AGEBA TREUHAND AG
STEPHAN REVISIONS AG

FACHINFO

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO):

FÄLLT IHR UNTERNEHMEN IN DEN ANWENDUNGSBEREICH?

Befinden sich natürliche Personen, deren Daten Sie verarbeiten in der EU? Sobald dies der Fall ist, ist die EU Datenschutzgrundverordnung (EU-DSGVO) anzuwenden.

In der Praxis dürfte diese Regelung grundsätzlich nicht für kleine Geschäfte wie eine Bäckerei usw. gelten. Diese Läden bieten keine Güter oder Dienstleistungen für Personen in der EU an und verfolgen auch nicht deren Verhalten. Dagegen könnte diese für einen Entwickler einer App gelten, wenn dieser Dienstleistungen für in der EU-wohnhafte Personen anbietet. Jedes Unternehmen (unabhängig vom Standtort des Firmensitzes), welches am europäischen Markt agiert, muss sich daranhalten.

WELCHES SIND TYPISCHE DSGVO-FALLEN?

1. Akten landen im Papierkorb: Druck-Erzeugnisse mit personenbezogenen Daten landen im Papierkorb und sind vor unberechtigten Zugriffen nicht geschützt.

2. Private Geräte am Arbeitsplatz oder Nutzung von Firmengeräte für private Zwecke: mit USB-Sticks kann Schadensoftware von privaten Geräten auf einen geschäftlichen Server gelangen und so vertrauliche Daten in Gefahr bringen.

3. Nutzung des privaten E-Mail Accounts: Durch die Verwendung von privaten E-Mailadressen kommen oft unsichere Transfermethoden zum Einsatz.

4. Passworte werden weitergegeben

5. Hereinspaziert! Betriebsfremde Personen haben Zugang zu Büroräumlichkeiten.

6. Zu viel Auskunft am Telefon

7. Chaos am Arbeitsplatz: Vertrauliche Dokumente bleiben ungeschützt liegen.

8. DATENPANNEN VERSCHWEIGEN VIELE NEUE PFLICHTEN: WAS IST JETZT ZU TUN, BZW. WELCHE FRAGEN SOLLTE MAN SICH STELLEN?

Die DSGVO bringt viele neue Pflichten (siehe Erläuterung der sieben Pflichten weiter unten). Der Datenschutz ist ein weitläufiges Thema. Einerseits muss die betriebliche IT den aktuellen Anforderungen entsprechen und den Zugriff auf persönliche Daten verhindern. Andererseits müssen betriebliche Prozesse und die Verantwortung diesen Schutz gewährleisten. Welche Fragen sollte man als Unternehmer stellen?

Kommen bei E-Mails Verschlüsselungstools zum Einsatz? Nicht verschlüsselte E-Mails müssen generell als unsicher qualifiziert werden.

Genügt die Website aktuellen technischen Sicherheitsstandards/Verschlüsselungen?

- Kommen wir unseren Informationspflichten nach (z.B. Datenschutzerklärungen auf Website)?
- Haben wir die Einwilligung aller Personen, deren persönliche Daten wir verwenden (z.B. für einen Newsletter)?
- Genügen unsere bestehenden Verträge dem Datenschutz?
- Haben wir die nötigen organisatorischen und technische Schutzmassnahmen (einschl. IT) getroffen?
- Sind die internen Prozesse zur Sicherstellung der Rechte der Betroffenen klar? (Recht auf Information, Auskunft, Berichtigung, Löschung und Widerspruch)
- Wer ist unser Datenbeauftragter oder gar Vertreter in der EU?
- Haben wir ein Verfahren bei Verletzung des Datenschutzes?

SIEBEN PFLICHTEN NACH DSGVO

1. Informieren und Einwilligung betreffend der Datenverarbeitung

Die Einwilligung hat aktiv und ausdrücklich durch die betroffene Person zu erfolgen. Und es muss jederzeit möglich sein, sie zu widerrufen.

2. "Privacy by design" und "Privacy by default" gewährleisten

Schon bei der Planung der Datenverarbeitung muss das Unternehmen technische und organisatorische Massnahmen ergreifen, um die Einhaltung der DSGVO sicherzustellen und die Daten der betroffenen Personen zu schützen (Privacy by design). Darüber hinaus muss es über Voreinstellungen gewährleisten, dass standardmässig nur Daten erhoben werden, die für den jeweiligen Verwendungszweck erforderlich sind (Privacy by default).

3. Einen Vertreter in der EU ernennen

Die Pflicht, einen Vertreter in der EU zu benennen, entfällt, wenn die Datenverarbeitung nur gelegentlich erfolgt, keine besonderen Datenkategorien betrifft und nahezu kein Risiko mit sich bringt.

4. Ein Verzeichnis der Verarbeitungstätigkeiten erstellen

Das Unternehmen oder seine Zwischenhändler müssen eine Übersicht mit einer Reihe von Informationen zu den Methoden der Datenverarbeitung führen.

5. Verstösse gegen den Datenschutz an die Aufsichtsbehörde melden

Die Firma muss schnelle Mechanismen vorsehen, mit denen die betroffenen Personen und die zuständigen Aufsichtsbehörden im Falle einer Datenschutzverletzung benachrichtigt werden.

6. Eine Datenschutz-Folgenabschätzung durchführen

Eine Art der Datenverarbeitung, die ein hohes Risiko mit sich bringt, dass Rechte und Freiheiten verletzt werden könnten, muss einer Folgenabschätzung unterzogen werden.

7. Verstössen gegen die DSGVO Geldbussen zahlen

Die Geldbusse, die Unternehmen im Fall einer Datenschutzverletzung zahlen müssen, kann bis zu 4% des weltweiten Jahresumsatzes im vergangenen Geschäftsjahr betragen

BEI FRAGEN UND FÜR EINE UMFASSENDE BERATUNG WENDEN SIE SICH AN IHREN MANDATSLEITER ODER AN:

Herr Thomas Germann
Geschäftsführer, Partner,
Bereichsleiter Treuhand und Recht
lic. jur., Steuerexperte

Tel.: +41 61 467 96 62
thomas.germann@ageba.ch
www.ageba.ch

AGEBA TREUHAND AG

STEPHAN REVISIONS AG