GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

DS-GVO Info

Wichtige Änderungen durch das neue Datenschutzrecht mit 25. Mai 2018

Hier gibt es einen Überblick über die wichtigsten Änderungen, die durch die neue Rechtslage zum Datenschutz entstehen. Die fünf wichtigsten Themenbereichen werden zusammengefasst und derzeitige mit zukünftiger Rechtslage gegenübergestellt. (Ausführlichere Informationen bieten euch die attachten Unterlagen und die Sekretärinnen der Abteilung Arbeit & Technik.)

1. Rechtsgrundlagen

1.1. Derzeitige Rechtsgrundlage: europäische Datenschutzrichtlinie 95/46/EG und österreichisches Datenschutzgesetz 2000

Die Datenschutzrichtlinie 95/46/EG ist (noch) die Grundlage für alle nationalen Datenschutz-Gesetze in den EU-Mitgliedsstaaten, also auch des derzeit geltenden österreichischen Datenschutzgesetzes 2000 (DSG 2000). Eine EU-Richtlinie muss immer innerstaatlich umgesetzt werden, jeder Mitgliedstaat hat also sein eigenes Datenschutzrecht geschaffen. In Österreich wurde das damalige Datenschutzgesetz aus dem Jahr 1978 durch das DSG 2000 abgelöst.

Das DSG 2000 regelt alle Aspekte des Datenschutzes, also implizit auch den betrieblichen Datenschutz, obwohl dieser nicht explizit Erwähnung findet.

Für die konkrete betriebliche Umsetzung sind entsprechende Informations-, Beratungs- und Mitbestimmungsrechte des Betriebsrates im Arbeitsverfassungsgesetz festgelegt.

Die Datenschutzrichtlinie 95/46/EG wird durch die Europäische Datenschutz-Grundverordnung (DS-GVO) mit Wirkung 25. Mai 2018 aufgehoben**.** Das DSG 2000 wird mit dem 25. Mai 2018 durch ein neues nationales Datenschutz-Gesetz ersetzt werden (das Datenschutz-Anpassungsgesetz 2018). Das zuständige Bundeskanzleramt hat einen Entwurf erarbeitet, der derzeit im Parlament liegt und auf seine Verabschiedung wartet. (Die Frist zur Stellungnahme endete am 23. Juni 2017. Der ÖGB hat seine – unter reger Beteiligung der GPA-djp erarbeitete – Stellungnahme eingebracht: https://www.parlament.gv.at/PAKT/VHG/XXV/SNME/SNME_12340/imfname_642856.pdf).

1.2. Neue Rechtslage mit 25. Mai 2018: Europäische Datenschutz-Grundverordnung

Mit der DS-GVO kommt es zu einer europaweiten Harmonisierung. Alle Mitgliedstaaten unterliegen damit demselben Datenschutz-Recht (etwa 60 sogenannte Öffnungsklauseln ermöglichen es den Mitgliedsstaaten allerdings, spezifischere Regelungen auf nationaler Ebene zu erlassen). Neu ist, dass durch die DS-GVO das sogenannte „**Marktort-Prinzip**" eingeführt wird. D.h., jede Person, jedes Unternehmen, das auf dem europäischen Marktplatz, also auf EU-Territorium, (Dienst-)Leistungen und Produkte anbietet, muss sich an die DS-GVO halten – unabhängig davon, wo sich der Hauptsitz des Unternehmens befindet.

Wesentliche Grundprinzipien der Datenverarbeitung wie Rechtmäßigkeit, Zweckbindung, Transparenz oder Datenminimierung bleiben erhalten.

2. Transparenzprinzip und Publizitätsprinzip

2.1. Derzeitige Rechtslage: Meldepflicht beim Datenverarbeitungsregister (DVR)

Österreich hat (als einzigem EU-Land) im DSG die Verpflichtung festgelegt, dass Auftraggeber (=Arbeitgeber) DVR-Meldungen erstatten müssen: Prinzipiell muss jeder Auftraggeber jede Anwendung melden. Für die einen stellt die derzeitige Regelung des öffentlich zugänglichen Datenverarbeitungsregisters eine bürokratische Hürde dar, für die anderen ist es eine Möglichkeit, Einsicht zu nehmen und Kenntnis über Datenanwendungen zu erlangen.

