EU-Datenschutz-Grundverordnung

Überblick über die neuen EU-Datenschutzbestimmungen

Ziel der Europäischen Datenschutz-Grundverordnung (DSGVO) ist es, das Recht der Verwendung personenbezogener Informationen (Daten) zu vereinheitlichen und ein unionsweit einheitliches Datenschutzniveau herzustellen.
Die DSGVO wird ab 25. Mai 2018 in allen Mitliedstaaten direkt anwendbar sein, sie lässt jedoch dem nationalen Gesetzgeber gewisse Spielräume offen, sodass sich die konkrete Rechtslage erst durch die Adaptierung des österreichischen Datenschutzgesetzes 2000 ergeben wird. Alle Datenanwendungen müssen an die neue Rechtslage angepasst werden.

Die DSGVO betrifft alle Unternehmer, die personenbezogene Daten natürlicher Personen erfassen oder verarbeiten. Die Unternehmer erhalten mehr Eigenverantwortung bei der Datenverarbeitung und damit zahlreiche neue Pflichten, die sie selbständig in ihren Organisationen umsetzen müssen.
Verstöße dagegen können drastische Strafen zur Folge haben: Je nach Art des Verstoßes können Unternehmen künftig mit Bußgeldern bis zu 20 Mio. Euro bzw. bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres belegt werden.

Zulässigkeit der Datenverarbeitung

Die EU-DSGVO wird als Verbotsgesetz mit Erlaubnisvorbehalt ausgestaltet. Das bedeutet, dass die Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn eine Einwilligung des Betroffenen vorliegt, wenn die Verarbeitung für die Erfüllung eines Vertrages nötig ist oder wenn die DSVGO oder eine andere gesetzliche Vorschrift dies erlauben. Die Mitgliedstaaten können spezifischere Regelungen treffen.

Bedingungen für die Einwilligung

Beruht die Datenverarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass der Betroffene zugestimmt hat.

Die Einwilligung muss durch eine **eindeutige bestätigende Handlung** erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Stillschweigen oder Untätigkeit stellen keine Einwilligung dar. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig.
Die Verarbeitung **sensibler** Daten ist nur bei **ausdrücklicher** Einwilligung erlaubt.

Wichtige Neuerungen für Unternehmer:

Eine Meldepflicht bei der Datenschutzbehörde (Datenverarbeitungsregister) wird es nicht mehr geben. Stattdessen wird den datenschutzrechtlichen „Verantwortlichen“, also jenen Personen oder Stellen, die über die Verarbeitung von personenbezogenen Daten entscheiden (derzeit „Auftraggeber“) mehr Eigenverantwortung übertragen. Die Verantwortlichen sind für den gesamten Datenverarbeitungsvorgang verantwortlich und müssen auch den Nachweis erbringen können, dass sämtliche Pflichten erfüllt werden.

Auch den „Auftragsverarbeitern“, also jenen Personen oder Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten (derzeit „Dienstleister“), werden weitreichende Pflichten bei der Datenverarbeitung auferlegt.

- **Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen**

  Bei **Data protection by design** (Datenschutz durch Technik) sollen Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden. Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen (zB Pseudonymisierung) zu treffen, damit die Verarbeitung den Anforderungen der Verordnung genügt und die Rechte der betroffenen Personen geschützt werden.

  Bei **Data protection by default** (datenschutzfreundliche Einstellungen) sollen IT-Systeme datenschutzfreundlich voreingestellt sein, so dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind. Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen. Hintergrund dieser Regelung ist, dass viele Nutzer nicht über ausreichende IT Kenntnisse verfügen und somit keine Einstellungen zum Schutz ihrer personenbezogenen Daten vornehmen können.

  Adressat dieser Vorschrift sind nicht nur Verantwortliche sondern auch die Entwickler von IT-Systemen und Produkten.

  Die Missachtung der Verpflichtung zu Datensicherheitsmaßnahmen sowie zu Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen ist mit bis zu 10 Mio Euro oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

- **Verfahrensverzeichnis statt Datenverarbeitungsregister**

  Nach derzeitiger Rechtslage gemäß dem österr. Datenschutzgesetz muss grundsätzlich jede Datenanwendung bei der Datenschutzbehörde gemeldet werden. Die DSGVO sieht ein anderes Konzept vor, nämlich die **Führung eines „Verzeichnisses aller Verarbeitungstätigkeiten“ durch Verantwortliche und Auftragsverarbeiter**.
  In diesem Verzeichnis sind sämtliche Verarbeitungstätigkeiten anzuführen. Anzugeben sind darin insbesondere die Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung, eine Beschreibung der Datenkategorien und der Empfängerkategorien, weiters separat ausgewiesen Datentransfers in Drittstaaten und, soweit möglich, die geplante Speicherdauer sowie eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.
  Bis auf die Angabe der Speicherdauer entspricht das Verfahrensverzeichnis dem Inhalt der bisherigen DVR-Meldungen. Neu ist, dass die Verpflichtung zur Führung eines Verfahrensverzeichnisses nicht nur Verantwortliche, sondern auch Auftragsverarbeiter trifft.

