Was bringt das neue Datenschutzrecht mit 25. Mai 2018?

EU Datenschutz-Grundverordnung und Datenschutzgesetz 2018:

Die europäische **Datenschutz-Grundverordnung (DS-GVO)** ist ab 25. Mai 2018 unmittelbar anwendbar und hebt die DS-RL 95/46/EG auf. Damit soll europaweit ein einheitliches Datenschutzrecht gelten, das einerseits **personenbezogene Daten** schützen und andererseits den freien Datenverkehr sichern soll. Die DS-GVO bedürfte grundsätzlich keines weiteren innerstaatlichen Umsetzungsaktes. Da sie aber zahlreiche „Öffnungsklauseln" für den nationalen Gesetzgeber enthält, wird es neben der DS-GVO weiterhin auch ein **Datenschutzgesetz (DSG)** in Österreich geben.

(Neue) Begriffe:

Personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

Besondere Kategorien personenbezogener Daten (bisher sensible Daten): Daten, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder Gewerkschaftszugehörigkeit hervorgehen sowie Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung, genetische Daten sowie biometrische Daten

Verarbeitung: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang (oder Vorgangsreihe) im Zusammenhang mit personenbezogenen Daten

Dateisystem: jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien geordnet sind

Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

Auftragsverarbeiter (bisher Dienstleister): eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

Anwendungsbereich:

Sachlich: Der sachliche Anwendungsbereich erstreckt sich auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, sowie auf die nichtautomatisierte Verarbeitung personenbezogener Daten, welche in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Örtlich: Neu ist das **Marktortprinzip** – das europäische Datenschutzrecht gilt somit auch für außereuropäische Unternehmen:

- Die DS-GVO ist anwendbar, wenn die Verarbeitung von einem Verantwortlichen vorgenommen wird, der seine **Niederlassung in der EU** hat – und das unabhängig davon, ob die Verarbeitung von personenbezogenen Daten selbst in der EU stattfindet oder nicht.

- Auch wenn ein Unternehmen keine Niederlassung in der EU hat, ist die DSGVO anwendbar und zwar dann, wenn dieses Unternehmen **in der EU aufhältigen** Personen Waren oder Dienstleistungen anbietet oder ihr Verhalten beobachtet und in diesem Zusammenhang deren personenbezogene Daten verarbeitet.

Grundsätze der Datenverarbeitung:

Bei jeder Verarbeitung von personenbezogenen Daten müssen bestimmte Grundsätze eingehalten werden. Diese bestanden im Wesentlichen schon nach der bisherigen DS-RL und dem DSG 2000:

- Die Daten müssen rechtmäßig, nach Treu und Glauben und transparent (nachvollziehbar) für den Betroffenen verarbeitet werden **(Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz).**

- Die Verarbeitung erfolgt für genau festgelegte, eindeutige und legitime Zwecke **(Grundsatz der Zweckbindung).**

- Die Verwendung ist auf das für die Zwecke ihrer Verarbeitung notwendige Maß zu beschränken **(Grundsatz der Datenminimierung).**

- Die Daten müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht werden **(Grundsatz der Richtigkeit).**

- Die Speicherdauer identifizierbarer Personendaten ist auf das unbedingt erforderliche Mindestmaß zu begrenzen. Neu ist, dass **Löschfristen** vorzusehen sind. **(Grundsatz der Speicherbegrenzung).**

- Die Verarbeitung muss Sicherheit und Vertraulichkeit der personenbezogenen Daten gewährleisten, geeignete technische und organisatorische Maßnahmen sind vorzusehen **(Grundsatz der Integrität und Vertraulichkeit).**

Neu ist die sogenannte **Rechenschaftspflicht.** Das bedeutet, dass der Verantwortliche die Einhaltung der Grundsätze nachweisen muss.

Rechtmäßigkeit der Datenverarbeitung:

Jede Verarbeitung personenbezogener Daten muss rechtmäßig sein. Das heißt, es muss ein Erlaubnistatbestand gegeben sein.

