REBER

Die neue EU-Datenschutzverordnung ist in Kraft – Was bedeutet das für Unternehmen in der Schweiz?

Am 25. Mai 2018 ist nach zweijähriger Übergangsfrist die neue EU-Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Sie ist direkt anwendbar und muss nicht mehr ins nationale Recht der EU-Staaten umgesetzt werden.

Hauptziel der neuen Datenschutzgesetzgebung ist es, im Zusammenhang mit der Bearbeitung von Personendaten ein einheitliches und hohes Schutzniveau innerhalb der EU zu schaffen. Die DSGVO gilt bei Vorliegen bestimmter Voraussetzungen auch für Schweizer Unternehmen. Im Vergleich zum gegenwärtigen schweizerischen Bundesgesetz über den Datenschutz und die Datenschutzverordnung (nachfolgend «DSG») bringt die DSGVO einige Neuerungen mit sich. Unter Umständen kann es somit für Schweizer Unternehmen erforderlich sein, ihre internen Prozesse und Datenschutzbestimmungen im Lichte der neuen Gesetzgebung anzupassen. Für gewisse, indirekt anwendbare Bestimmungen der neuen DSGVO wird es am schweizerischen Gesetzgeber liegen, entsprechende gesetzliche Anpassungen zu machen. Das DSG wird derzeit überarbeitet.

Nachfolgend wird das Wichtigste in Bezug auf die neue DSGVO kurz zusammengefasst:

Die DSGVO umfasst nur die Verarbeitung *personenbezogener* Daten. Darunter werden alle Informationen verstanden, die sich auf eine identifizierte oder identifizierbare *natürliche* Person beziehen. So fällt beispielsweise das Abspeichern von Kundendaten in den Anwendungsbereich der DSGVO, sofern es sich dabei um die Daten natürlicher Personen handelt. Nicht in den Anwendungsbereich der DSGVO fallen die Daten von Firmenkunden.
Die DSGVO gilt zusammengefasst für folgende Schweizer Unternehmen, die personenbezogene Daten verarbeiten:

- Unternehmen, welche ihre Waren oder Dienstleistungen in der EU anbieten (sog. Marktortprinzip). Ob ein Anbieten im Sinne der DSGVO vorliegt, ist fallweise zu beurteilen. Entscheidend ist die Absicht des Unternehmens, Kunden aus dem EU-Raum zu gewinnen. Nicht relevant ist, ob die Leistung in der Schweiz oder in der EU erbracht wird;

- Unternehmen, welche das Verhalten von Personen in der EU beobachten, indem sie deren Internetaktivitäten nachvollziehen können (u.a. verhaltensbasierte Werbung, welche auf die individuellen Interessen einer natürlichen Person zugeschnitten ist);

- Unternehmen, welche personenbezogene Daten im Auftrag eines Dritten mit Niederlassung in der EU bearbeiten. Neu dürfen Unternehmen, welche der DSGVO unterliegen, nur noch Daten an Dritte weitergeben, die den Datenschutzstandard der EU einhalten. Demnach ist eine Zusammenarbeit zwischen Schweizer Unternehmen und EU-Unternehmen, welche die Bearbeitung personenbezogener Daten mitumfasst nur dann möglich, wenn das Schweizer Unternehmen den EU-Standard erfüllt.

Grundsätze und wichtigste Pflichten

Zunächst gibt es eine Reihe von Grundsätzen, welche es bei der Verarbeitung von personenbezogenen Daten stets zu beachten gilt. Im Wesentlichen verlangen diese, dass die Erhebung von personenbezogenen Daten

- rechtmässig ist, d.h. auf einer legitimen Grundlage beruht;
- transparent ist, d.h. für den Betroffenen nachvollziehbar ist;
- auf einem angegebenen Zweck beruht und eine Vertrauensbasis besteht;
- auf das erforderliche Minimum eingeschränkt wird;
- durch technische und organisatorische Massnahmen vor Datenverlust oder unbefugten Eingriffen geschützt wird.

Die wichtigsten Pflichten können wie folgt umschrieben werden:

- **Rechtfertigungsgrund:** Gemäss DSGVO braucht es für jede Datenbearbeitung einen Rechtfertigungsgrund. Die wichtigsten Rechtfertigungsgründe sind: Einwilligung der betroffenen Person, Ausführung eines Vertrags sowie berechtigtes Interesse. Eine Einwilligung der betroffenen Person wird etwa benötigt, wenn Daten über deren Gesundheit bearbeitet werden. Bei der Formulierung der Einwilligungserklärung ist darauf zu achten, dass der Zweck der Datenverarbeitung möglichst genau umschrieben wird. Pauschale Einwilligungen sind nicht mehr zulässig.

  Darüber hinaus haben Unternehmen der neuen DSGVO durch technische Massnahmen und durch Anpassung interner Abläufe Rechnung zu tragen. Es sollten nur jene Daten gesammelt werden, welche für die Erfüllung des Zwecks erforderlich sind.

- **Informationspflicht:** Es besteht gegenüber den natürlichen Personen eine Informationspflicht; betroffene Personen sind darüber zu informieren, welche Daten zu welchem Zweck bearbeitet werden und wie lange diese gespeichert werden (bspw. mittels Link zu einer Datenschutzerklärung). Ferner müssen die betroffenen Personen über ihre Rechte bzgl. Auskunft, Berichtigung, Löschung und Widerspruch sowie das Beschwerderecht bei einer Aufsichtsbehörde informiert werden. Diese Hinweise müssen verständlich, präzise und leicht zugänglich sein.

