WENGERPLATTNER

Handels- und Gesellschaftsrecht / IP & IT - Dezember 2017

EU-Datenschutz-Grundverordnung: Auswirkungen auf Schweizer Unternehmen

Autoren: Dr. Oliver Künzler und Dr. Martina Braun

Zurzeit sind zahlreiche Bemühungen im Gange, das Datenschutzrecht den rasanten technologischen Entwicklungen anzupassen. Unter anderem gilt ab dem 25. Mai 2018 die neue Datenschutz-Grundverordnung (EU-DSGVO) in der EU. Obwohl diese in der Schweiz nicht direkt anwendbar ist, werden zahlreiche Schweizer Unternehmen von ihrem Anwendungsbereich erfasst.

Der vorliegende Newsletter zeigt auf, inwieweit Schweizer Unternehmen von der EU-DSGVO betroffen sind und ob Handlungsbedarf besteht.

Anwendbarkeit der EU-DSGVO

Die EU-DSGVO gilt, wenn Unternehmen in der Schweiz:

- **betroffenen Personen in der EU Waren oder Dienstleistungen anbieten und deren Personendaten bearbeiten;**
- **das Verhalten von Personen in der EU beobachten (Webtracking);**
- **Personendaten im Auftrag eines Unternehmens in der EU bearbeiten (Auftragsdatenbearbeitung);**
- **die Datenbearbeitung an ein Unternehmen in der EU auslagern;**
- **vertraglich die Anwendung des Rechts eines EU-Mitgliedstaates vereinbaren.**

EU-Datenschutz-Grundverordnung: Auswirkungen auf Schweizer Unternehmen

Die EU-DSGVO beschränkt sich nicht auf eine Harmonisierung der nationalen Gesetzgebungen und eine Bestätigung der bislang im europäischen Datenschutzrecht geltenden Grundsätze, sondern verstärkt den Datenschutz zum Teil in erheblicher Hinsicht. Dies hat auch Auswirkungen auf das Schweizer Datenschutzrecht, da dieses revidiert und dem europäischen Niveau angepasst werden soll.

Dr. Oliver Künzler
Partner in der Businessgruppe für Handels- und Gesellschaftsrecht
oliver.kuenzler@wenger-plattner.ch

Dr. Martina Braun
Senior Associate in der Fachgruppe IP & IT
martina.braun@wenger-plattner.ch

Einleitung

Die EU-DSGVO wurde am 27. April 2016 verabschiedet. Für die Umsetzung wurde eine zweijährige Übergangsfrist bis am 25. Mai 2018 gewährt. Ab diesem Zeitpunkt gilt die EU-DSGVO unmittelbar und grundsätzlich einheitlich in allen EU-Mitgliedsstaaten. Letztere verfügen aber über gewisse Spielräume, um nationale Ausführungsbestimmungen zu erlassen.

Anwendbarkeit der EU-DSGVO auf Schweizer Unternehmen?

In persönlicher Hinsicht gilt die EU-DSGVO sowohl für diejenige Person, die über Zweck und Mittel der Datenbearbeitung entscheidet (Verantwortlicher bzw. *controller*), als auch für diejenige, die Daten im Auftrag eines Verantwortlichen bearbeitet (Auftragsverarbeiter bzw. *processor*).

Für den sachlichen Anwendungsbereich der EU-DSGVO wird nicht nach dem Volumen der Datenbearbeitung oder der Art der bearbeiteten Personendaten unterschieden. Nicht vom Schutz der EU-DSGVO erfasst werden jedoch die Daten von juristischen Personen. Zudem fällt die Datenbearbeitung im Rahmen von privaten oder familiären Tätigkeiten nicht in den Anwendungsbereich der EU-DSGVO.

