeben werden. Sie ist immer an einen bestimmten Zweck gebunden. Eine stillschweigende Zustimmung reicht nicht. Eine eindeutige Einwilligung wird z.B. durch Mitteilung oder das Setzen eines Häkchens gegeben. Zur Verarbeitung sensibler Daten (Religions- oder Parteizugehörigkeit, biometrische Daten) braucht es immer eine ausdrückliche Einwilligung. Die betroffene Person muss die Einwilligung jederzeit widerrufen können. Vor Abgabe der Einwilligung muss die Person über das Recht zum Widerruf der Einwilligung in Kenntnis gesetzt werden. Der Abschluss eines Vertrags darf nicht von der Verarbeitung weiterer Daten abhängig gemacht werden.

Bei Kindern (Artikel 8) und besonderen Kategorien personenbezogener Daten (Artikel 9-11) gelten besondere Vorschriften.

Im Weiteren gilt es namentlich folgende **Rechte und Pflichten** der Betroffenen zu berücksichtigen:

- **Informationspflicht:** Werden Daten erhoben, muss die betroffene Person über diesen Umstand umfassend informiert werden (vgl. Artikel 13 und 14).

- **Auskunftsrecht:** Die betroffene Person hat ein Recht auf ausführliche Auskunft ob bzw. welche Daten zu welchem Zweck erhoben werden, umfassend Informationen wie Speicherdauer, Herkunft der Daten, Widerspruchsrecht etc. (vgl. Artikel 15).

- **Recht auf Berichtigung, Löschung und Einschränkung der Bearbeitung:** Die betroffene Person hat das Recht, falsche Daten berichtigen zu lassen (vgl. Artikel 16), bei gegebenen Voraussetzungen löschen (vgl. Artikel 17) oder deren Verarbeitung beschränken zu lassen (vgl. Artikel 18).

- **Recht auf Datenübertragbarkeit:** Die betroffene Person kann verlangen, dass ihr der Verantwortliche die Daten, die sie ihm bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format überlässt und kann diese an einen Dritten übermitteln (vgl. Artikel 20).

- **Widerspruchsrecht:** Die betroffene Person kann gegen die Verarbeitung ihrer Daten Widerspruch einlegen (vgl. Artikel 21).

Weiter sind für Schweizer Unternehmen insbesondere die folgenden Vorschriften der DSGVO relevant:

- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:** Es müssen Massnahmen getroffen werden, die dem Grundsatz des Datenschutzes durch die Ausgestaltung der Technik (Data Protection by Design) und durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) gerecht werden (vgl. Artikel 25). Bereits ab dem Zeitpunkt der Planung einer Datenverarbeitung (via IT-System) soll das Risiko von Persönlichkeitsverletzungen verringert werden, z.B. über eine standardmässige Anonymisierung. Standardmässig sollen nur diejenigen Personendaten verarbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.

- **Verzeichnis der Verarbeitungstätigkeiten:** Unternehmen haben ein Verzeichnis von Datenverarbeitungstätigkeiten zu führen (Dokumentationspflicht, vgl. Artikel 30). Das Verzeichnis soll eine Übersicht über alle Prozesse und Verfahren geben, in welchen personenbezogene Daten verarbeitet werden. Die Pflicht gilt nicht für Unternehmen, die weniger als 250 Mitarbeitende beschäftigen, sofern die Datenverarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt.

- **Sicherheit der Verarbeitung:** Bei der Datenverarbeitung sind Anforderungen bzw. Massnahmen zum Schutz der Daten zu berücksichtigen wie Pseudonymisierung, Verschlüsselung etc. (vgl. Artikel 32).

- **Datenschutz-Folgeabschätzung:** Verursacht eine Form der Datenverarbeitung wahrscheinlich ein hohes Risiko, muss eine Datenschutz-Folgeabschätzung vorgenommen werden (vgl. Artikel 35 f.). Sie ist vor allem in folgenden Fällen erforderlich: Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die auf automatisierte Verarbeitung einschliesslich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.

- **Ernennung eines Datenschutzbeauftragten und eines Vertreters in der EU:** Umfasst die Kerntätigkeit eines Unternehmens regelmässige und systematische Überwachungen von Personen oder betrifft sie besondere Kategorien von Daten, ist ein Datenschutzbeauftragter zu benennen, der mit entsprechenden Aufgaben und Kompetenzen zu betrauen ist (vgl. Artikel 37-39). Für der DSGVO unterstehende Unternehmen ohne Niederlassung besteht die Pflicht, einen Vertreter in der EU zu bezeichnen. Die Pflicht entfällt, wenn die Verarbeitung nur gelegentlich erfolgt, keine besonderen Datenkategorien verarbeitet werden und die Verarbeitung nicht zu Risiken führt (vgl. Artikel 27).

