DATENSCHUTZ-GRUNDVERORDNUNG (EU-DSGVO) AUSWIRKUNGEN FÜR UNTERNEHMEN

1. Entstehung

Trotz massiver Kritik unterschiedlichster österreichischer Interessensvertretungen, wurde der Entwurf des Datenschutz-Anpassungsgesetzes 2018 am 29.06.2017 im Nationalrat beschlossen.

Somit werden zukünftig sowohl die Datenschutz-Grundverordnung als auch das Datenschutz-Anpassungsgesetz 2018 die entscheidenden Rechtsgrundlagen für Datenverarbeitung österreichischer Unternehmen darstellen.

Die neue Rechtslage stellt Unternehmen vor umfassende und teilweise komplexe Herausforderungen. Daher empfiehlt es sich, entsprechende Anpassungsmaßnahmen, sowie die Entwicklung einer Datenschutz-Compliance rechtzeitig zu beginnen und durchzuführen.

2. Geltungsbereich der DSG-VO

Juristische Personen sind weder vom Schutzbereich der EU Datenschutz-Grundverordnung noch vom Datenschutz Anpassungsgesetz 2018 erfasst. Der Anwendungsbereich erfasst gemäß Artikel 1 Abs 1 DSG-VO lediglich Vorschriften zum Schutz natürlicher Personen bei Datenverarbeitungsvorgängen.

Grundsätzlich ist die DSG-VO auf den EU Raum begrenzt, allerdings ist sie im Falle der Datenspeicherung auf ausländischen Servern, welche außerhalb der Grenzen der europäischen Union stationiert sind, anwendbar.

3. Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten

Die Frage, was unter dem Begriff "personenbezogener Datensatz" zu verstehen ist, wurde gemäß Art 4 Z 1 DSG-VO dahingehend beantwortet, dass der Datensatz einerseits einen **bestimmten Informationsgehalt über eine individuelle Person** aufweisen muss und andererseits dessen **Zuordnung zum Betroffenen ermöglicht**.

Durch das Inkrafttreten der DSG-VO werden die datenschutzrechtlichen Betroffenenrechte nur geringfügig geändert. Neben den bereits bestehenden Rechten auf Auskunft, Berichtigung, Löschung, Widerspruch, kommt nun das **Recht auf Datenübertragung** des Betroffenen hinzu. Dies bedeutet, dass der Betroffene gemäß Art 20 DSG-VO das Recht hat, seine personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen zu übermitteln.

Darüber hinaus normiert die DSG-VO das "Recht auf Vergessen werden" (Art 17 Abs 3 DSG-VO), wodurch demjenigen, dessen Daten verarbeitet wurden – unter bestimmten Vorrausetzungen – das Recht auf Löschung zusteht. Die Frist, innerhalb derer auf die entsprechenden Anträge reagiert werden muss, beträgt grundsätzlich 4 Wochen, allerdings kann diese im Falle von komplexen Löschungsvorgängen auf 12 Wochen verlängert werden.

Die Voraussetzungen, unter welchen personenbezogene Daten zulässigerweise verarbeitet werden dürfen, regeln die Art 5 ff DSG-VO. So ist die Verarbeitung jedenfalls zulässig, wenn der Betroffene seine Zustimmung dazu erteilt hat oder die Interessen des Betroffenen an der Geheimhaltung, der ihn betreffenden Daten, nicht verletzt werden.

Darüber hinaus ist bemerkenswert, dass es nicht nur in den Verantwortungsbereich des Verarbeitenden fällt, die von ihm geführte Datenverarbeitung datenschutzrechtskonform zu gestalten, sondern auch, dass er deren Einhaltung im Bedarfsfall der Datenschutzbehörde nachweisen können muss.

Besondere Bedeutung hat überdies der sogenannte **Zweckbindungsgrundsatz**, der in Art 6 DSG-VO verankert wurde. Demnach dürfen personenbezogene Daten nur zu dem Zweck verarbeitet werden, zu dem sie tatsächlich erhoben worden sind. Der Zweckbindungsgrundsatz wurde in der DSG-VO allerdings gelockert. Insbesondere Art 6 Abs 4 DSG-VO sieht Ausnahmen vor, die eine Datenverarbeitung zu anderen Zwecken möglich machen.

Besonders sensible (biometrische) Daten dürfen gemäß Art 9 DSG-VO nur unter der Voraussetzung verarbeitet werden, dass die betroffene Person der Verarbeitung ausdrücklich zugestimmt hat bzw. schützenswerte, öffentliche Interessen berührt werden.

4. Zwingende Bestellung eines Datenschutzbeauftragten

Die DSG-VO verpflichtet bestimmte Unternehmen einen eigenen Datenschutzbeauftragten zu bestellen. Zur Bestellung verpflichtet sind insbesondere Unternehmen, bei denen die Verarbeitung von Daten zur Kerntätigkeit gehört bzw. Unternehmen, die Tätigkeiten zum Gegenstand haben, die die umfassende Überwachung von Personen nötig machen. Beispiele für solche Unternehmen sind Krankenhäuser, Versicherungen, Banken sowie Telefon- und Internetanbieter. Vor diesem Hintergrund sollte jedes Unternehmen prüfen, ob es verpflichtet ist, einen Datenschutzbeauftragen zu bestellen. Ebenso kann aber auch freiwillig ein Datenschutzbeauftragter bestellt werden.

