FAQ - Datenschutz

Welches Ziel verfolgt der Datenschutz?

Der Datenschutz gibt betroffenen Personen das Recht, den Umgang mit ihren persönlichen Daten zu kontrollieren und allfällige Mängel zu beheben.

Welches sind die rechtlichen Grundlagen des Datenschutzes?

In der Schweiz gilt grundsätzlich das Eidgenössische Datenschutzgesetz (DSG).

https://www.admin.ch/opc/de/classified-compilation/19920153/index.html

Unter Umständen ist für Unternehmen in der Schweiz auch die Datenschutz-Grundverordnung (DSGVO) der EU zu beachten, welche am 25. Mai 2018 in Kraft getreten ist.

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679

Zu wissen ist, dass momentan ein Schweizer Pendant zur DSGVO der EU, ein neues Datenschutzgesetz, ausgearbeitet wird. Unternehmen, die sich schon auf die DSGVO eingestellt haben, dürften, wenn die Schweizer Version fertig ist, bei deren Umsetzung eine erhebliche Zeitersparnis haben.

Wann ist die DSGVO anwendbar?

Die DSGVO ist anwendbar, wenn ein Unternehmen seine Niederlassung in der Europäischen Union hat. In diesem Fall findet die Verordnung automatisch Anwendung und zwar unabhängig davon, ob die Datenbearbeitung in der EU stattfindet oder nicht.

Die DSGVO ist ebenfalls anwendbar, wenn sich die Niederlassung eines Unternehmens zwar ausserhalb der EU befindet (also z.B. in der Schweiz), die Datenbearbeitung aber Waren oder Dienstleistungen betrifft, die für Personen in der EU bestimmt sind.

Schliesslich ist die DSGVO anwendbar, wenn die Datenbearbeitung die Beobachtung des Verhaltens einer Person betrifft, soweit dieses Verhalten in der EU erfolgt. Diese Regelung bezieht sich vor allem auf die Beobachtung des Verhaltens von Internetnutzern.

Welches sind die wichtigsten Pflichten, welche die DSGVO enthält?

Schweizer Unternehmen, die von der DSGVO betroffen sind, müssen ab dem 25. Mai 2018 insbesondere folgende Pflichten erfüllen:

1. informieren und die Einwilligung der Person einholen, deren Daten verarbeitet werden;

   Wenn eine Datenverarbeitung aufgrund der Einwilligung der betroffenen Person erfolgt, muss diese Einwilligung freiwillig gegeben werden und auf einer ausführlichen, erkennbaren und bestimmten Information beruhen. Sie hat aktiv und ausdrücklich zu erfolgen. Nicht erforderlich ist eine bestimmte Form; sie kann auch mündlich gegeben werden. Wichtig ist, dass das Unternehmen die Einwilligung nachweisen kann. Und es muss jederzeit möglich sein, die Einwilligung zu widerrufen.

2. "Privacy by design" und "Privacy by default" garantieren;
   Bereits bei der Planung einer Datenverarbeitung muss ein Unternehmen technische und organisatorische Massnahmen ergreifen, um die Einhaltung der DSGVO sicherzustellen und die Daten der betroffenen Personen zu schützen (sog. Privacy by design). Darüber hinaus muss das Unternehmen gewährleisten, dass standardmässig nur Daten erhoben werden, die für den jeweiligen Verwendungszweck erforderlich sind (sog. Privacy by default).

3. einen Vertreter in der EU benennen;
   Unternehmen sind verpflichtet, einen Datenschutz-Vertreter in der EU zu bestimmen. Diese Pflicht entfällt, wenn die Datenverarbeitung nur gelegentlich erfolgt, keine besonderen Datenkategorien betrifft und nahezu kein Risiko mit sich bringt.

4. ein Verzeichnis der Verarbeitungstätigkeiten erstellen;
   Unternehmen müssen eine Übersicht mit einer Reihe von Informationen zu den Methoden der Datenverarbeitung führen.

5. Verletzungen des Datenschutzes an die Aufsichtsbehörde melden;
   Unternehmen müssen schnelle Mechanismen vorsehen, mit denen die betroffenen Personen und die zuständigen Aufsichtsbehörden im Falle einer Datenschutzverletzung benachrichtigt werden können.

6. eine Datenschutz-Folgenabschätzung durchführen;
   Eine Datenverarbeitung, die ein hohes Risiko mit sich bringt, dass Rechte und Freiheiten verletzt werden könnten, muss einer Folgenabschätzung unterzogen werden.

Welches sind die wichtigsten Grundsätze des Datenschutzrechts?

1. Rechtmässigkeit

Daten dürfen nur rechtmässig bearbeitet werden. Die wichtigsten Bedingungen für die Rechtmässigkeit sind die folgenden: Die Verarbeitung ist entweder für eine Vertragserfüllung notwendig, oder sie erfolgt aufgrund einer freiwilligen, informierten und unmissverständlichen Einwilligung.

