Starke Verschärfungen durch die Datenschutz-Grundverordnung

Am 25. Mai 2018 wird die **europäische Datenschutz-Grundverordnung** Geltung erlangen, welche in Österreich durch das **Datenschutz-Anpassungsgesetz 2018** umgesetzt wurde. Bis dahin gelten noch die Regelungen des **Datenschutzgesetzes 2000**. Die Notwendigkeit für Änderungen ist auch auf den stetig wachsenden Binnenmarkt und damit unionsweiten Austausch **personenbezogener Daten** zurückzuführen. Schließlich soll auch der raschen technologischen Entwicklung (Cloud Computing, Big Data, usw.) und den Herausforderungen durch die **Globalisierung** besser Rechnung getragen werden. Unternehmen sind gut beraten, die Maßnahmen für einen besseren Datenschutz entsprechend umzusetzen – auch weil **sehr hohe Strafen** drohen. Betroffen von den Neuregelungen sind Unternehmen (innerhalb der EU bzw. aus Drittstaaten, sofern sie Leistungen an EU-Bürger anbieten) bereits dann, wenn sie in irgendeiner Weise **personenbezogene Daten verarbeiten**, indem z.B. Kundendateien geführt werden, Rechnungen ausgestellt werden oder Lieferantendaten gespeichert werden. Immerhin wird es zukünftig **keine Meldepflicht** mehr bei der **Datenschutzbehörde** (Datenverabeitungsregister) geben.

Das Recht auf Datenschutz ist ein **Grundrecht**, welches in Österreich im Verfassungsrang steht. Es ist nicht nur vom Staat, sondern auch unter Privaten einzuhalten – wesentlich ist dabei das Prinzip "**Verbot mit Erlaubnisvorbehalt**". Dahinter verbirgt sich die strenge Maxime, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist und nur dann vorgenommen werden darf, wenn es das Gesetz (ausnahmsweise) erlaubt. Nachfolgend sind **wesentliche Aspekte** bzw. **Neuerungen** dargestellt.

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Durch passende **technische und organisatorische Maßnahmen** und Verfahren müssen die **Rechte** der betroffenen Personen **geschützt** werden. **Datenschutzrechtliche Voreinstellungen** sollen sicherstellen, dass nur jene personenbezogenen Daten verarbeitet werden, welche für den jeweiligen

bestimmten **Verarbeitungszweck erforderlich** sind. Praktisch bedeutet dies, dass personenbezogene Daten (von Bewerbern, ehemaligen Mitarbeitern, Kunden, usw.) strenger geschützt werden müssen und auch **gelöscht werden müssen**, wenn der **Verarbeitungszweck erfüllt** ist. Zugleich muss **mehr Transparenz** gegenüber Aufsichtsbehörden, Kunden sowie Mitarbeitern sichergestellt werden. Insgesamt betrachtet müssen bei der Verarbeitung personenbezogener Daten die **Grundsätze Rechtmäßigkeit**, Verarbeitung nach **Treu und Glauben**, **Transparenz** (d.h. die Datenverarbeitung muss für die betroffene Person nachvollziehbar sein), **Zweckbindung** (im Vorhinein festgelegter eindeutiger und legitimer Zweck), **Datenminimierung**, **Richtigkeit** (es sollen nur sachlich richtige Daten verarbeitet werden – unrichtige Daten sind unverzüglich zu löschen bzw. zu berichtigen), **Speicherbegrenzung** sowie **Integrität und Vertraulichkeit** (die personenbezogenen Daten müssen vor unbefugter/unrechtmäßiger Verarbeitung und auch vor unbeabsichtigtem Verlust geschützt werden) **erfüllt** sein.

Verzeichnis von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten hat vergleichbar den derzeitigen DVR-Meldungen neben dem **Zweck der Datenverarbeitung** weitere Informationen zu enthalten wie z.B. die **Beschreibung** der Kategorien der von der Datenverarbeitung betroffenen **Personen** und der entsprechenden Daten (etwa Rechnungs- und Adressdaten von Kunden und Lieferanten). Ebenso muss das Verzeichnis die **Empfängerkategorien** der personenbezogenen Daten enthalten (z.B. Sozialversicherung, Finanzamt, Rechtsanwalt, Steuerberater, usw.) einschließlich der Empfänger in Drittländern oder internationalen Organisationen. Das Verzeichnis wird durch die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien sowie eine Beschreibung der **technischen und organisatorischen Datensicherheitsmaßnahmen** vervollständigt. Unternehmen mit **weniger als 250 Mitarbeitern** sind von der Verpflichtung zur Führung solcher Verzeichnisse **nur dann befreit**, sofern die **Datenverarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt, die Verarbeitung nur gelegentlich** erfolgt oder die Verarbeitung **keine sensiblen Daten** bzw. Daten über strafrechtliche Verurteilungen beinhaltet.

Meldung von Datenschutzverletzungen

Verletzungen des Schutzes personenbezogener Daten müssen den **nationalen Aufsichtsbehörden** sowie der **betroffenen Person möglichst rasch mitgeteilt** werden. Ausnahmen davon gelten, sofern die Verletzung nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt.

Datenschutzbeauftragter

Für das Unternehmen muss **verpflichtend** ein **Datenschutzbeauftragter** bestellt werden, wenn die **Kerntätigkeit** des Unternehmens in Verarbeitungsvorgängen besteht, welche eine **umfangreiche, regelmäßige und systematische Beobachtung** von betroffenen Personen erforderlich macht oder etwa besonders sensible Daten über strafrechtliche Verurteilungen oder Straftaten verarbeitet werden. Bei der Bestellung des Datenschutzbeauftragten ist zu bedenken, dass die Person **weisungsfrei** ist, **Kündigungsschutz** genießt und **uneingeschränkte Einsichtsrechte** in die verarbeiteten Daten hat.

Informationspflichten und Betroffenenrechte

Vielfältige **Informationen und Betroffenenrechte** sind **zeitnah** zur Verfügung zu stellen bzw. zu erledigen. Davon umfasst sind etwa **Auskunftsrechte** (auch über die geplante Speicherdauer), das Recht auf Berichtigung, das Recht auf Löschung und auf "Vergessenwerden", das Recht auf Einschränkung der Verarbeitung, die Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger, das Recht auf Datenübertragbarkeit sowie das Widerspruchsrecht.

Hohe Geldstrafen

Die Verbesserungen beim Datenschutz bzw. die neuen Bestimmungen sind durch **sehr hohe Geldbußen** bei Verstößen begleitet. So können bei **besonders schwerwiegenden Verstößen**, z.B. bei Verletzung der Betroffenenrechte oder auch bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde, **Geldbußen bis zu 20 Mio. €** bzw. bis zu **4% des weltweit erzielten Vorjahresumsatzes** verhängt werden. Bei weniger schwerwiegenden Verstößen (z.B. bei Verletzung der Datensicherheitsvorschriften) beträgt die **maximale Geldbuße** immer noch **10 Mio. €** bzw. **2%** des weltweit erzielten **Vorjahresumsatzes**.