Publikation vom Juli 2018
Datenschutzrecht
Claudia Keller Rechtsanwältin claudia.keller@raggenbass.com

Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf Schweizer Unternehmen

Am 25. Mai 2018 ist die neue Datenschutzgrundverordnung («DSGVO») der Europäischen Union («EU») in Kraft getreten. Diese ist in der gesamten EU unmittelbar anwendbar, ohne dass es einer Umsetzung in nationales Recht bedarf. Der Datenschutz in der EU wird damit erstmals auf eine einheitliche Grundlage gestellt. Schweizer Unternehmen sind von der DSGVO in zweifacher Hinsicht betroffen – zum einen durch eine direkte Anwendung der DSGVO, zum anderen durch das sich in Revision befindliche schweizerische Datenschutzrecht, in welches das neue EU-Recht zwangsläufig einfliessen wird, damit die Gleichwertigkeit des schweizerischen Datenschutzes mit demjenigen der EU gewährleistet ist, andernfalls der für Schweizer Unternehmen wichtige Datenaustausch mit Unternehmen in der EU erheblich erschwert würde.

Wann bin ich als Schweizer Unternehmen von der DSGVO betroffen?

Die DSGVO gilt unmittelbar für Schweizer Unternehmen, welche personenbezogene Daten verarbeiten, und

a) die Datenverarbeitung im Zusammenhang mit den Geschäftsaktivitäten einer EU-Niederlassung des Unternehmens oder eines von diesem mit der Datenbearbeitung beauftragen, in der EU ansässigen Dritten (sog. Auftragsverarbeiter) erfolgt (**„Niederlassung in der EU“**); oder
b) wenn das Unternehmen oder der Auftragsverarbeiter über keine Niederlassung in der EU verfügen, die Datenverarbeitung zu dem Zweck geschieht, in der EU ansässigen Personen Waren oder Dienstleistungen anzubieten oder deren Verhalten zu beobachten (**„Zielgruppe in der EU“**).

Welche Verpflichtungen habe ich als unter die DSGVO fallender Unternehmer?

Bearbeiter von Personendaten haben die betroffenen Personen (Kunden, Mitarbeiter etc.) über die Verarbeitung ihrer Daten sowie die ihnen zustehenden Rechte, wie insbesondere das Recht auf Berichtigung, Löschung und Übertragung der Daten, umfassend und in verständlicher Sprache zu informieren. Beruht die Datenverarbeitung auf einer Einwilligung, ist eine solche ausdrücklich einzuholen. Datenverarbeitungssysteme sind datenschutzfreundlich auszugestalten, ferner haben die Unternehmen ihre Datenverarbeitungsaktivitäten aufzuzeichnen. Auch die zum Schutz der Daten ergriffenen Massnahmen müssen dokumentiert werden, so dass diese jederzeit nachgewiesen werden können. Datenschutzverstösse sind innert 72 Stunden an die zuständige Datenschutzbehörde sowie an die betroffene Person selbst zu melden. Schliesslich haben Unternehmen unter bestimmten Voraussetzungen einen Datenschutzbeauftragten sowie einen Vertreter in der EU zu benennen.

Was passiert, wenn ich mich nicht an die Vorgaben der DSGVO halte?

Unternehmen, die gegen die DSGVO verstossen, drohen Geldstrafen von bis zu CHF 20 Millionen Euro oder 4% des weltweit erzielten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Für kleinere Unternehmen, die erstmalig oder versehentlich gegen das Datenschutzrecht verstossen, sieht die DSVGO eine Reihe von abschreckenden Massnahmen vor, wie Mahnungen, Verwarnungen oder eine vorübergehende oder dauerhafte Beschränkung der Datenverarbeitung.

Heutiger Handlungsbedarf

Schweizer Unternehmen wird empfohlen, zu prüfen, ob sie von der DSGVO betroffen sind und welche Massnahmen gegebenenfalls zur Umsetzung der DSGVO erforderlich sind. Insbesondere werden Standarddokumente, wie Musterverträge mit Kunden und Auftragsverarbeitern (z.B. Dienstleister im Bereich Buchhaltung, Fakturierung, Inkasso, IT-Support) und allgemeine Geschäftsbedingungen, zu überarbeiten und das Compliance-Programm (interne Weisungen und Reglemente betreffend Datenschutz) zu aktualisieren sein. Ferner müssen Unternehmen ihre Datenverarbeitungsprozesse, Applikationen und Website so anpassen, dass nur diejenigen Personendaten erhoben und bearbeitet werden, die effektiv benötigt werden, ausserdem sind die Sicherheitsstandards der Bearbeitungssysteme zu überprüfen. Schliesslich sind Management und Mitarbeiter für die neuen Datenschutzstandards zu sensibilisieren und zu schulen. Im Hinblick auf die drohenden Sanktionen sollte das Management von Datenschutzrisiken keine einmalige Angelegenheit bleiben, sondern unternehmensintern als fortlaufender Prozess institutionalisiert werden.