SWITZERLAND GLOBAL ENTERPRISE

EU-DSGVO – Merkblatt

Hintergrund

Am 25. Mai 2018 ist die Europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft getreten. Obwohl es sich bei der EU-DSGVO um eine Europäische Verordnung handelt, ist diese unter gewissen Voraussetzungen auch auf Schweizer Unternehmungen anwendbar.

Das Schweizerische Datenschutzgesetzt (CH-DSG) befindet sich derzeit ebenfalls in Revision und wird dem Europäischen Recht angeglichen. Eine Inkraftsetzung des CH-DSG wird frühestens im Jahr 2019 erwartet.

Dieses Merkblatt gibt einen Überblick über die Anwendbarkeit der EU-DSGVO auf Schweizer Unternehmen sowie über den Handlungsbedarf. Das Merkblatt ist als Arbeitshilfe gedacht und erhebt keinen Anspruch auf Vollständigkeit. Eine individuelle Analyse der betroffenen Unternehmung ist in jedem Fall erforderlich.

Für wen gilt die EU-DSGVO?

Die EU-DSGVO betrifft **jeden Umgang mit Personendaten** (einschliesslich Beschaffung, Speicherung, Löschung, Anonymisierung, Weitergabe etc.; kurz "Verarbeitung") durch schweizerische Unternehmen, wenn das Unternehmen

- **in der EU eine Niederlassung unterhält**, etwa eine Zweigniederlassung, eine Agentur, eine lokale Repräsentanz oder eine Tochtergesellschaft, sofern letztere nicht unabhängig, sondern im Auftrag der Schweizer Mutter agiert, und im Zusammenhang mit der Niederlassung Personendaten verarbeitet (Beispiel: eine Niederlassung in Frankreich verkauft Produkte oder Leistungen für die Hauptniederlassung in der Schweiz und verwendet dafür Name und Adresse von Endkunden oder Kontaktpersonen des Käufers aus Frankreich);
- **in der EU keine Niederlassung unterhält**: wenn das Unternehmen Güter oder Dienstleistungen in die EU anbietet (Beispiel: ein Unternehmen in der Schweiz vertreibt über eine Website Waren oder Dienstleistungen aktiv nach Deutschland oder ein Software as a Service (SaaS)-Anbieter in der Schweiz hat Kunden in der EU) oder das Verhalten von Personen in der EU beobachtet (Beispiel: es werden auf der eigenen Website in der Schweiz Cookies verwendet, mittels denen man Rückschlüsse auf das Verhalten der Website-Besucher ziehen kann und diese Daten ausgewertet werden).

Welche datenschutzrechtlichen Prinzipien müssen gemäss EU-DSGVO beachtet werden?

Folgende datenschutzrechtlichen Prinzipien müssen bei jeder Datenverarbeitung beachtet und eingehalten werden:

- **Grundsatz der Rechtmässigkeit:**
  Personendaten dürfen nur rechtmässig und nach Treu und Glauben verarbeitet werden (u.a. Gesetz, Vertrag, Einwilligung, legitimes Interesse).

- **Grundsatz der Zweckbindung:**
  Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- **Grundsatz der Transparenz:**
  Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein. Der Verarbeiter muss aktiv über die Bearbeitung von Personendaten informieren. Die Betroffenen haben ein Auskunftsrecht.

- **Grundsatz der Datenrichtigkeit:**
  Wer Personendaten bearbeitet, hat sich laufend über deren sachliche Richtigkeit und Aktualität zu vergewissern.

- **Grundsatz der Datenminimierung und der Speicherbegrenzung:**
  Die Bearbeitung muss angemessen und auf das für den Bearbeitungszweck notwendige Mass beschränkt sein.
  Die Speicherdauer soll so definiert werden, dass Daten nur so lange aufbewahrt werden, wie dies für den Verarbeitungszweck notwendig ist (Implementierung von Archivierungs- und Löschungsprozessen).