Folgende Möglichkeiten bestehen:

- Eine Datenverarbeitung ist grundsätzlich dann rechtmäßig, wenn die **betroffene Person nachweislich ihre Zustimmung** (Einwilligung) gegeben hat.

- Die Datenverarbeitung ist entweder zu Erfüllung einer **vertraglichen Verpflichtung** gegenüber der betroffenen Person oder zur Erfüllung einer **rechtlichen Pflicht** erforderlich.

- Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im **öffentlichen Interesse** liegt oder in **Ausübung öffentlicher Gewalt** erfolgt.

- Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder anderer natürlicher Personen zu schützen.

- Die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten **erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, **überwiegen.**

Die Betroffenenrechte wurden erweitert:

- Betroffene haben ein **Recht auf transparente Information** bei Erhebung bzw Verwendung ihrer Daten.

- Die betroffene Person hat das Recht auf eine Bestätigung, ob sie betreffende personenbezogene Daten verarbeitet werden **(Recht auf Auskunft)**. Eine Kopie der Daten, die Gegenstand der Verarbeitung sind, ist vom Verantwortlichen zur Verfügung zu stellen. Die erste Kopie ist kostenfrei.

- Sind Daten unrichtig oder unvollständig, kann eine unverzügliche Berichtigung oder Vervollständigung verlangt werden **(Recht auf Berichtigung**).

- Wird die Einwilligung einer betroffenen Peron zur Verarbeitung ihrer Daten widerrufen, kann die Löschung dieser Daten verlangt werden **(Recht auf Löschung)**. Dieses Recht besteht auch, wenn die Daten für die Verarbeitungszwecke nicht mehr notwendig sind.

- Verantwortliche haben Betroffene bei der Durchsetzung ihres Löschungsanspruchs gegenüber Dritten stärker zu unterstützen als bisher **(Recht auf Vergessen).**

- Betroffene können die Herausgabe ihrer Daten zudem in einem Format verlangen, das es ihnen ermöglicht, diese Daten bei einem anderen Anbieter weiter zu nutzen **(Recht auf Datenübertragbarkeit)**.

- Ein Widerspruch gegen die Verarbeitung von personenbezogenen Daten kann eingelegt werden, wenn kein berechtigtes Interesse des Verantwortlichen zur Verarbeitung vorliegt oder Daten ohne öffentlichem Interesse zu Forschungs- oder statistischen Zwecken verwendet werden oder Daten zur Direktwerbung verarbeitet werden **(Recht auf Widerspruch)**.

- Die Rechte der Betroffenen wurden auch gestärkt, indem bereits Hersteller und Verantwortliche zu datenschutzfreundlichen Produkten (Prozessen) und Voreinstellungen verpflichtet sind (**Privacy by Design/Privacy by Default**).

Erweiterte Dokumentations- und Nachweispflichten auf Unternehmensebene:

Die Meldung an das Datenverarbeitungsregister (DVR) wird mit 25. Mai 2018 wegfallen. Künftighin müssen die Verantwortlichen selbst die **Einhaltung der Grundsätze** für die Verarbeitung personenbezogener Daten (etwa Rechtmäßigkeit, Zweckbindung, Transparenz oder Datenminimierung) nachweisen. Der Nachweis wird in der Regel durch eine entsprechende Dokumentation erfolgen.

Eigens gefordert wird auch die Dokumentation der getroffenen **technischen und organisatorischen Maßnahmen,** die ein Schutzniveau bieten, das dem mit der beabsichtigten Verarbeitung geschaffenen Risiko für die betroffenen Personen angemessen ist. Diese Maßnahmen schließen auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein.

Verzeichnis von Verarbeitungstätigkeiten

Im Detail geregelt ist zudem die Führung eines **Verzeichnisses von Verarbeitungstätigkeiten.** Dieses hat folgende Informationen zu enthalten:

- Name und Kontaktdaten des Verantwortlichen bzw eines allfälligen Vertreters
- Name und Kontaktdaten des Datenschutzbeauftragen (sofern einer bestellt wurde)
- Zweck(e) der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern
- gegebenenfalls Übermittlungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen

Die Verpflichtung zur Führung eines Verarbeitungsverzeichnisses trifft alle Unternehmen und Einrichtungen, die 250 und mehr MitarbeiterInnen beschäftigen. Unternehmen und Einrichtungen, die weniger als 250 MitarbeiterInnen beschäftigen, müssen ebenfalls ein Verarbeitungsverzeichnis führen, wenn die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt oder die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Kategorien von Daten verarbeitet werden (diese Ausnahme wird in der Praxis nur in wenigen Fällen zutreffen).