Dieser Datenschutzbeauftragte hat einerseits Mitarbeiter und Vorgesetzte über die Regelungen der DSG-VO aufzuklären und andererseits die Einhaltung der DSG-VO im Unternehmen regelmäßig zu prüfen. Der Datenschutzbeauftragte nimmt diese Aufgaben weisungsfrei wahr, alle Ressourcen zur Verfügung zu stellen, die zur ordnungsgemäßen Erfüllung dieser Aufgaben notwendig sind.

Zum Datenschutzbeauftragten können sowohl Mitarbeiter als auch externe Personen bestellt werden.

5. Datenschutz-Folgenabschätzung

Darüber hinaus normiert Art 35 DSG-VO die zwingende Erstellung einer Datenschutz-Folgenabschätzung, sofern die Verwendung von Daten ein hohes Risiko für persönliche Rechte und Freiheiten betroffener Personen darstellt.

Die Abschätzung der Folgen hat insbesondere bei Fällen des sog. Profiling (automatisierte Mustererkennung) zu erfolgen, aber auch bei der Verarbeitung sensibler Daten oder weiträumiger, systematischer Überwachung (Ton, Video) öffentlich zugänglicher Bereiche.

Der Mindestinhalt einer solchen Datenschutz-Folgenabschätzung umfasst eine systemische Beschreibung der Verarbeitungsvorgänge, die Abschätzung der Notwendigkeit der Verarbeitung, die Einschätzung der Risiken, die durch den Verarbeitungsprozess entstehen, sowie geeignete Abhilfemaßnahmen zum Schutz personenbezogener Daten.

6. Verzeichnis von Verarbeitungstätigkeiten – Verfahrensverzeichnis

Um Transparenz in Bezug auf den Datenschutz zu schaffen, verpflichtet die DSG-VO Unternehmen mit mehr als 50 Mitarbeitern, künftig zur Führung eines Verzeichnisses aller im Unternehmen durchgeführter Datenverarbeitungstätigkeiten. Unternehmen mit weniger als 50 Mitarbeitern sind allerdings verpflichtet, trotzdem ein solches Verzeichnis zu führen, sofern ein Risiko für die Rechte und Freiheiten betroffener Personen besteht oder besonders sensible Daten – beispielsweise Daten über strafrechtliche Verurteilungen – verarbeitet werden.

Ebenso wie die Datenschutz-Folgenabschätzung, ist für das Verfahrensverzeichnis ein gewisser Mindestinhalt vorgeschrieben, insbesondere die Kontaktdaten des oder der Verantwortlichen bzw. des Datenschutzbeauftragten. Weiters müssen Angaben zur Kategorie der personenbezogenen Daten und zum Zweck der Verarbeitung festgehalten werden.

Jeder Verarbeitungsvorgang ist in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann. Verstöße gegen diese Dokumentationspflichten werden von Mitgliedstaat zu Mitgliedstaat unterschiedlich sanktioniert, da es gemäß Art 84 DSG-VO den einzelnen Mitgliedstaaten überlassen ist, die Höhe zu bestimmen. Aus diesem Grund sollte bereits vor dem Inkrafttreten der DSG-VO Vorsorge getroffen werden, dass die Dokumentationspflichten eingehalten werden und die notwendigen Informationen dafür zur gegebenen Zeit, für die Erstellung des Verzeichnisses, entsprechend verfügbar sind.

7. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Die DSG-VO normiert, dass bereits bei der Verarbeitungsvorbereitung, beispielsweise bei der Auswahl von Datenverarbeitungsprogrammen, in punkto Datenschutz vorgesorgt werden muss (Stichwort "privacy by design"). Außerdem sind vorab Voreinstellungskonfigurationen, zu wählen, die den Anforderungen der DSG-VO bestmöglich gerecht werden können

(Stichwort "privacy by default"). Maßstab hierfür sind der Stand der Technik, die Höhe des Risikos und der Umfang, in dem Daten verarbeitet werden.

Geeignete Maßnahmen sind beispielsweise Datenminimierung, Pseudoanonymisierung, Anonymisierung, sowie Sammlung von aussagekräftigen Daten, die Rückschlüsse auf die Datenverarbeitungsvorgänge ermöglichen und dazu beitragen den Datenschutz im Unternehmen zu verbessern.

8. Sanktionen bei Verstößen

Im Vergleich zu den Strafen des DSG 2000 sieht die DSG-VO erhebliche Strafverschärfungen vor. Die Geldstrafen reichen bis zu einer Höhe von EUR 20 Mio. oder können bis zu 4 % des gesamten Vorjahresumsatzes betragen.

9. Fazit

Die neugeschaffene Rechtslage (EU-DSG-VO und Datenschutzanpassungsgesetz 2018) stellt Unternehmen vor unterschiedlichste Herausforderungen. Die Einhaltung der Datenschutzbestimmungen wird künftig wesentlich umfassender geprüft werden und kann bei Verstößen zu bemerkenswert hohen Verwaltungsstrafen führen. Vor diesem Hintergrund sollte sich jedes Unternehmen möglichst rasch mit der nach zukünftiger Rechtslage rechtmäßigen Verarbeitung von personenbezogenen Daten auseinandersetzen und eine Prüfung durchführen, ob Anpassungsmaßnahmen im Unternehmen notwendig werden, um einerseits die verstärkten Rechte der Betroffenen und Pflichten des Verantwortlichen zu wahren und andererseits um möglicherweise gravierenden Strafen vorzubeugen.

RA Mag. Reinhard Kollros
RAA Mag. Christoph Sailer