- **Integrität und Vertraulichkeit:**
  Die personenbezogenen Daten müssen in einer Weise bearbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (einschliesslich Schutz mittels geeigneter technischer und organisatorischer Massnahmen vor unbefugter oder unrechtmässiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung).

- **Rechenschaftspflicht:**
  Der Datenverarbeiter ist verantwortlich dafür, dass die oben genannten Grundsätze eingehalten werden und muss dies entsprechend nachweisen können.

Welche organisatorischen und operationellen Massnahmen sind zu treffen?

Schweizerische Unternehmen, die der EU-DSGVO unterstehen, aber keine europäische Niederlassung haben, müssen in einem der betroffenen Staaten einen lokalen Vertreter bestimmen[1]. Unter bestimmten Voraussetzungen[2] muss zudem ein Datenschutzbeauftragter bestimmt werden. Unternehmen, die der EU-DSGVO unterstehen, müssen zahlreiche Anforderungen erfüllen. In erster Linie muss durch Richtlinien, Vorlagen und weitere Dokumentationen sichergestellt sein, dass die folgenden Anforderungen eingehalten werden (nicht abschliessend):

- Aktivitäten zur Umsetzung der Anforderungen müssen organisiert und dokumentiert werden (z.B. Datenschutz-Organisation, Erstellen von Datenschutz-Reglementen und Weisungen, Schulung von Mitarbeitenden);
- Unternehmen, die personenbezogene Daten verarbeiten, sind für die Einhaltung der Verarbeitungsgrundsätze verantwortlich (Rechenschaftspflicht) und müssen ein Verzeichnis von Verarbeitungstätigkeiten führen[3];
- betroffene Personen müssen über vorbestimmte Punkte informiert werden, bevor die Verarbeitung ihrer Daten aufgenommen wird (insbesondere Information mittels einer Datenschutzerklärung);
- die Speicherdauer von Personendaten ist im Voraus zu bestimmen und Daten sind zu löschen, wenn der Verarbeitungszweck weggefallen ist, die Aufbewahrungsfrist abgelaufen ist und unter Umständen und unter Vorbehalt von Aufbewahrungspflichten auch auf Begehren der betroffenen Person;
- im Falle einer Datenschutzverletzung muss der Verantwortliche ohne Verzögerung und nicht später als 72 Stunden nachdem ihm die Verletzung bekannt wurde, 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 ebenfalls informiert werden;
- vor riskanten Datenbearbeitungen ist eine Datenschutz-Folgenabschätzung durchzuführen;
- betroffene Personen haben verschiedene Rechte in Bezug auf ihre Personendaten (z.B. Recht auf Auskunft oder Löschung), denen in der Regel innerhalb eines Monats nachzukommen ist, was entsprechende interne Abläufe verlangt;
- mit Dienstleistern, die Personendaten verarbeiten, müssen schriftliche Auftragsvereinbarungen geschlossen werden;

[1] Ausnahmen zu dieser Bestimmung sind in Art. 27 Abs. 2 EU-DSGVO aufgelistet.
[2] Siehe dazu Art. 37 EU-DSGVO.
[3] Es gibt Ausnahmen zu dieser Bestimmung für Unternehmen mit weniger als 250 Mitarbeiter, Art. 30 Abs. 5 EU-DSGVO.

- vor der Übermittlung von personenbezogenen Daten in Länder ausserhalb Europas/EWR oder der Schweiz muss sichergestellt werden, dass das betroffene Land über ein angemessenes Schutzniveau verfügt. Falls dies nicht der Fall ist, müssen geeignete Massnahmen ergriffen werden (z.B. Abschluss von Datenschutzverträgen).

Welche Konsequenzen drohen bei Nichteinhaltung?

