Kap 3 Geltungsbereich der DSGVO

3.1 Sachlicher Geltungsbereich

Die DSGVO gilt gem Art 2 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Der Fokus liegt somit in elektronisch verarbeiteten Daten; allerdings fallen auch manuell (idR also in Papierform) verarbeitete Daten darunter, wenn diese in einer strukturierten Sammlung vorliegen, die nach bestimmten Kriterien zugänglich sind. Einzelne Papierakten sind jedoch nicht als Dateisystem zu subsumieren.

Hinweis

Eine nach Namen geordnete Verwaltung von Personalakten in Papierform wird die Kriterien eines Dateisystems erfüllen. Die DSGVO ist somit anwendbar.

Personenbezogene Daten sind all jene Informationen, die sich auf eine identifizierte Person oder identifizierbare Person beziehen. Die Identifizierbarkeit ist objektiv zu beurteilen, dh es ist nicht rein auf die rechtliche oder faktische Möglichkeit des Verantwortlichen abzustellen, sondern auch die Möglichkeiten Dritter zu berücksichtigen. Daher ergibt sich ein durchaus breiter Auslegungsbereich der Identifizierbarkeit.

Beispiel:

Informationen, die zur Identifizierbarkeit von Personen führen: Name, Adresse, Geburtsdatum, Mitarbeiternummer, Sozialversicherungsnummer, Steuernummer, Bankkonto, Standorte, Kfz-Kennzeichen, IP-Adresse

Auch der Begriff der Verarbeitung ist weit auszulegen, weshalb sich ein breiter sachlicher Anwendungsbereich der DSGVO ergibt.

Beispiel:

Unter die Verarbeitung von Daten fällt: Erheben, Speichern, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Löschen, Einschränken, Vernichten.

Keine Anwendung findet die DSGVO, wenn die Verarbeitung der personenbezogenen Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt („Household Exemption“).

Hinweis

Die private Nutzung sozialer Netzwerke oder die Erfassung von Kontaktdaten am privaten Handy fallen aufgrund des privaten Anwendungsbereichs nicht unter die DSGVO.

3.2 Persönlicher Geltungsbereich

Verbindliche Vorschriften schafft die DSGVO für Verantwortliche und Auftragsverarbeiter. Diese sind daher als Normadressaten der DSGVO zu sehen. Die Abgrenzung der beiden Gruppen ist wie folgt vorzunehmen:

- Verantwortlicher: Person/Einheit, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- Auftragsverarbeiter: Person/Einheit, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Die Regelungen und Verantwortungen sind auf die beiden Gruppen im Einzelfall abgestuft ausgestaltet. Gesamt gesehen kommt es aber zur Annäherung der beiden Gruppen.

Ein in der Praxis wichtiger Punkt ist auch das Zusammenspiel der beiden. Rechte und Pflichte von Auftragsverarbeiter und Verantwortlichen sind gem Art 28 Abs 9 DSGVO zwingend in einem schriftlichen

Kap 4 Grundsätze der Verarbeitung personenbezogener Daten

Damit personenbezogene Daten iSd DSGVO korrekt verarbeitet werden und für die Betroffenen das nötige Schutzniveau sichergestellt ist, müssen vom Verantwortlichen bzw Auftragsverarbeiter die Grundsätze für die Verarbeitung personenbezogener Daten gem Art 5 DSGVO eingehalten werden.

Wichtig ist in diesem Zusammenhang, dass die Einhaltung ebendieser Grundsätze vom Verantwortlichen bzw Auftragsverarbeiter nachzuweisen ist (Rechenschaftspflicht). Dieses Prinzip der Selbstverantwortung des Verantwortlichen bzw Auftragsverarbeiters zieht sich wie ein roter Faden durch die DSGVO und ist als Paradigmenwechsel gegenüber der bisherigen Praxis des DSG 2000 zu sehen.

4.1 Rechtmäßigkeit

Wie bereits mehrfach erläutert, stellt der Schutz der Verarbeitung personenbezogener Daten ein Grundrecht dar. Demnach ist das Datenschutzgesetz als Verbotsgesetz zu verstehen, welches die Verarbeitung personenbezogener Daten grundsätzlich untersagt.

Diesem Grundgedanken folgend, darf eine Datenverarbeitung nur dann vorgenommen werden, wenn eine entsprechende Rechtsgrundlage dafür vorliegt. Nur dann kann von einer rechtmäßigen Datenverarbeitung ausgegangen werden.

Welche rechtlichen Maßnahmen nötig sind, um den Grundsatz der Rechtmäßigkeit zu erfüllen, wird ausführlich im Kapitel 5 „Rechtmäßigkeit der Datenverarbeitung“ dargestellt.