  Erleichterungen gibt es für **Unternehmen, die weniger als 250 Arbeitnehmer beschäftigen.** Solche Unternehmen müssen nicht verpflichtend ein Verfahrensverzeichnis führen, es sei denn, bei der vorgenommenen Verarbeitung besteht ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es werden sensible Daten verarbeitet.

  Die Verletzung der Dokumentationspflicht ist mit bis zu 10 Mio. Euro oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

- **Melde- und Dokumentationspflichten bei Datenschutzverletzungen**

  Die im österr. Datenschutzgesetz bestehende Informationspflicht im Falle einer Verletzung des Schutzes personenbezogener Daten wird durch die DSGVO europaweit eingeführt. Schon jetzt sind Unternehmen verpflichtet, Betroffene umgehend zu informieren, wenn ein Datenmissbrauch erfolgt ist und den Betroffenen ein Schaden droht. Nach der DS-GVO muss der Verantwortliche zusätzlich binnen 72 Stunden **an die zuständige Aufsichtsbehörde (Datenschutzbehörde) Meldung erstatten**, außer die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen.

  Daneben bestehen **Dokumentationspflichten**. Die Dokumentation muss der Aufsichtsbehörde eine Überprüfung der Einhaltung der Meldepflicht ermöglichen. Sie muss unter anderem die Verletzungen, Auswirkungen und ergriffenen Abhilfemaßnahmen umfassen.

  Bei Verstößen gegen diese Melde- und Benachrichtigungspflicht drohen Geldbußen von bis zu 10 Mio. Euro oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres.

- **Verpflichtende Datenschutz-Folgenabschätzung**

  Meldungen an das Datenverarbeitungsregister (und auch die DVR-Nummern) gehören nach der DSGVO der Vergangenheit an. Anstelle der Überprüfung der Datenanwendungen bei der Datenschutzbehörde werden Verantwortliche verpflichtet, selbstverantwortlich eine Datenschutz-Folgenabschätzung durchzuführen.

  Die DSGVO bestimmt, dass eine Datenschutz-Folgenabschätzung dann zu erfolgen hat, wenn die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge hat. **Generelle Ausnahmen für KMU bestehen hier nicht.**

  Die Verpflichtung besteht vor allem im Fall einer systematischen und extensiven Auswertung von persönlichen Aspekten, insbes. durch **Profiling**, welche rechtliche Konsequenzen für die Betroffenen haben kann, und bei einer Verarbeitung von **sensiblen Daten**.
  Die DSGVO sieht vor, dass die nationalen Aufsichtsbehörden eine Liste mit jenen Verarbeitungsvorgängen veröffentlichen, für die eine Folgenabschätzung durchzuführen ist.

  Die Folgenabschätzung hat gewisse Mindestinhalte zu umfassen, z.B. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke derselben, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck, sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen.

  Vorherige Konsultation

  Sollte auf Basis der Datenschutz-Folgenabschätzung ein **hohes Risiko** für die Rechte und Freiheiten der betroffenen Person festgestellt werden und kann der Verantwortliche **keine Maßnahmen zur Eindämmung** des Risikos treffen, hat er vor der Verarbeitung die Datenschutzbehörde zu konsultieren. Diese kann dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraumes von bis zu 8 Wochen nach Erhalt des Konsultationsersuchens schriftliche Empfehlungen erteilen.

  Die Missachtung der Verpflichtung zur Datenschutz-Folgenabschätzung und zur vorherigen Konsultation ist mit bis zu 10 Mio. Euro oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

- **Datenschutzbeauftragter**

  Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht für Verantwortliche und Auftragsverarbeiter, wenn

  - die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird,
  - die **Kerntätigkeit** des Verantwortlichen oder Auftragsverarbeiters in Datenverarbeitungen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische **Beobachtung** von betroffenen Personen erforderlich machen, oder
  - die **Kerntätigkeit** des Verantwortlichen oder Auftragsverarbeiters in der umfangreichen Verarbeitung von **sensiblen Daten** oder strafrechtlich relevanten Daten besteht.