- **Verhaltensregeln und Zertifizierung:** Verbände können Verhaltensregeln erarbeiten, die die Anwendung der Verordnung präzisieren (vgl. Artikel 40 f.). Ebenso können Zertifizierungen vorgenommen werden (vgl. Artikel 42 f.).

- **Meldepflicht bei Datenschutzverletzungen:** Verletzungen des Schutzes personenbezogener Daten müssen der zuständigen nationalen Aufsichtsbehörden innert 72 Stunden gemeldet werden. Es besteht keine Meldepflicht, wenn ein Risiko für Rechte und Freiheiten von natürlichen Personen unwahrscheinlich ist (vgl. Artikel 33). Im Falle eines hohen Risikos sind in der Regel auch die betroffenen Personen unverzüglich von der Verletzung zu informieren (vgl. Artikel 34).

4. Welches sind die Folgen bei Verstössen?

Die Verordnung sieht eine Reihe von Untersuchungsbefugnissen (Informationsanforderungen, Datenschutzüberprüfungen, Hausdurchsuchungen etc.) und Abhilfebefugnissen (Verwarnungen, förmliche Bekanntmachungen, vorübergehende oder dauerhafte Beschränkungen der Bearbeitung etc.) vor (vgl. Artikel 58).

Die zuständigen nationalen Aufsichtsbehörden können gegen Verstösse gegen die DSGVO auch Sanktionen in Form von Geldbussen verhängen, die wirksam, verhältnismässig und abschreckend sind (vgl. Artikel 83). Sie können je nach Art des Verstosses und nach den zu berücksichtigenden Umständen bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes betragen.

Die Verordnung regelt auch die Amtshilfe zwischen den EU-Staaten (vgl. Artikel 61) und ermöglicht die Amtshilfe zu Drittstaaten (vgl. Artikel 50). Umgekehrt soll die internationale Amtshilfe zu Drittstaaten auch in der laufenden Revision des DSG ausgebaut werden. Insgesamt ist mit einer Intensivierung der Zusammenarbeit zwischen der Schweiz und der EU im Bereich des Datenschutzes zu rechnen. Fraglich ist indes, ob Geldbussen europäischer Aufsichtsbehörden gegen Unternehmen in der Schweiz umsetzbar sein werden.

Zu beachten ist ferner, dass gegebenenfalls auch ein aus einem Gerichtsverfahren resultierende Schadenersatz zu bezahlen ist (vgl. Artikel 82). Ferner ist bei öffentlich werdenden/gemachten Datenschutzverletzungen auch mit Reputationsrisiken zu rechnen.

5. Was empfiehlt sich zu tun?

Fällt ein Schweizer Unternehmen unter die europäische DSGVO, empfiehlt sich namentlich die Klärung bzw. Regelung folgender Aspekte:

- Wer ist für den Datenschutz im Unternehmen zuständig?
- Sind die Mitarbeiter des Unternehmens in Sachen Datenschutz sensibilisiert/geschult?
- Welche Personendaten werden wie bearbeitet? Ist es notwendig, besonders schützenswerte Daten zu bearbeiten?
- Welches sind die Rechtsgrundlagen (Rechtmässigkeit) zur Bearbeitung der Personendaten?
- Ist die Datenverarbeitung aus betrieblicher Sicht überhaupt nötig oder können diese gelöscht werden?
- Werden die Bestimmungen in den Verträgen des Unternehmens, in den Allgemeinen Geschäftsbedingungen sowie in den Datenschutzerklärungen den datenschutzrechtlichen Vorgaben gerecht?
- Ist das Unternehmen genügend dokumentiert, um die Erfüllung der datenschutzrechtlichen Pflichten angemessen nachweisen zu können?

6. Wichtiger Hinweis und Disclaimer

Dieses Faktenblatt hat ausschliesslich informativen Zweck und ist weder eine vollständige Checkliste noch kann es eine Rechtsberatung ersetzen. Der Schweizerische Gewerbeverband sgv lehnt jede Haftung ab, die sich im Zusammenhang mit der Anwendung oder der Unterlassung einer Handlung durch dieses Faktenblatt ergeben kann. Zudem empfehlen wir, sich an die zuständige Branchenorganisation zu wenden, die weitere Hinweise vermitteln kann.

Stand: 16. März 2018

Dossierverantwortlicher

Dieter Kläy, Ressortleiter
Tel. 031 380 14 45, E-Mail d.klaey@sgv-usam.ch