Jede natürliche Person in der EU soll den von der EU-DGSVO gewährten Schutz beanspruchen können. Aus diesem Grund findet diese in räumlicher Hinsicht auch dann Anwendung, wenn der Datenbearbeiter zwar keine Niederlassung in der EU hat, seine Waren und Dienstleistungen aber Personen in der EU anbietet und in diesem Zusammenhang deren Personendaten bearbeitet. Dasselbe gilt für Unternehmen ohne Niederlassung in der EU, die das Verhalten von betroffenen Personen in der EU erfassen und auswerten.

Im Übrigen gilt die EU-DSGVO – unabhängig vom Ort der Datenbearbeitung – für die Personendatenbearbeitung im Zusammenhang mit der Geschäftstätigkeit einer EU-Niederlassung eines Unternehmens. Dies ist beispielsweise der Fall, wenn ein Schweizer Rechenzentrum für in der EU ansässige Kunden tätig ist, oder wenn eine Schweizer Muttergesellschaft die Kundendaten einer Tochtergesellschaft mit Sitz in der EU bearbeitet, um deren Geschäftsaktivitäten zu unterstützen.

Angesichts des Gesagten werden viele Schweizer Unternehmen vom Anwendungsbereich der EU-DSGVO erfasst.

Überblick über die EU-DSGVO

Gemäss EU-DSGVO ist die Bearbeitung von Personendaten nur zulässig, wenn der Betroffene in die fragliche Datenbearbeitung eingewilligt hat oder einer der anderen gesetzlich vorgesehenen Tatbestände (z.B. Vertragserfüllung, rechtliche Verpflichtung, berechtigte Interessen) vorliegt.

An die gültige Einwilligung des Betroffenen werden hohe Anforderungen gestellt. Letzterer muss seine Zustimmung freiwillig, informiert und unmissverständlich für jeden Einzelfall in einer eindeutig bestätigenden Handlung abgeben. Eine rein stillschweigende Zustimmung genügt demgegenüber nicht mehr (die Einwilligung muss z.B. mittels Anklicken eines Buttons erfolgen). Zudem kann die Einwilligung jederzeit widerrufen werden.

Revision des Schweizer Datenschutzrechts

Am 15. September 2017 hat der Bundesrat die Botschaft zur Totalrevision des Bundesgesetzes über den Datenschutz (DSG) und den entsprechenden Gesetzesentwurf vorgelegt.

Ziel sind die Modernisierung des DSG sowie die Angleichung der Schweizer Gesetzgebung an das europäische Datenschutzrecht. Insbesondere soll die Ratifikation der revidierten Europaratskonvention SEV 108 und die Übernahme der EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts ermöglicht werden. Die Schweiz muss diese umsetzen, um ihren Verpflichtungen aus dem Schengen Abkommen nachzukommen. Zudem soll eine inhaltliche Annäherung an die EU-DSGVO erfolgen, um sicherzustellen, dass die Schweiz von der EU in einem sogenannten Angemessenheitsbeschluss weiterhin als Drittstaat mit einem gegenüber der EU gleichwertigen Datenschutzniveau anerkannt wird. Letzteres ist für die Schweizer Wirtschaft von zentraler Bedeutung.

Gemäss dem Entwurf sollen die Rechte der betroffenen Personen gestärkt werden (erhöhte Pflichten zur Transparenz, strengere Bedingungen an die Einwilligung und Vorgaben betreffend datenschutzfreundliche Voreinstellungen). Weiter werden Selbstregulierungsmassnahmen gefördert, die Befugnisse des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) erweitert und die Strafbestimmungen verschärft.

Zunächst wird nun das Parlament den Entwurf beraten. Es ist jedoch absehbar, dass das DSG dem europäischen Datenschutzrecht angenähert wird.