  Unternehmen, welche nur in einer untergeordneten Weise diese Kerntätigkeiten durchführen, sind nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen. Erfasst werden v.a. jene Unternehmen sein, welche Profiling durchführen.

  Die Hauptaufgaben des Datenschutzbeauftragten umfassen unter anderem die Beratung des Verantwortlichen bzw. des Auftragsverarbeiters und der Beschäftigten über ihre Pflichten, die Überwachung der Einhaltung der DSGVO, die Beratung bei der Datenschutz-Folgenabschätzung und die Überwachung ihrer Durchführung, sowie die Zusammenarbeit mit der Aufsichtsbehörde (Datenschutzbehörde).

  Die Missachtung der Verpflichtung zur Bestellung eines Datenschutzbeauftragten ist mit bis zu 10 Mio. Euro oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

- **Erweiterte und neue Betroffenenrechte**

  Betroffenenrechte sind die Rechte der von einer Datenanwendung betroffenen Person gegenüber dem Verantwortlichen. Betroffene können sich damit z.B. gegen unrichtige oder unvollständige Datensätze zur Wehr setzen oder verlangen, dass Daten wieder gelöscht werden. Die Betroffenenrechte werden durch die DSGVO deutlich erweitert und umgestaltet.

  So erhält der Verpflichtete erheblich aufwändigere **Informationspflichten** bei der Datenerhebung, beim Erhalt oder dem Weiterleiten von Daten gegenüber den Betroffenen. Ebenso wurden die **Betroffenenrechte** auf Auskunft, Richtigstellung und Löschung erweitert.

  Zum Beispiel wird das „**Recht auf Vergessenwerden**“ eingeführt, wonach jeder Betroffene vom Verantwortlichen verlangen kann, seine Daten unverzüglich zu löschen.

  Vollkommen neu ist das „**Recht auf Datenübertragbarkeit**“. Dieses ermöglicht dem Betroffenen, seine Daten vom Auftraggeber zu verlangen und einem anderen Verantwortlichen zu übermitteln. Dabei hat der Betroffene sogar das Recht, dass die Daten direkt von einem Verantwortlichen auf den anderen übertragen werden.

  Die DSGVO enthält aber auch einige spezifische Besonderheiten für **Träger von Berufsgeheimnissen**, die auch für ZiviltechnikerInnen relevant sein könnten:
  So entfällt beispielsweise die Pflicht, einen Betroffenen über die Verarbeitung seiner personenbezogenen Daten zu informieren, wenn die Daten nicht bei ihm erhoben wurden und diese einem Berufsgeheimnis unterliegen und deshalb vertraulich behandelt werden müssen.

Weiters erlaubt es die DSGVO den Mitgliedstaaten nur zum Zweck der Wahrung von Berufsgeheimnissen in nationalen Rechtvorschriften Ausnahmen dafür vorzusehen, dass die Aufsichtsbehörde Zugang zu personenbezogenen Daten oder zu den Räumlichkeiten des Verantwortlichen hat.

Die Verletzung der Informationspflicht bzw. der Betroffenenrechte ist mit bis zu 20 Mio. Euro oder 4% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

- **Vertrag zwischen Verantwortlichem und Auftragsverarbeiter**

  Wie bisher muss auch nach der DSGVO zwischen dem Verantwortlichen und dem Auftragsverarbeiter ein Vertrag abgeschlossen werden, dessen Mindestinhalt die DSVGO vorgibt.

  Die Nichteinhaltung ist mit bis zu 10 Mio. Euro oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

- **Haftung**

  Betroffene Personen haben neben verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfen auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche und Auftragsverarbeiter im Falle einer Rechtsverletzung.

  Betroffene können auf materiellen oder immateriellen Schadenersatz klagen. Jeder an einer Verarbeitung Beteiligte haftet für den Schaden, den er durch eine unrechtmäßige Verarbeitung verursacht. Die Haftung entfällt nur dann, wenn der Verantwortliche oder Auftragsverarbeiter nachweisen kann, dass er nicht für den Schaden verantwortlich ist.

  Ist mehr als ein Verantwortlicher bzw. Auftragsverarbeiter oder sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt, haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden. Er kann aber bei den übrigen Beteiligten Regress nehmen.

  Die Pflichten des Verantwortlichen bleiben auch bei Bestellung eines Auftragsverarbeiters bestehen.