4.2 Treu und Glauben

Der Grundsatz von „Treu und Glauben“ wird innerhalb der DSGVO nicht näher definiert. In einer Gesamtbetrachtung wird er aber wohl als Auffangklausel zu sehen sein. Inhaltlich setzt Datenverarbei-

Kap 5 Rechtmäßigkeit der Datenverarbeitung

Ein wesentlicher Grundsatz nach der DSGVO besagt, dass rechtmäßige Datenverarbeitung auf einer zulässigen Rechtsgrundlage basieren muss. Für den Betroffenen muss klar und nachvollziehbar sein, wer seine Daten verarbeitet und auf welcher (Rechts-)Grundlage die Datenverarbeitung erfolgt.

Die Rechtsgrundlage für die Datenverarbeitung steckt dabei den Rahmen ab, in dem sich eine zulässige Datenverarbeitung in der Regel bewegen darf. Der Umfang der zu einem rechtmäßigen Zweck erhobenen Daten muss in einem angemessenen Verhältnis zum Erhebungszweck stehen, wobei Geheimhaltung und Sicherheit der Daten gewährleistet sein muss. Nachdem die erhobenen Daten ihren Zweck erfüllt haben, sind sie wieder zu löschen.

Beispiel:

Typischer Anwendungsfall ist der Unternehmer, der mit seinem Kunden (Verbraucher) einen Vertrag abschließt und gegen Entgelt eine bestimmte Leistung erbringen muss. Bei der Erfüllung seiner Leistungsverpflichtung muss der Unternehmer oftmals auf Daten zurückgreifen, die er bei seinem Kunden erhebt. Abgesehen von der Erfüllung des Vertrages gegenüber dem Kunden darf der Unternehmer erhobene Daten nur innerhalb der gesetzlich zulässigen Grenzen weiterverarbeiten. Je nach Art der erbrachten Leistung ist der Unternehmer früher oder später angehalten, zweckentsprechend erhobene Daten wieder zu löschen.

Rechtmäßige Datenverarbeitung knüpft an folgende Erlaubnistatbestände nach Art 6 Abs 1 lit a bis f DSGVO:

- Einwilligung der betroffenen Person;
- Vertrag/vorvertragliche Maßnahmen auf Anfrage;
- rechtliche Verpflichtung des Verantwortlichen;

Kap 6 Rechte der betroffenen Personen

Um die in Kapitel 4 dargestellten Grundsätze der Datenverarbeitung für die Betroffenen prüfbar zu machen und um deren Durchsetzbarkeit sicherzustellen, normiert die DSGVO in den Art 15ff die folgenden Betroffenenrechte:

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch

Ergänzt wird dieser Abschnitt der DSGVO durch die Informationspflicht der Verantwortlichen gegenüber den Betroffenen. In der Praxis wird die Informationspflicht oftmals den Betroffenenrechten zugeordnet, obwohl es sich hier eigentlich um eine aktive Verpflichtung des Verantwortlichen handelt; es braucht daher – anders als bei den echten Betroffenenrechten – keine Initiierung durch den Betroffenen.

Hinweis

Angaben zur Informationspflicht und den Betroffenenrechten sind vom Verantwortlichen in präziser, transparenter, verständlicher und leicht zugänglicher Form und Sprache zu machen.

Generell gültig für sämtliche Betroffenenrechte sind folgende Punkte:

- Übermittlung der Informationen erfolgt grundsätzlich schriftlich (gegebenenfalls auch elektronisch);
- falls vom Betroffenen gewollt, kann die Information auch mündlich erfolgen (Identitätsnachweis erforderlich);
- Informationen werden grundsätzlich unverzüglich zur Verfügung gestellt; in jedem Fall allerdings innerhalb eines Monats;

Kap 7 Datenschutzbeauftragte

Der Datenschutzbeauftragte stellt eine wesentliche Neuerung der DSGVO dar, da es diese Rechtsfigur in Österreich bisher nicht gab.

Zwar gab es schon bisher in Behörden und Unternehmen oftmals Personen, die sich mit der Einhaltung des Datenschutzes auseinandergesetzt haben, allerdings waren die Ausprägungen aufgrund der fehlenden gesetzlichen Vorgaben bisher durchaus unterschiedlich. Zukünftig wird sich durch die DSGVO ein klares Rollenbild entwickeln.

7.1 Notwendigkeit der Bestellung

Bei der Frage der gesetzlichen Notwendigkeit einen Datenschutzbeauftragen gem Art 37 DSGVO zu bestellen, ist zwischen

- Behörden und öffentlichen Stellen sowie
- privatrechtlichen Unternehmen

zu unterscheiden.

7.1.1 Behörde und öffentliche Stelle

Behörden und öffentliche Stellen haben stets einen Datenschutzbeauftragten zu bestellen, wenn von ihnen eine Verarbeitung von personenbezogenen Daten durchgeführt wird. Ausgenommen sind lediglich Gerichte, die im Rahmen ihrer justiziellen Tätigkeiten handeln.