Das Verzeichnis ist schriftlich zur führen (allenfalls in einem elektronischen Format) und ist auf Anfrage der Datenschutzbehörde zur Verfügung zu stellen.

Datenschutz-Folgenabschätzung

Hat eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine **Datenschutz-Folgenabschätzung** durchzuführen. Diese ist insbesondere erforderlich, wenn

- eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und diese als Grundlage für automatisierte Entscheidungen dient, die natürliche Personen in erheblicher Weise benachteiligen können (zB Profiling, Bonitätsentscheidungen)
- eine umfangreiche Verarbeitung besonderer Kategorien von Daten (ehemals sensibler Daten) erfolgt oder

- eine systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche erfolgt.

Die Datenschutzbehörde wird eine Liste von Verarbeitungen erstellen, für die jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen ist („schwarze“ Liste) und sie kann auch eine Liste von Verarbeitungen erstellen, für die keine Datenschutz-Folgenabschätzung erforderlich ist („weiße“ Liste).

Bei hohem Risiko besteht eine Pflicht zur **Vorabkonsultation der Datenschutzbehörde**

Verantwortliche müssen daher jederzeit in der Lage sein, die Einhaltung der Vorgaben für die Datenverarbeitungen sowohl in rechtlicher wie in technischer und organisatorischer Sicht **nachweisen** zu können. Eine fehlende Dokumentation kann zu empfindlichen Bußgeldern führen.

Der/die Datenschutzbeauftragte

Die Benennung von Datenschutzbeauftragen ist nun verpflichtend vorgesehen, und zwar bei allen **öffentlichen Stellen** und bei solchen **nicht-öffentlichen Stellen**, bei denen **besonders risikoreiche Datenverarbeitungen** erfolgen. Dies ist der Fall, wenn

- deren Kerntätigkeit eine umfangreiche regelmäßige und systematische Beobachtung der betroffenen Personen erforderlich macht, oder

- wenn deren Kerntätigkeit die Verarbeitung besonderer Kategorien von Daten (vormals sensible Daten) betrifft.

Die Mitgliedstaaten haben zudem die Möglichkeit, eine weitergehende Bestellpflicht einzuführen. Davon wurde im DSG kein Gebrauch gemacht. Den Unternehmen ist es allerdings unbenommen, **freiwillig** eine/n Datenschutzbeauftragte/n zu benennen.

Der/die Datenschutzbeauftragte benötigt eine entsprechende Qualifikation und Fachwissen, er/sie ist in seiner/ihrer Funktion **weisungsfrei**, darf wegen seiner/ihrer Tätigkeit nicht abberufen oder benachteiligt werden und unterliegt einer Verschwiegenheitspflicht.

Die für die betriebliche Ebene **wichtigsten Aufgaben** des/der Datenschutzbeauftragten bestehen darin:

- die Betroffenen zu unterrichten und ihnen Auskunft zu erteilen
- das Einhalten des Datenschutzrechtes zu überwachen (zB die Abhaltung von Schulungen für die MitarbeiterInnen)
- die Verantwortlichen/ die Unternehmensführung zu unterstützen

- der höchsten Managementebene zu berichten

- mit der Behörde zusammenzuarbeiten, insb im Zusammenhang mit der Datenschutz-Folgenabschätzung

Die Datenschutzbehörde (=Aufsichtsbehörde):

Die Datenschutzbehörde (vormals Datenschutzkommission) sorgt für die Einhaltung des Datenschutzes in Österreich. Sie ist bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig **unabhängig** und daher **weisungsfrei** und zur Verschwiegenheit verpflichtet.