2. Datenminimierung

Es sind nur so viele Daten wie notwendig zu bearbeiten. Die Datenbearbeitung "auf Vorrat" ist nicht zulässig.

3. Datensicherheit

Daten sind so zu sichern, dass diese vor Verlust, Zerstörung, Missbrauch, Zugriff durch Unberechtigte geschützt werden.

4. Erforderlichkeit / Zweckbindung

Es dürfen nur soweit Daten bearbeitet werden, als dies für den konkreten Zweck erforderlich ist. Die Daten dürfen nur für den angegebenen oder erkennbaren Zweck bearbeitet werden.

5. Richtigkeit

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit unrichtige Daten berichtigt oder vernichtet werden bzw. dass unvollständige Daten vervollständigt werden.

6. Transparenz

Die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein. Erfolgt eine Datenbeschaffung bei einem Dritten, ist sicherzustellen, dass die Datenbearbeitung für die betroffene Person erkennbar wird. Dies erfordert in aller Regel eine Information der betroffenen Person.

7. Zweckbindung

Jede Datenbearbeitung hat mit einem bestimmten Ziel oder Zweck zu erfolgen. Eine Datenbearbeitung ohne Zweck ist rechtswidrig, so etwa die Datenbeschaffung auf Vorrat. Der festgelegte Zweck der Datenbearbeitung ist verbindlich.

Welche Rechte haben die betroffenen Personen?

1. Recht auf Information

Werden personenbezogene Daten über eine betroffene Person bei dieser Person selbst erhoben, so muss der Verantwortliche ihr zum Zeitpunkt der Erhebung der Daten eine Reihe von Informationen liefern (insb. der Zweck für die Datenbearbeitung). Der Verantwortliche muss die betroffene Person aber auch dann informieren, wenn die Daten nicht bei dieser selbst erhoben wurden. Werden bspw. beim Besuch einer Homepage Daten aufgezeichnet, so sind die Internetbenutzer darüber zu informieren. Die hierfür erforderlichen Erklärungen können im Internet mit den gängigen Generatoren automatisch erstellt werden.

2. Auskunftsrecht

Eine betroffene Person hat das Recht, eine Bestätigung zu verlangen, dass personenbezogene Daten über sie bearbeitet werden bzw. dass keine Daten bearbeitet werden. Im Fall einer Bearbeitung hat sie das Recht, Zugang zu diesen Daten und zusätzlichen Informationen zu erhalten. Dieses Recht umfasst auch das Recht, eine Kopie der bearbeiteten Daten zu erhalten.

3. Recht auf Berichtigung

Eine betroffene Person hat das Recht, zu verlangen, dass unrichtige bzw. unvollständige Daten so rasch wie möglich berichtigt oder ergänzt werden.

4. Recht auf Löschung

Eine betroffene Person hat das Recht zu verlangen, dass sie betreffende Daten so schnell wie möglich gelöscht werden, wenn die Daten für den Zweck, für den sie erhoben worden sind, nicht mehr notwendig sind bzw. wenn die betroffene Person ihre Einwilligung wiederruft.

5. Recht auf Einschränkung der Bearbeitung

Eine betroffene Person hat in bestimmten Fällen das Recht, vom Verantwortlichen die Einschränkung der Bearbeitung ihrer Daten zu verlangen (bspw. wenn die Richtigkeit der Daten bestritten wird oder wenn die Daten für den ursprünglichen Zweck nicht mehr benötigt werden). Wird eine Einschränkung verlangt, so kann der Verantwortliche die Daten nur noch aufbewahren. Andere Bearbeitungen dieser Daten dürfen grundsätzlich nicht mehr erfolgen.

6. Recht auf Mitteilung

Einer betroffenen Person muss jede Berichtigung, Löschung oder Einschränkung der Datenbearbeitung mitgeteilt werden.

7. Recht auf Datenübertragbarkeit

Eine betroffene Person hat das Recht, die Daten, die sie einem Unternehmen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen zu übermitteln, beispielsweise um den Dienstleistungsanbieter zu wechseln. Dieses Recht kann jedoch nur ausgeübt werden, wenn die Datenbearbeitung auf der Einwilligung der betroffenen Person oder auf einem Vertrag beruht.

Welche Sanktionen können bei einem Verstoss gegen die DSGVO drohen?

Die DSGVO sieht eine ganze Reihe von abschreckenden Massnahmen vor, z. B. Mahnungen, Verwarnungen, förmliche Bekanntmachungen, vorübergehende oder dauerhafte Beschränkungen der Bearbeitung. Als letztes Mittel können Verantwortliche mit Geldbussen von bis zu 20 Millionen Euro oder 4 Prozent ihres weltweiten Jahresumsatzes belegt werden.