- **Herausgabe von Daten:** Die betroffene Person hat das Recht, die sie betreffenden Daten in einem gängigen, maschinenlesbaren Format anzufordern.

Empfehlungen und praktische Beispiele

Aufgrund der weitreichenden Kompetenzen der Aufsichtsbehörden mit einem Bussenrahmen von bis zu 20 Millionen Euro bzw. bis zu 4% des weltweit erzielten Jahresumsatzes sowie des potentiellen Reputationsschadens bei einer Verletzung von datenschutzrechtlichen Bestimmungen lohnt es sich auch für Unternehmen in der Schweiz zu prüfen, ob die DSGVO generell anwendbar ist und falls ja, welche Bestimmungen konkret zu beachten sind (z.B. falls ein Unternehmen seine Produkte und Dienstleistungen auch auf dem europäischen Markt anbietet). Falls dies der Fall ist, wäre festzustellen, welche personenbezogenen Daten, zu welchen Zwecken, wie und von wem erhoben und bearbeitet werden. Die Verarbeitungsprozesse und bestehende Datenschutzmassnahmen sollten dokumentiert werden. Sodann wäre festzustellen, wo Lücken bestehen und wie diese geschlossen werden können. Ferner ist anhand eines risikobasierten Ansatzes zu entscheiden, welche zusätzlichen Massnahmen umgesetzt werden sollten.

Es ist ganz generell zu empfehlen, innerhalb des Unternehmens das Bewusstsein für den

Datenschutz zu stärken (bspw. mittels Aufstellen von Verhaltensregeln oder Durchführen von Schulungen).

- **Beispiel Verkauf von Produkten oder Dienstleistungen über Online-Shop in die EU**
  In diesem Fall werden durch die Anfragen und Bestellvorgänge persönliche Daten erfasst (bspw. Kredit- und Zahlungsinformationen). Die von der Verarbeitung betroffenen Personen müssen deshalb informiert werden, wie und wozu die Daten verwendet werden.

  Hierzu könnte ein Link zu einer Datenschutzerklärung in das Bestellformular eingefügt werden. In der Datenschutzerklärung könnte folgender Text verwendet werden: «Sämtliche Personendaten, welche wir über das Kontakt- oder Bestellformular von Ihnen erhalten, bearbeiten wir ausschliesslich zum Zwecke der Vertragserfüllung».

  Ferner ist in der Datenschutzerklärung ein Kontakt (bspw. E-Mail-Adresse) anzugeben, damit die von der Datenverarbeitung betroffenen Personen ihre Rechte wahrnehmen können (z.B. das Recht auf Auskunft).

- **Beispiel Versand eines Newsletters an Kunden in der EU**
  Unternehmen dürften interessiert sein, ihre Kunden regelmässig durch einen Newsletter über ihre laufenden Angebote zu informieren. In einem solchen Fall ist Folgendes zu beachten: Ein Unternehmen darf E-Mailadressen von bestehenden Kunden ohne deren Einwilligung verwenden. Die Aufrechterhaltung der Kundenbeziehung und Werbemassnahmen begründen einen zulässigen Zweck zur Datenverarbeitung, namentlich ein berechtigtes Interesse.

  Wiederum wären jedoch die betroffenen Personen mittels Datenschutzerklärung aufzuklären und im Newsletter wäre ein entsprechender Link einzufügen. Ferner sollte im Newsletter eine Abmeldefunktion eingefügt werden. Wird der Newsletter über einen Dritten versandt, könnte der Datenschutzerklärung bspw. folgender Text hinzugefügt werden: «Ihre E-Mail-Adresse wird an die datenschutz-zertifizierte Newsletter-Software XY zum technischen Versand weitergegeben».

Anzumerken ist letztlich, dass das überarbeitete DSG in absehbarer Zeit in Kraft treten wird. Vorgesehen ist gemäss dem aktuellen Entwurf eine Angleichung des DSG an die DSGVO. Dies stellt einen weiteren Grund dar, weshalb Unternehmen in der Schweiz ihre internen Datenverarbeitungsprozesse an diesen neuen Datenschutz-Standard anpassen sollten.

Bitte beachten Sie, dass dieses Merkblatt lediglich einen Überblick über die wichtigsten Änderungen vermittelt.[1] Jeder Einzelfall bedarf einer gesonderten Prüfung. Bei Fragen stehen wir Ihnen gerne zur Verfügung.

Version 6/2018

[1] Die Informationen in diesem Merkblatt sind genereller Natur und dienen nur zu allgemeinen Informationszwecken. Die Anwendbarkeit der DSGVO ist im konkreten Einzelfall zu prüfen. Dieses Merkblatt stellt keine Rechtsberatung dar, weshalb jegliche Haftung in diesem Zusammenhang abgelehnt wird. Dieses Merkblatt ist urheberrechtlich geschützt. Es richtet sich nur an den Adressaten und darf ohne die vorgängige schriftliche Zustimmung von REBER weder kopiert, bearbeitet, weitergeleitet noch anderweitig genutzt werden.