Die Datenschutzbehörde hat eine **Vielzahl an Aufgaben**, wesentliche davon sind:

- Überwachung und Durchsetzung der DS-GVO
- Sensibilisierung und Aufklärung der Öffentlichkeit, Sensibilisierung der Verantwortlichen und Auftragsverarbeiter
- Beratung des Parlaments, der Regierung und Gremien
- Befassung mit Beschwerden einer betroffenen Person oder einer sie vertretenden Stelle oder Organisation
- Zusammenarbeit mit anderen Aufsichtsbehörden
- Untersuchungen über die Anwendung dieser Verordnung durchführen, Entwicklungen verfolgen
- Festlegung von Standardvertragsklauseln, Liste der Verarbeitungen erstellen, für die eine Datenschutz-Folgenabschätzung erforderlich ist, Ausarbeitung von Verhaltensregeln fördern, Aufgaben im Zusammenhang mit Zertifizierungsmechanismen usw

Um die Aufgaben erfüllen zu können, werden der Datenschutzbehörde **umfangreiche Befugnisse** eingeräumt. Diese umfassen **Untersuchungsbefugnisse**, wie etwa Einschau in Datenverarbeitungen und Unterlagen, bei der der Verantwortliche bzw Auftragsverarbeiter zur Mitwirkung und Unterstützung verpflichtet ist und sogenannte **Abhilfebefugnisse**. Damit kann die Behörde rechtswidriges Verhalten beenden. Sie kann Warnungen oder Verwarnungen aussprechen, Anweisungen erteilen, rechtswidrige Verarbeitungsvorgänge zu unterlassen oder sogar Verarbeitungen beschränken oder verbieten. Auch **Geldbußen** können verhängt werden. Dazu kommen **Genehmigungsbefugnisse** und **Beratungsbefugnisse**.

Bei **grenzüberschreitenden Fällen** steht den Unternehmen die Datenschutzbehörde an ihrem Hauptsitz als Ansprechpartner zur Verfügung. Betroffene Personen können sich bei Beschwerden an die Datenschutzbehörde ihres Wohnsitzstaates wenden, die den Sachverhalt (wenn er grenzüberschreitend ist) mit den übrigen betroffenen Datenschutzbehörden unter Federführung der Datenschutzbehörde am Hauptsitz des Unternehmens klärt.

Rechtsbehelfe und Sanktionen:

Bei Verletzungen des Datenschutzrechts hat eine betroffene Person **Anspruch auf Unterlassung und Beseitigung des rechtswidrigen Zustands**:

- Dazu kann jede betroffene Person eine **Beschwerde bei der Datenschutzbehörde einbringen**
- **gegen Bescheide der Datenschutzbehörde** und gegen Untätigkeit der Datenschutzsbehörde kann eine Bescheidbeschwerde bzw Säumnisbeschwerde an das Bundesverwaltungsgericht (BVwG) gerichtet werden

- Unklar ist, ob neben der Möglichkeit, eine Beschwerde bei der Datenschutzbehörde einzubringen, jede betroffene Person auch einen **gerichtlichen Rechtsbehelf** ergreifen kann

Betroffene können auch Schadenersatzansprüche geltend machen: Es ist der materielle (erlittene) und immaterielle Schaden (Entschädigung für die erlittene Kränkung) zu ersetzen; zuständig ist das Landesgericht für Zivilrechtssachen in dessen Sprengel der Kläger seinen gewöhnlichen Aufenthalt hat (allenfalls auch am Aufenthaltsort des Beklagten)

Daneben kommt den **Datenschutzbehörden (=Aufsichtsbehörden) auch Strafbefugnis** zu: Je nach Art des Datenverstoßes können **Geldbußen**

- von bis zu Euro 10.000.000,- oder im Falle eines Unternehmens bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (zB bei einem Verstoß gegen die Bestimmungen über die Führung eines Verzeichnisses von Verarbeitungstätigkeiten, die Bestimmungen zur Datenschutz-Folgenabschätzung etc)

- von bis zu Euro 20.000.000,- oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (zB bei einem Verstoß gegen die Grundsätze der Verarbeitung, Rechte der betroffenen Personen, Bestimmungen zur Datenübermittlung an Drittstaaten, Nichtbefolgung von Anweisungen der Datenschutzbehörde etc),

Die Höhe der Geldbuße hängt ua von der Art, Schwere und Dauer des Datenschutzverstoßes und vom Verschulden (Vorsatz, Fahrlässigkeit) ab.