Problematisch ist es in diesem Zusammenhang, dass die DSGVO selbst nicht definiert, was unter Behörden und öffentlichen Stellen zu verstehen ist. Insbesondere die Abgrenzung der „öffentlichen Stelle“ erscheint hier problematisch.

Gemessen am Zweck der DSGVO erscheint es zweckmäßig, die Begriffe in Anlehnung an den Begriff des „öffentlichen Auftraggebers“ nach Art 2 Abs 1 Z 1 Richtlinie 2014/24/EU zu definieren.

Kap 8 Verarbeitungsverzeichnis

Mit Art 30 normiert die DSGVO die Pflicht, dass der Verantwortliche (sowie in etwas anderer Form auch der Auftragsverarbeiter) ein internes Verzeichnis der seiner Zuständigkeit unterliegenden Verarbeitungstätigkeiten führen muss. Dieses Erfordernis der internen Verzeichnisführung ist in Österreich neu. Nach bisherigem Recht gab es nur die (externe) DVR-Meldepflicht an die Datenschutzbehörde. Allerdings wurde diese Meldepflicht aufgrund der Erleichterungen der Standard- und Musterverordnung 2004 in der Praxis stark ausgehöhlt. Denn dadurch ergab sich die Situation, dass im Falle der Nutzung der in der Verordnung genannten Standardanwendungen die Meldepflicht unterbleiben konnte.

Somit ergeben sich durch die DSGVO gegenüber der bisherigen Rechtslage zwei wesentliche Neuerungen:

- Das Verarbeitungsverzeichnis ist vom Verantwortlichen bzw Auftragsverarbeiter intern zu erstellen; die externe Meldepflicht an die Datenschutzbehörde entfällt.
- Die Erleichterungen aus der Standard- und Musterverordnung 2004 fallen weg; im Verarbeitungsverzeichnis sind sämtliche Verarbeitungstätigkeiten (auch Standardanwendungen) zu führen.

Inhaltlich kann das Verarbeitungsverzeichnis als Inventar aller Verarbeitungsvorgänge in der Zuständigkeit der Verantwortlichen bzw Auftragsgebers verstanden werden. Es soll einen Überblick über die Verarbeitungstätigkeiten der Einheit geben und wird in dieser Funktion sowohl intern als auch extern für die Aufsichtsbehörde als erste Informationsquelle dienen. Dieser „externe Empfängerhorizont“ ist in den Erwägungsgründen zur DSGVO auch explizit verankert und sollte daher bei der Erstellung mitbedacht werden.

Das Verzeichnis ist aufgrund des Nachweischarakters in schriftlicher Form zu führen. Nähere Vorschriften dazu gibt es nicht. Demnach erscheinen für eine überschaubare Menge an Verarbeitungstätigkeiten

Kap 9 Datenschutz-Folgenabschätzung

9.1 Notwendigkeit der Durchführung

Ziel der Datenschutz-Folgenabschätzung gem Art 35 DSGVO ist, sich vor der Aufnahme einer Verarbeitungstätigkeit, die hohe Risiken für die Rechte und Freiheiten der betroffenen Personen hat, mit dessen Auswirkungen auf die Betroffenen auseinanderzusetzen und entsprechende Datenschutzmaßnahmen zu treffen.

Demnach muss der Verantwortliche vorab das Risiko evaluieren, welches sich aufgrund der Art, des Umfangs, der Umstände sowie der Zwecke der Verarbeitung ergibt. Die DSGVO nennt die folgenden Fälle, in denen insbesondere eine Datenschutz-Folgenabschätzung nötig ist:

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für die Entscheidungen dient, die Rechtswirkung gegenüber Personen entfaltet oder diese in ähnlicher Weise beeinträchtigt.
- Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gem Art 9 oder von personenbezogenen Daten über Straftaten gem Art 10.
- Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Konkrete Beispiele dazu sind in der DSGVO nicht genannt, allerdings wurde von der Datenschutzbehörde angekündigt, sowohl eine „White-List“ als auch eine „Black-List“ an Verarbeitungen herauszugeben, für die keine bzw eine zwingende Datenschutzfolgenabschätzung nötig ist.

Wie eingangs erwähnt, hat die Datenschutz-Folgenabschätzung vorab – also vor Aufnahme einer Verarbeitungstätigkeit – zu erfolgen und zielt damit bereits auf die Konzeptphase ab. Umgelegt auf die derzeitige Situation der erstmaligen Anwendung die-

Kap 10 Datenschutz durch technische Maßnahmen

Um die datenschutzrechtlichen Ziele zu erreichen, normiert die DSGVO auch direkte technische Aspekte. Dies sind einerseits Maßnahmen zur Datensicherheit gem Art 32 sowie zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen („Privacy by Design" & „Privacy by Default").