Erleichtert wurde die Meldung für vordefinierte Datenverarbeitungen, die in Unternehmen typischerweise vorkommen mittels so genannter „Standard- und Muster-Verordnungen" (z.B. zur Personalverwaltung für privatrechtliche Dienstverhältnisse, Datenübermittlung im Konzern).

Einige wenige Datenanwendungen sind vorabkontrollpflichtig: Das bedeutet, dass sie erst nach ihrer Prüfung durch die Datenschutzbehörde in Betrieb genommen werden dürfen (wie etwa Gesundheitsdaten).

Mit 25. Mai 2018 wird die Verpflichtung zur Erstattung von DVR-Meldungen an die Datenschutzbehörde entfallen, die Standard- und Musterverordnung tritt außer Kraft.

2.2. Neue Rechtslage mit 25. Mai 2018: Verarbeitungsverzeichnis und Datenschutz-Folgenabschätzung

Die Datenanwendungen eines Unternehmens müssen nun in einem „**Verzeichnis von Verarbeitungstätigkeiten**" angeführt werden. Ein solches Verarbeitungsverzeichnis enthält in etwa dasselbe wie vormals die DVR-Meldung (Name, Kontaktdaten, Empfänger, Kategorien, Verarbeitungszwecke, etc). Ergänzend müssen nun auch **Löschfristen** im Verzeichnis („wenn möglich") angeführt werden.

Das Verfahrensverzeichnis muss der Aufsichtsbehörde auf Anfrage vorgezeigt werden.

Ausgenommen sind Unternehmen (in der DS-GVO „Verantwortliche" genannt) mit weniger als 250 Beschäftigten, Unternehmen die keine besonderen Datenkategorien verarbeiten, und Verantwortliche, deren Verarbeitungen kein Risiko für Freiheiten der betroffenen Personen darstellen.

Die Vorabkontrolle durch die Datenschutzbehörde ist nun einer „**Datenschutz-Folgenabschätzung**" gewichen, die das Unternehmen bei großem Risiko durchführen und auf Anfrage der Behörde vorlegen muss. Konkret muss eine solche Prüfung für neue Technologien durchgeführt werden, die

- mit hohem Risiko für die Freiheitsrechte der Betroffenen(z.B. Monitoring von Gesundheitsdaten) einhergehen,
- für umfangreiche Verarbeitungsvorgänge für eine große Zahl von Betroffenen (z.B. Tracking im Verkehr),
- und wenn wesentliche Einzelentscheidungen aufgrund von profiling getroffen werden (z.B. Kreditscoring) oder bei biometrischen Datenverarbeitungen.

3. Sanktionen und Strafen

3.1. Derzeitige Rechtslage: Schadenersatz und Verwaltungsstrafen nach § 52 DSG 2000

Bei Verletzungen des DSG 2000 hat ein Betroffener Anspruch auf Unterlassung und Beseitigung des rechtswidrigen Zustands.

Betroffene können Schadenersatzansprüche geltend machen, wobei der erlittene (materielle) Schaden zu ersetzen ist. Für „besonders schwerwiegende Datenverstöße" kann auch eine angemessene Entschädigung für die erlittene Kränkung (d.h. immaterieller Schadenersatz) gefordert werden. Bei Datenverwendung in Gewinn- und Schädigungsabsicht ist eine Freiheitsstrafe bis zu einem Jahr vorgesehen. Geldstrafen gehen bis zu 25.000,- EUR.