Bei einer Verletzung der EU-DSGVO drohen folgende Konsequenzen:

- Europäische Behörden können gegenüber dem fehlbaren Unternehmen bei einer Verletzung Bussen von bis zu 20 Millionen Euro oder – falls höher – 4 Prozent des weltweiten Jahresumsatzes verhängen.
- Verträge verlangen häufig die Einhaltung des anwendbaren Rechts im Allgemeinen oder des Datenschutzrechts im Besonderen. Eine Verletzung kann in solchen Fällen zu Vertragsstrafen, vorzeitiger Beendigung, Schadenersatzforderungen und dem Verlust von Rechten führen.
- In der heutigen Zeit können Verletzungen sehr schnell verbreitet werden, besonders bei Unternehmen, die über einen bekannten Namen verfügen, sensible Daten bearbeiten, bereits früher Bestimmungen verletzt haben oder die in exponierten Bereichen tätig sind. Entsprechend drohen Reputationsrisiken.

EU-DSGVO – Merkblatt 2: Massnahmen von S-GE – neue Bestimmungen

Umgang mit Daten aus Visitenkarten:

Handhabung Abgabe Visitenkarten:

- bei Abgabe in Sammelbox (auf Messe/Event in EU)
- bei Abgabe direkt an die Firma (in die Hand von Person)

Hinweis zur Handhabung von Daten aus Visitenkarten:

Bei Daten aus Visitenkarten handelt es sich um personenbezogene Daten. Diese müssen rechtmässig verarbeitet werden. Eine Verarbeitung ist insbesondere dann rechtmässig, wenn Sie auf Gesetz, Einwilligung oder auf einem Rechtfertigungsgrund (wie beispielsweise das legitime Interesse des Datenverarbeiters) beruht.

Im Zusammenhang mit der Verarbeitung von personenbezogenen Daten aus Visitenkarten hat sich einerseits noch keine gefestigte Praxis entwickelt, andererseits kommt es immer auf die Umstände des Einzelfalls an.

Grundsätzlich kann aber in den meisten Fällen davon ausgegangen werden, dass das Unternehmen (Empfänger der Visitenkarten auf Messen) ein legitimes Interesse an der Datenverarbeitung geltend machen kann, und dass es zudem im Erwartungshorizont der Messeteilnehmer liegt, dass seine an der Messe verteilte Visitenkarte von den Unternehmen genutzt wird.

Eine Information (entweder bei Entgegennahme der Visitenkarte, z.B. auf dem Leadsheet oder bei der ersten Kontaktaufnahme mit der entsprechenden Person) reicht demnach grundsätzlich aus - eine explizite Einwilligung ist meist nicht notwendig. Die Information kann wie folgt lauten:

> *Hiermit informieren wir Sie, dass die [Name der Firma / Visitenkartenempfänger] aufgrund der erhaltenen Visitenkarte Ihre persönlichen Daten in ihrem System speichert. Die Daten beschränken sich auf Ihren Namen, Position, E-Mail-Adresse und Telefonnummer.*
>
> *Die Daten werden gespeichert, damit wir mit Ihnen in Kontakt bleiben und Sie über Aktualitäten informieren können. Bitte teilen Sie uns mit, falls Sie keine Informationen, Einladungen und Newsletter von uns erhalten möchten.*
>
> *Wir werden Ihre Daten nicht an Dritte weitergeben.*

Für eine weitergehende Verwendung (wie beispielsweise die Weitergabe der Daten an Dritte) müsste eine Einwilligung eingeholt werden. Die Einwilligung ist nur gültig, wenn sie auf umfassender Information, abgestimmt auf den konkreten Fall, basiert. Daher ist eine Überprüfung in jedem Einzelfall empfehlenswert.

Im Fall von einer Weitergabe der Daten an Dritte könnte die Einwilligung wie nachfolgend beispielhaft erläutert lauten. Die Einwilligung müsste bei Einverständnis vom Inhaber der Visitenkarte angekreuzt werden (entweder auf dem Leadsheet inkl. Unterschrift oder bei der ersten Kontaktaufnahme – in jedem Fall aber vor der Weitergabe an Dritte):

☐ *Ich bin damit einverstanden, dass die [Name der Firma / Visitenkartenempfänger] meine persönlichen Daten (Name, Position, E-Mail-Adresse, Adresse und Telefonnummer) zu Marketingzwecken in den Bereichen [bitte auflisten] an Dritte weitergibt.*

Sie können Ihr Einverständnis zu der obgenannten Erklärung jederzeit widerrufen und die Löschung Ihrer Personendaten verlangen. Bitte kontaktieren Sie uns hierzu unter [e-mail Adresse].