- In Österreich kann die **Datenschutzbehörde** daneben für bestimmte Datenverstöße eine **Verwaltungsstrafe** von bis zu Euro 50.000,- verhängen (zB für das vorsätzliche widerrechtliche Verschaffen eines Zugangs zu einer Datenverarbeitung etc).

Die Datenschutzbehörde soll bei der Anwendung des Strafenkatalogs die "Verhältnismäßigkeit" wahren und so bei erstmaligen Verstößen von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen.

Betriebsrat und Beschäftigtendatenschutz nach Art 88 DS-GVO:

Eine Öffnungsklausel in **Artikel 88 DS-GVO** ermöglicht es den Mitgliedstaaten im Bereich des Beschäftigtendatenschutzes „**spezifischere" Vorschriften** durch eigene Rechtsvorschriften vorzusehen. Daneben kommen diesbezüglich auch Kollektivvereinbarungen, worunter nach Erwägungsgrund 155 auch Betriebsvereinbarungen zu verstehen sind, in Betracht. Derartige Regelungen können für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrages oder der Beendigung des Beschäftigungsverhältnisses getroffen werden.

Hinzuweisen ist, dass **generell die Vorschriften der DS-GVO und des DSG** (zB die allgemeinen Grundätze der Datenverarbeitung, die Zulässigkeit einer konkreten Datenverwendung, die Rechte der betroffenen Personen, weitere datenschutzrechtlichen Verpflichtungen des Verantwortlichen, wie Datensicherheitsmaßnahmen, Geheimnisschutz) selbstverständlich **auch im Arbeitsverhältnis** gelten.

Betriebsrat und Mitwirkungsbefugnisse nach dem ArbVG; § 10 AVRAG

Hervorzuheben sind weiters die Regelungen in **arbeitsrechtlichen Vorschriften, wie etwa die Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG (§§ 89 ff ArbVG)** oder auch **§ 10 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG)**, der den Einsatz von Kontrollmaßnahmen, die die Menschenwürde berühren, in betriebsratslosen Betrieben an die Zustimmung des Arbeitnehmers bindet.

Datenverarbeitungen des Betriebsrates

Die Datenschutz-Grundverordnung ist nicht nur von den Unternehmen anzuwenden, sondern auch von den Betriebsräten zu beachten. Die Arbeitnehmer-VertreterInnen verarbeiten unter Umständen personenbezogene Beschäftigtendaten, die sie aufgrund ihrer Mitwirkungsbefugnisse vom/von der ArbeitgeberIn erhalten und solche, die sie selbst erheben.

Der Betriebsrat hat die **Datensicherheit** und den **Datenschutz** der von ihm verarbeiteten personenbezogenen Beschäftigtendaten sicherzustellen. Die entsprechenden Maßnahmen können technischer und/oder organisatorischer und/oder personeller Art sein.

Empfehlenswert ist auch für den Betriebsrat, ein **Verzeichnis der Verarbeitungstätigkeiten** zu führen. Dies schafft einen Überblick über die Datenverarbeitungen und der verwendeten Datenkategorien im Betriebsratsbüro. Zudem sollten alle Maßnahmen zur Gewährleistung von Datensicherheit und Datenschutz dokumentiert werden.

Rechtsquellen:

Datenschutz-Grundverordnung: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

https://www.dsb.gv.at/recht-auf-datenschutz-in-der-eu

Datenschutz-Anpassungsgesetz 2018: Das Datenschutzgesetz 2000 wird novelliert und auf „Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)“ umbenannt

https://www.dsb.gv.at/gesetze-in-osterreich

Links:

https://www.dsb.gv.at
(Homepage der Datenschutzbehörde)

http://www.forba.at/
(Homepage von FORBA, Forschungs- und Beratungsstelle Arbeitswelt)