3.2. Neue Rechtslage mit 25. Mai 2018: massive Erhöhung des Strafrahmens

Die Neu-Gestaltung und massive Erhöhung des potentiellen Strafrahmens hat wesentlich dazu beigetragen, dass die DS-GVO derzeit so breite – auch mediale – Beachtung findet. Unternehmen aller Branchen sind auf den Plan gerufen und versuchen, sich auf die DS-GVO vorzubereiten. Warum? Weil (angelehnt an das Europäische Wettbewerbsrecht) nun bis zu 4% des weltweiten Umsatzes oder 20 Mio. EUR als Sanktion verhängt werden können. Diese Strafen drohen bei Verstößen gegen Grundprinzipien der DS-GVO oder Nicht-Befolgung von Auflagen der Behörde.

Bis zu 10 Mio. EUR oder 2 % des weltweiten Umsatzes können bei Verstößen gegen Verfahrensregeln der DS-GVO (z.B. wenn keine Konsultation der Aufsichtsbehörde bei Risiko-Folgenabschätzung erfolgt, Meldung von Verletzungen der DS-GVO unterlassen wurde, datenschutzfreundliche Voreinstellungen fehlen, etc.) als Strafe verhängt werden.

Die konkrete Höhe der Geldbuße (Strafe) richtet sich nach der Schwere und Dauer des Vergehens, den durch das Unternehmen getroffenen Sicherheitsmaßnahmen, der Anzahl der Betroffenen, der Häufigkeit des Vergehens, der Kooperation mit der Aufsichtsbehörde und Ähnlichem. Eine Strafe muss **wirksam, verhältnismäßig und abschreckend** sein.

Verhängt wird die Strafe nun europaweit von der jeweils national zuständigen Aufsichtsbehörde.

4. Datenschutzbeauftragter

4.1. Derzeitige Rechtslage: freiwilliger Datenschutzbeauftragter

Das österreichische DSG 2000 sieht keinen verpflichtenden betrieblichen Datenschutzbeauftragten vor. Die freiwillige Einrichtung ist möglich.

In Deutschland hat ein/e Datenschutzbeauftragte/r allerdings lange Tradition. Die Stelle ist einzurichten sobald zehn oder mehr ArbeitnehmerInnen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Er/Sie ist weisungsfrei und direkt der Geschäftsleitung unterstellt. Er/Sie hat einen besonderen Kündigungsschutz und ArbeitgeberInnen haben Geld und Zeit für die Fortbildung zur Verfügung zu stellen. In kleineren und mittleren Unternehmen in Deutschland

ist es auch üblich, den Datenschutzbeauftragten aus Kosten und Risikogründen extern zu bestellen. Zunehmend werden auch in Österreich - vor allem in größeren Unternehmen - freiwillig betriebliche Datenschutzbeauftragte bestellt.

4.2. Neue Rechtslage mit 25. Mai 2018: verpflichtende/r Datenschutzbeauftragte/r

Ein/e betriebliche/r Datenschutzbeauftragte/r (DSB) muss gemäß der DS-GVO bestellt werden, wenn:

- es sich um eine öffentliche Stelle, eine Behörde, ein Amt handelt
- die Kerntätigkeit des Unternehmens eine umfangreiche regelmäßige und systematische Überwachung ist
- die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten besteht (besondere Kategorien sind: rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person).

Die wichtigsten Aufgaben bestehen darin:

- die Betroffenen zu schulen, zu unterrichten und ihnen Auskunft zu erteilen
- das Einhalten des Datenschutzrechtes zu überwachen,
- die Verantwortlichen/die Unternehmensführung zu unterstützen und der höchsten Managementebene zu berichten,
- mit der Behörde zusammenzuarbeiten, insbes. im Zusammenhang mit der Datenschutz-Folgenabschätzung

Der/die DSB benötigt berufliche Qualifikation und Fachwissen in Datenschutzrecht und Praxis.

DSB arbeitet betriebsintern oder extern aber jedenfalls **vollständig unabhängig** vom Verantwortlichen.

Es reicht aus, einen betrieblichen DSB an der Hauptniederlassung des Konzerns in Europa zu bestellen – vorausgesetzt er/sie kann dort seine/ihre konzernweiten Aufgaben erfüllen (was in der Praxisvermutlich bereits an Sprachbarrieren scheitern wird).