Die EU-DSGVO misst dem Grundsatz der Transparenz eine fundamentale Bedeutung zu. Dieser Grundsatz wird durch ausführliche Informationspflichten und Auskunftsansprüche konkretisiert. Der Verantwortliche muss den betroffenen Personen unter anderem seine Identität und Kontaktangaben (sowie ggfs. diejenigen seines Vertreters und/oder seines Datenschutzbeauftragten) mitteilen. Es ist darüber zu informieren, welche Daten erhoben und bearbeitet werden, zu welchen Zwecken dies geschieht und für welche Dauer die Daten gespeichert werden. Gegebenenfalls sind Angaben zu den Empfängern der Daten sowie zur Datenübermittlung an Nicht-EU/EWR-Staaten zu machen. Weiter müssen die betroffenen Personen auf ihre Rechte bezüglich Auskunft, Berichtigung, Löschung und Widerspruch sowie das Beschwerderecht bei einer Aufsichtsbehörde hingewiesen werden. Diese Informationen müssen präzise, leicht zugänglich und verständlich sein sowie in klarer und einfacher Sprache abgefasst werden. Zusätzlich können visuelle Elemente verwendet werden.

Zusätzlich zu den oben genannten Rechten hat jede betroffene Person unter bestimmten Voraussetzungen das Recht, die Übermittlung der sie betreffenden Personendaten in einem strukturierten, gängigen und maschinenlesbaren Format zu fordern (Datenportabilität).

Nebst den bislang geltenden Grundsätzen der Datenbearbeitung wird der Grundsatz der Eigenverantwortung der Datenbearbeiter verankert. Wer Personendaten bearbeitet, ist nicht mehr nur dafür verantwortlich, die Datengesetzgebung einzuhalten, sondern muss dies auch nachweisen können. Als Ausfluss dieser Rechenschaftspflicht ist ein Verzeichnis aller Datenbearbeitungstätigkeiten zu führen. Von der Pflicht, ein Verzeichnis zu führen, befreit sind nur Unternehmen, die weniger als 250 Mitarbeiter haben und nur gelegentlich Personendaten bearbeiten, es sei denn, die Bearbeitung berge erhebliche Risiken oder betreffe sensible Personendaten.

Bietet ein Unternehmen ohne EU-Niederlassung Waren oder Dienstleistungen in der EU an oder beobachtet es das Verhalten von Personen in der EU, muss es einen Vertreter in der EU bestellen, ausser (i) die Datenbearbeitung erfolgt nur gelegentlich, (ii) betrifft keine sensiblen Personendaten und (iii) birgt kein besonderes Risiko. Ebenfalls eingeführt wird die Pflicht, unter bestimmten Voraussetzungen einen unternehmensinternen Datenschutzbeauftragten zu ernennen. Dies ist insbesondere der Fall, wenn die Kerntätigkeit eines Unternehmens in der regelmässigen oder systematischen Beobachtung von betroffenen Personen oder der umfangreichen Bearbeitung sensibler Daten besteht.

Weiter verlangt die EU-DSGVO, dass die Grundsätze der Datenbearbeitung mittels geeigneter Technikausgestaltung (*privacy by design*) sowie datenschutzfreundlichen Grundeinstellungen (*privacy by default*) umgesetzt werden (z.B. Minimierung der Datenerhebung, Pseudonymisierung).

Führt die Datenbearbeitung voraussichtlich zu einem grossen Risiko für die Betroffenen, so muss eine Datenschutz-Folgeabschätzung (*privacy impact assessment*) vorgenommen werden. Eine solche beinhaltet unter anderem eine Beschreibung der geplanten Datenbearbeitungen, eine Bewertung der damit verbunden Risiken sowie eine Auflistung der Abhilfemassnahmen.

Wird der Schutz von Personendaten verletzt, hat die für die Datenbearbeitung verantwortliche Person dies unverzüglich, jedoch spätestens innert 72 Stunden nach Kenntnis der Verletzung, den Aufsichtsbehörden zu melden, es sei denn, es bestehe kein Risiko für die Rechte und Freiheiten der betroffenen Personen. Führt die Datenschutzverletzung zu einem hohen Risiko für die Betroffenen, so müssen auch diese benachrichtigt werden. Die verantwortliche Person muss in jedem Fall die Verletzung sowie die ergriffenen Massnahmen dokumentieren.