Welche Fragen muss sich ein KMU in der Schweiz stellen?

- **Braucht ein CH-KMU einen Datenschutzbeauftragen?**

  Gemäss Art. 37 EU-DSGVO muss ein Datenschutzbeauftragter ernannt werden, wenn

  a) die **Kerntätigkeit des Unternehmens** in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche **regelmässige und systematische Überwachung** von betroffenen Personen erforderlich machen, oder
  b) die **Kerntätigkeit des Unternehmens** in der **umfangreichen Verarbeitung besonderer Kategorien von Daten** (d.h. personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person**)** oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.

  Die Kriterien der Beurteilung, ob ein Datenschutzbeauftragter ernannt werden muss, sind nicht eindeutig und bedürfen einer Analyse der tatsächlichen Tätigkeiten eines KMU und der damit verbundenen Datenverarbeitungsaktivitäten.

- **Welche weiteren Anforderungen für ein CH-KMU müssen erfüllt werden, um nicht von den Sanktionen getroffen zu werden?**

  Diese Frage kann nicht allgemein beantwortet werden, da der Umfang der datenschutzrechtlichen Massnahmen von der individuellen Verarbeitung von personenbezogenen Daten abhängt. Es ist daher in jeder Unternehmung eine Einzelfallbetrachtung erforderlich.

  In jedem Fall sollten Sie sich folgende Überlegungen über die datenschutzrechtlichen Anforderungen machen:

  - Beachten Sie bei jeder Datenverarbeitung folgende datenschutzrechtlichen Grundsätze:
    - ✓ Grundsatz der Rechtmässigkeit und Treu und Glauben
    - ✓ Grundsatz der Zweckbindung
    - ✓ Grundsatz der Transparenz
    - ✓ Grundsatz der Datenrichtigkeit
    - ✓ Grundsatz der Datenminimierung und Speicherbegrenzung
    - ✓ Grundsatz der Integrität und Vertraulichkeit
    - ✓ Grundsatz der Rechenschaftspflicht

- Achten Sie auf eine gute Governance
  - ✓ Sie müssen Ihre internen Abläufe kennen und Ordnung in der Datenverarbeitung halten, so dass Sie jederzeit Ihren Auskunfts- und Informationspflichten nachkommen können
  - ✓ Arbeiten Sie eng mit Ihrer IT-Abteilung zusammen
  - ✓ Erteilen Sie Zugriffsberechtigungen und –beschränkungen
  - ✓ Schulen Sie Ihre Mitarbeitenden und erstellen Sie interne Weisungen
  - ✓ Definieren Sie Verantwortlichkeiten in Bezug auf Datenschutz

- Erstellen Sie eine Datenschutzerklärung
- Prüfen Sie, ob Sie einen Vertreter in der EU gemäss Art. 27 EU-DSGVO bestellen müssen
- Stellen Sie sicher, dass Sie im Falle einer datenschutzrechtlichen Verletzung die 72-Stunden-Frist für die Meldung an die Aufsichtsbehörde einhalten können
- Erstellen Sie ein Verzeichnis über Verarbeitungstätigkeiten gemäss Art. 30 EU-DSGVO
- Treffen Sie die notwendigen technischen und organisatorischen Massnahmen, die dafür ausgelegt sind, die Datenschutzgrundsätze einzuhalten («Privacy by design» / «Privacy by default»).
- Prüfen Sie, ob Sie zur Bestellung eines Datenschutzbeauftragten verpflichtet sind.

Für weiterführende Fragen finden Sie uns unter www.s-ge-com/de/exporthelp oder in direkter Anschrift auf exporthelp@s-ge.com oder telefonisch auf 0844 811 812.

Copyright © Switzerland Global Enterprise 2019