Neue Datenschutzverpflichtungen für Unternehmen ab 25.5.2018

Mit der vom Europäischen Parlament beschlossenen Datenschutz-Grundverordnung (**DSGVO**) werden die Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen EU-weit vereinheitlicht. Zur Durchführung der DSGVO wurde in Österreich das Datenschutz-Anpassungsgesetz 2018 beschlossen.

Die **neuen Bestimmungen treten mit 25.5.2018 in Kraft**. Bis zu diesem Zeitpunkt müssen alle Datenanwendungen und Geschäftsprozesse an die neue Rechtslage angepasst werden. Daher ergibt sich für jedes Unternehmen (unabhängig von der Branche), das in irgendeiner Weise personenbezogene Daten verarbeitet (zB eine Kundendatei führt, Rechnungen ausstellt,), dringender Handlungsbedarf, da die internen Abläufe und alle Datenanwendungen in Bezug auf den Datenschutz analysiert und gegebenenfalls rechtzeitig angepasst werden müssen.

Der Schwerpunkt der DSGVO liegt auf der Stärkung der Betroffenenrechte. Grundsätzlich werden alle Datenverarbeitungen mit **personenbezogenen Daten** verboten, außer es gibt eine Rechtfertigung. Diese kann nur aufgrund einer gesetzlichen Verpflichtung, der Einwilligung des Betroffenen oder aus überwiegendem Interesse bestehen. Wie bisher muss auch zukünftig **jede Datenverwendung einem konkreten Rechtfertigungsgrund zugeordnet** werden. Und nur für diese Aufgabe dürfen die Daten verwendet werden.

Insbesondere die folgenden DSGVO Anforderungen beinhalten für österreichische Unternehmen einen hohen Arbeitsaufwand und Kosten:

- Feststellung, ob man Verantwortlicher oder Auftragsverarbeiter für die Daten Betroffener ist
- Erstellung und Führung eines Datenanwendungsverzeichnisses
- Erweiterung der Informationspflichten gegenüber den Betroffenen
- Nominierung eines **Datenschutzbeauftragten**

Bislang wurden die Daten in einem Unternehmen oft abteilungs- und unternehmensübergreifend verwendet. Beispielsweise wurde die Personalverrechnung im Konzernverbund zentral von einer Tochtergesellschaft durchgeführt oder die Kundenstammdaten wurden von mehreren Konzerngesellschaften gemeinsam genutzt. Nun gibt es kein „Konzernprivileg“ mehr. Jede Gesellschaft muss feststellen, ob sie **Verantwortlicher** für die Daten ist oder im Auftrag eines Anderen die Informationen verarbeitet (**Auftragsverarbeiter**). Der Verantwortliche bleibt dem Betroffenen gegenüber immer verantwortlich für die Sicherheit und den Einsatz seiner Daten. Daher müssen zwischen allen Verantwortlichen und Auftragsverarbeitern Verträge oder Service Level Agreements (SLA) geschlossen werden, um die DSGVO-konforme Verarbeitung zu gewährleisten. Jedes Unternehmen muss daher die Datenflüsse analysieren und mit Verträgen sichern.

Bisher wurden Anwendungen bei der Datenschutzkommission gemeldet, wenn Daten Betroffener verarbeitet werden sollten. Diese prüfte die Anmeldung, führte eine Risikoanalyse durch und speicherte die Anwendung im DVR-Register. Mit der DSGVO fällt die Meldung an das DVR Register weg und jedes Unternehmen muss selbst das **Datenanwendungsverzeichnis** führen, inklusive einer Risikoanalyse und gegebenenfalls der Datenschutz-Folgenabschätzung.

Die **Betroffenenrechte** wurden gestärkt. Jeder, der von Datenverarbeitungen betroffen ist, muss **proaktiv** (bei Erstkontakt) und **umfassend** informiert werden, wobei auch technisch die folgenden Anforderungen umgesetzt werden müssen:

- Auskunftsrecht (u.a. auch über die geplante Speicherdauer)
- Recht auf Berichtigung
- Recht auf Löschung und auf „Vergessen“
- Recht auf Datenübertragbarkeit
- Recht auf Einschränkung der Verarbeitung
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger
- Widerspruchsrecht

Die Bestellung eines (internen oder externen) **Datenschutzbeauftragten** ist u.a. dann verpflichtend vorgesehen, wenn der Geschäftszweck in der Verarbeitung personenbezogener Daten besteht (zB ein

Steuerberater, der für Klienten die Lohnverrechnung durchführt). Der **Datenschutzbeauftragte ist an die Datenschutzbehörde zu melden.**

Zusammenfassend ist festzuhalten, dass Verträge, Prozesse und IT-Systeme angepasst werden müssen, um diese neuen Anforderungen zuverlässig gewährleisten zu können. Außerdem müssen die Mitarbeiter umfassend geschult werden, um die neuen Anforderungen geeignet unterstützen zu können. In Anbetracht der Komplexität der Materie und der möglichen hohen Strafen ist es jedenfalls empfehlenswert, sich bei der Umsetzung von Experten unterstützen zu lassen.