Es ist höchste Zeit für jedes Unternehmen in der Schweiz, sofern nicht bereits geschehen, zu prüfen, ob unter der EU-DSGVO Handlungsbedarf besteht und die erforderlichen Massnahmen einzuleiten.

Den von jedem Mitgliedsstaat zu bestellenden Aufsichtsbehörden kommen im Vergleich zum Schweizerischen Eidgenössischen Datenschutzbeauftragten (EDÖB) sehr viel weitreichendere Befugnisse zu. Diese haben unter anderem die Kompetenz, Administrativsanktionen in Form von hohen Geldbussen (bis maximal EUR 20'000'000 oder 4% des gesamten weltweiten Jahresumsatzes des vergangenen Geschäftsjahres) zu verhängen.

Zu ergreifende Massnahmen

Unabhängig von seiner Grösse sollte jedes Unternehmen in der Schweiz klären, ob es von der EU-DSGVO betroffen ist. Falls dem so ist, ist zu ermitteln, welche Personendaten, zu welchen Zwecken, wie, wo und von wem erhoben und bearbeitet werden. Auch sind die bestehenden Datenschutzmassnahmen und Prozesse zu dokumentieren.

In einem nächsten Schritt ist zu prüfen, welche datenschutzrechtlichen Vorgaben einschlägig sind und ob diese eingehalten werden bzw. welche Lücken bestehen. Sodann sind, anhand eines risikobasierten Ansatzes, die notwendigen Massnahmen zu ergreifen, beispielsweise:

- Umsetzung der Informationspflichten (z.B. Datenschutzerklärungen);
- Abschluss bzw. Anpassung von Verträgen mit Auftragsverarbeitern;
- Prüfung der Grundlagen der Datenbearbeitungen;
- ggfs. Einholen von Einwilligungen;
- Festlegung von internen Prozessen zur Sicherstellung der Rechte der Betroffenen (Recht auf Information, Auskunft, Berichtigung, Löschung und Widerspruch);
- organisatorische und technische Schutzmassnahmen;
- Dokumentation der Datenbearbeitungen;
- Implementierung von Verfahren bei Verletzungen des Datenschutzes;
- ggfs. Datenschutzfolge-Abschätzungen;
- ggfs. Bestellung eines Datenbeauftragten und/oder eines Vertreters in der EU.

Schliesslich sind die kontinuierliche Umsetzung und Aufrechterhaltung der implementierten Massnahmen und Prozesse sicherzustellen. Unabdingbar hierfür ist, (i) unternehmensintern verantwortliche Personen zu benennen, (ii) diese mit ausreichenden Ressourcen auszustatten und (iii) generell ein Bewusstsein für datenschutzrechtliche Belange zu schaffen.

Ausblick und praktische Empfehlungen

Die EU-DSGVO betrifft viele Schweizer Unternehmen. Zudem wird das Schweizer Datenschutzgesetz dem europäischen Datenschutzrecht angenähert werden. Es empfiehlt sich daher für jedes Schweizer Unternehmen, seine Datenbearbeitungsprozesse und Datenschutzmassnahmen einer Überprüfung zu unterziehen.

Um die oben dargelegten Schritte möglichst effektiv umzusetzen, ist es zielführend, eine Projekt-Gruppe einzusetzen. Diese sollte aus Mitarbeitern aus den Bereichen IT, Legal & Compliance und HR sowie den für die Datenbearbeitung verantwortlichen Personen zusammengesetzt sein und mit den notwendigen Ressourcen ausgestattet werden. Wichtig ist es schliesslich, die notwendigen Entscheidungsträger in den Prozess einzubinden.

Basel: Aeschenvorstadt 55 | CH-4010 Basel | T +41 61 279 70 00 | basel@wenger-plattner.ch
Zürich: Seestrasse 39 | CH-8700 Küsnacht-Zürich | T +41 43 222 38 00 | zuerich@wenger-plattner.ch
Bern: Jungfraustrasse 1 | CH-3000 Bern 6 | T +41 31 357 00 00 | bern@wenger-plattner.ch

www.wenger-plattner.ch