Cornelia Mattig
RechtsanwÃ¤ltin und Urkundsperson
MLaw mit Vertiefung im Wirtschaftsrecht UZH
LL.M. in European Law Queen Mary University of London

The clock is ticking - Ist Ihr Unternehmen fit für das neue EU-Datenschutzrecht?

Am 25. Mai 2018 tritt die Datenschutzgrundverordnung (DSGVO) der EU in Kraft. Diese wird nicht nur Auswirkungen auf die EU-Mitgliedstaaten haben, sondern auch auf Schweizer Unternehmen. Das neue EU-Datenschutzrecht ist auf Schweizer Unternehmen direkt anwendbar, wenn sie Güter und Dienstleistungen in der EU anbieten oder aus der Schweiz solche Güter oder Dienstleistungen an Personen, die in der EU niedergelassen sind, zur Verfügung stellen. Fehlbare Unternehmen werden von hohen Bussen betroffen sein. Indirekt betrifft die DSGVO Schweizer Unternehmen im Rahmen des neuen Schweizerischen Datenschutzgesetzes, welches auch im Verlauf dieses Jahres in Kraft treten soll.

Frage:
Was bedeutet dies für Schweizer Unternehmen? Ist das EU-Datenschutzrecht auf Schweizer Unternehmen überhaupt anwendbar?

Antwort:
Das neue EU-Datenschutzrecht ist über die Grenzen der EU hinaus anwendbar und wird direkt auf einige Schweizer Unternehmen angewandt werden. Direkte Anwendung findet die Regelung, wenn ein Schweizer Unternehmen Daten von Bürgern oder Unternehmen in der EU bearbeitet. Bis am 25. Mai 2018 müssen diese Unternehmen die EU-Massnahmen umgesetzt haben, ansonsten drohen hohe Bussen von bis zu 20 Millionen Euro bei natürlichen Personen oder 4% des weltweiten Umsatzes bei Unternehmen. So kurz – so gut, aber was bedeutet dies und betrifft dies alle Schweizer Unternehmen? Auf diese und weitere Punkte wird im nachfolgenden Artikel kurz eingegangen. Im Zweifel ist es jedoch empfehlenswert, sich an einen Spezialisten im Datenschutzrecht zu wenden. Das Datenschutzrecht bezweckt die Regelung des Umgangs mit bestimmten Daten, insbesondere mit geschützten Geheimnissen oder Telekommunikationsgeheimnissen, aber auch die Selbstbestimmung über Informationen. Gerade Personendaten sind sehr wertvoll, weil Unternehmen grosses wirtschaftliches Interesse an ihnen haben, aber auch, weil es so etwas wie ein informationelles Selbstbestimmungsrecht gibt. Das Datenschutzrecht ist ein Versuch, die Interessen des Einzelnen an Daten und den berechtigten Interessen der Allgemeinheit sowie der Datenverarbeiter auszubalancieren. Als persönliche Daten gelten alle Informationen einer natürlichen Person, welche zur direkten oder indirekten Identifizierung dieser Person gebraucht werden können. Solche sind insbesondere Namen, Fotografien, Mailadressen, Dossiers, Akten, Bankverbindungen oder Statistiken.

Ist die DSGVO auf mein Unternehmen anwendbar?
Die neuen datenschutzrechtlichen Regelungen der EU finden über ihre Grenzen hinaus Anwendung. Für Schweizer Unternehmen bedeutet dies, dass die DSGVO angewendet wird, wenn das Unternehmen personenbezogene Daten von natürlichen Personen verarbeitet, die sich in der EU befinden, sofern das Schweizer Unternehmen

1. diesen Personen in der EU Waren oder Dienstleistungen anbietet; oder
2. das Verhalten der betroffenen Personen in der EU durch die Datenverarbeitung beobachten will

Dabei ist es irrelevant, ob die Tätigkeit aus der Schweiz vorgenommen wird oder durch eine Niederlassung in der EU. Damit die DSGVO aufgrund des Angebots von Waren und Dienstleistungen Anwendung findet, muss festgestellt werden, ob das Unternehmen das Anbieten offensichtlich beabsichtigt hat. Hinweise ergeben sich dabei unter anderem aus Sprach- oder Währungsangaben. Die blosse Zugänglichkeit der Homepage wird (wohl) nicht als Indiz gelten.

Was für Pflichten ergeben sich für Unternehmen?
1. Information und Einwilligung der betroffenen Person
Nach EU-Recht ist die Datenverarbeitung generell verboten, sofern diese nicht durch Gesetz ausdrücklich erlaubt ist oder eine Einwilligung der betroffenen Person vorliegt. Die Anforderungen an eine solche Einwilligung wurden durch die DSGVO verschärft. Die nachfolgenden Voraussetzungen müssen zwingend gegeben sein:

- freie Entscheidung;
- ausführliche, erkennbare und bestimmte Information;
- aktive Handlung;

- Widerruflichkeit

2. «Privacy by Design» und «Privacy by Default»
Der Grundsatz von «Privacy by Design» bedeutet, dass der Datenschutzverantwortliche bereits im Zeitpunkt der Planung der Datenverarbeitung das Risiko von Verletzungen verringern und/oder vorbeugen muss. Dies kann zum Beispiel durch regelmässige Löschung von Daten geschehen. Der dazugehörende Grundsatz des «Privacy by Default» hingegen bedeutet, dass der Verantwortliche durch Voreinstellungen sicherstellt, dass nur relevante Daten standardmässig verarbeitet werden.