Über die verpflichtenden Fälle hinaus bleibt es Verantwortlichen unbenommen, freiwillig eine/n DSB zu benennen.

5. Beschäftigtendatenschutz

5.1. Derzeitige Rechtslage: kein eigenes Beschäftigtendatenschutzgesetz

In Österreich besteht derzeit kein eigenes Beschäftigtendatenschutzgesetz. Das DSG 2000 enthält keine eigenen zentralen Regelungen zum Beschäftigtendatenschutz.

Das heißt aber nicht, dass die ArbeitnehmerInnen innerhalb ihrer Arbeitsverhältnisse derzeit rechtlos sind. Es gelten generell die Vorschriften des DSG 2000 selbstverständlich auch im Beschäftigtenverhältnis.

Es gibt einzelne wenige spezifische Regelungen des DSG 2000, die auf das Arbeitsverhältnis Bezug nehmen:

- in § 9 Z 11 wird dezidiert darauf hingewiesen, dass „die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse unberührt bleiben", d.h., die Mitwirkungsrechte des Betriebsrates werden durch das DSG 2000 nicht beeinträchtigt
- in § 50a Abs 5 ist die Unzulässigkeit einer Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten festgeschrieben
- im Zusammenhang mit Datensicherheitsmaßnahmen nach § 14 dürfen Protokoll- und Dokumentationsdaten nicht zum Zwecke der MitarbeiterInnenkontrolle weiterverwendet werden

Der Beschäftigtendatenschutz ist in arbeitsrechtlichen Vorschriften geregelt, wie etwa die Mitwirkungsbefugnisse des Betriebsrates nach dem Arbeitsverfassungsgesetz (§§ 89 ff ArbVG). Somit ist der Einsatz von Kontrollmaßnahmen, die die Menschenwürde berühren, mit einem Veto des Betriebsrates versehen. (In betriebsratslosen Betrieben bindet § 10 Arbeitsvertragsrechts-anpassungsgesetz (AVRAG) diese Kontrollmaßnahmen an die Zustimmung des/ der einzelnen Arbeitnehmers/-in.)

5.2. Neue Rechtslage mit 25. Mai 2018: Öffnungsklausel des Art 88 DS-GVO

In Artikel 88 der DS-GVO ist nun die **Datenverarbeitung im Beschäftigungskontext** erstmalig europaweit geregelt. Allerdings muss man zugeben, dass dies auf einem eher allgemeinen Niveau geschieht.

Sollen personenbezogene Daten der Beschäftigten im Arbeitsverhältnis Verwendung finden, müssen sie für „die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses maßgebend sein". Es handelt sich also um eine Konkretisierung der beiden Datenschutzprinzipien der Zweckmäßigkeit und der Rechtmäßigkeit.

Um den europaweit doch sehr unterschiedlichen Regelungen in den industriellen Beziehungen Rechnung zu tragen, wurden nationale **Öffnungsklauseln für Kollektivvereinbarungen** oder eigene nationale Rechtsvorschriften eingeführt. Im Erwägungsgrund 155 ist die Möglichkeit festgeschrieben, dass Kollektivverträge und Betriebsvereinbarungen beschlossenen werden können

um den betrieblichen Datenschutz zu regeln. Derartige kollektive Rechtsvorschriften *können* sich beziehen auf:

- Einstellung
- Erfüllung des Arbeitsvertrags
- Planung und Organisation der Arbeit
- Pflichten des Managements
- Gleichheit und Diversität am Arbeitsplatz
- Gesundheit und Sicherheit am Arbeitsplatz
- Schutz des Eigentums der ArbeitgeberInnen/der KundInnen
- Beendigung des Beschäftigungsverhältnisses

Der europäische Gesetzgeber weist also ausdrücklich auf die Möglichkeit hin, kollektive Rechtsakte zu setzen.