3. Ernennung eines Vertreters in der EU als Grundsatz
Schweizer Unternehmen ohne Niederlassung in der EU sind neu verpflichtet, einen Vertreter, welcher sie in ihren Pflichten in Bezug auf die DSGVO vertritt, zu bezeichnen. Ausgenommen davon sind Unternehmen, die nur gelegentlich Daten von EU ansässigen Personen bearbeiten und keine umfangreiche Bearbeitung von besonders schützenswerten Personendaten vornehmen. Solche sind insbesondere Gesundheitsdaten.

4. Verzeichnis von Verarbeitungstätigkeiten
Hierbei handelt es sich um eine Übersicht über alle Prozesse und Verfahren im Unternehmen zur Verarbeitung von personenbezogenen Daten. Dazu ist zunächst festzustellen, wo personenbezogene Daten in einem Unternehmen erhoben und verarbeitet werden, beispielsweise bei Kunden, Lieferanten oder Mitarbeitern. So dann zum Beispiel bei spezifischen Tools, wie Zeiterfassungs- oder Buchhaltungssystemen, die personenbezogene Daten speichern. Die Erstellung dieses Verzeichnisses bietet sich sogleich zur Evaluation an, ob ein Unternehmen unter den Anwendungsbereich der DSGVO fällt.

5. Meldepflicht
Im Falle, dass der Schutz von personenbezogenen Daten verletzt wurde, hat die Verletzung innerhalb von 72 Stunden gemeldet zu werden, ausser es besteht kein Risiko für die Verletzungen von Rechten und Freiheiten von Individuen. Oftmals sind auch die betroffenen Personen zu benachrichtigen.

6. Datenschutzfolgenabschätzung
Sofern eine bestimmte Form der Verarbeitung ein hohes Risiko für den Datenschutz birgt, ist eine Datenschutzfolgenabschätzung vorzunehmen. Dabei ist festzustellen, welches Risiko die Datenverarbeitung verursacht. Bei einem hohen Risiko ohne Massnahmen ist die zuständige Aufsichtsbehörde zu konsultieren. Solche Abschätzungen werden insbesondere im Zusammenhang mit neuen Technologien notwendig sein.

Was ist die Folge von Verstössen gegen die DSGVO?
Verstösse gegen die DSGVO führen zu hohen Bussen. Das neue EU-Recht sieht Bussen bis maximal 20 Millionen Euro für beteiligte natürliche Personen oder für Unternehmen bis zu 4% des weltweiten Jahresumsatzes vor.

Was sind die nächsten Schritte für Ihr Unternehmen?

1. Beschaffen Sie sich Informationen zur DSGVO.
2. Ernennen Sie einen Datenschutzverantwortlichen oder ein Datenschutzteam.
3. Überprüfen Sie, ob Sie unter den Anwendungsbereich der DSGVO fallen und wenn ja, ob Ihr Unternehmen den Anforderungen genügt.
4. Erstellen Sie ein Verarbeitungsverzeichnis und eine Risikoprüfung inkl. einer Datenschutzfolgenabschätzung, sofern dies notwendig erscheint.
5. Implementieren Sie technische und organisatorische Massnahmen auf drei Ebenen
    a. Datenverarbeitung innerhalb des Unternehmens;
    b. Übermittlung von Daten an Drittstaaten;
    c. Auftragsverarbeitung / Joint Controllership / Übermittlung an Dritte.
6. Beachten Sie Rechte der Betroffenen (z.B. Informations-, Auskunfts-, Berichtigungs- oder Löschungsrechte).

Einige Hinweise für die kommenden Monate:
Diese Regelungen werden relevant für Unternehmen aller Grössen, daher ist es empfehlenswert, dass sich insbesondere auch KMU – gerade hinsichtlich der hohen Sanktionen – mit diesen Neuerungen auseinandersetzen. Die dargestellten Pflichten stellen einen Einblick in die DSGVO dar. In Anbetracht der hohen Sanktionen ist der DSGVO grosse Beachtung zu schenken. Unternehmen sind gut beraten, ihre internen Prozesse, Richtlinien, Verträge und Datenschutzerklärungen zu überarbeiten und allenfalls ihre IT-Systeme anzupassen sowie gegebenenfalls mit einem Spezialisten zusammenzusitzen.
Diese internen Prozessanpassungen dürften für alle Schweizer Unternehmen lohnenswert sein, da die Schweiz zurzeit ihr geltendes Datenschutzrecht überarbeitet. Dies erscheint zentral, da die Schweizer Anpassung darauf abzielt, gegenüber dem EU-Recht adäquat zu sein und gleichzeitig nicht darüber hinausgehen möchte. Wie sich dies tatsächlich gestaltet ist noch abzuwarten. Es ist jedoch davon auszugehen, dass Unternehmen, die nach EU-Datenschutzrecht ihr Geschäft betreiben, auch den Schweizer datenschutzrechtlichen Regelungen genügen sollten.

Tags: Rechtsberatung, Datenschutz, Meldepflicht, EU, EU-Datenschutzrecht, Schweiz