10.1 Datensicherheit

Verantwortliche und Auftragsverarbeiter müssen technische und organisatorische Maßnahmen treffen, um die Sicherheit der Datenverarbeitung gewährleisten zu können. Sicherheit bezieht sich in diesem Zusammenhang auf die folgenden drei Ziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Welche Maßnahmen der Verantwortliche bzw Auftragsverarbeiter ergreifen muss, hängt sowohl vom Risiko für die betroffenen Personen als auch von den Implementierungskosten ab. Wie so oft in der DSGVO kommt es auch hier zu einer Abwägung zwischen den Interessen der Betroffenen und des Verantwortlichen bzw Auftragsverarbeiters.

Als Beispiele für Sicherheitsmaßnahmen nennt die DSGVO:

- Pseudonymisierung und Verschlüsselung von personenbezogenen Daten
- Maßnahmen zur Sicherung der IT-Systeme
- Backup- und Restore-Maßnahmen bis hin zur Wiederherstellung des Betriebs im Desasterfall („Business Continuity Management")
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

In der Praxis haben sich über die Jahre unabhängige Standards entwickelt, welche IT-Sicherheit normie-

ren. Aufgrund dieser Standards ist es auch möglich, Zertifizierungen von Unternehmen im Bereich der IT-Sicherheit durchzuführen. Insbesondere im Bereich der Auftragsverarbeiter werden künftig Zertifizierungen immer mehr an Bedeutung gewinnen, da es diese dem Verantwortlichen erleichtern, eine Beurteilung über die Befähigung des Auftragsverarbeiters abzugeben.

Einige internationale Beispiele dafür sind:

- ISO/IEC 27001: Information technology – Security techniques: Information security management systems – Requirements
- ISO/IEC 27002: Information technology – Security techniques: Code of practice for information security controls
- Critical Security Controls for Effective Cyber Defense (CIS): Vielzahl von Standards vorhanden, ua priorisierte Liste der 20 wichtigsten Sicherheitsmaßnahmen
- IT-Grundschutz des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI): umfassender Katalog zu Sicherheitsmaßnahmen

10.2 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Im Unterschied zu den allgemeinen Maßnahmen zur Datensicherheit verfolgen diese Maßnahmen insbesondere das Ziel, die Rechtmäßigkeit der Datenverarbeitung zu gewährleisten und datenschutzrechtliche Risiken ieS zu vermindern.

Datenschutz durch Technik („Privacy by Design“) erfordert, dass technische Maßnahmen implementiert werden, damit die Datenschutzgrundsätze erfüllt werden können. Die DSGVO nennt hier die Pseudonymisierung als explizites Beispiel.

Andere praktische Anwendungsfälle wären:

- Technische Umsetzung eines Löschkonzepts (Grundsatz der Speicherbegrenzung)
- Implementierung eines Benutzerberichtigungskonzepts (Grundsatz der Datenminimierung)

Kap 13 Sanktionen bei Verletzungen des Schutzes personenbezogener Daten

13.1 Geldbußen und Sanktionen durch die DSGVO

Verstöße gegen die DSGVO werden von der Aufsichtsbehörde einerseits mit empfindlichen Geldbußen, andererseits mit sonstigen Sanktionen geahndet. Bei den sonstigen Sanktionen handelt es sich um Abhilfebefugnisse (Verwarnung, Anweisung, Anordnung der Beschränkung der Datenverarbeitung, der Berichtigung oder der Löschung von Daten), die in Art 58 Abs 2 DSGVO geregelt sind. Beide Sanktionsformen können auch parallel verhängt werden.

Je nach Art des Verstoßes beträgt die Obergrenze der möglichen Geldbuße entweder

- bis zu € 10 Mio oder 2% des Konzernumsatzes oder
- bis zu € 20 Mio oder 4% des Konzernumsatzes.

Beispiel:

Strafen bis € 10 Mio oder 2% des Konzernumsatzes:

Verstöße im Zusammenhang mit der Datenschutz-Folgenabschätzung, der Bestellung eines Datenschutzbeauftragten oder den Bestimmungen über den Auftragsverarbeiter.

Strafen bis € 20 Mio oder 4% des Konzernumsatzes:

Verstöße gegen die Bestimmungen über die Grundsätze der Datenverarbeitung, die Rechte der betroffenen Personen, die Übermittlung personenbezogener Daten an einen Empfänger im Drittland oder eine internationale Organisation.

Für die Bestimmung der Geldbuße ist der jeweils höhere Betrag zu verhängen.

Kap 15 Der Weg zur Datenschutz-Compliance

Wie aus den bisherigen Ausführungen ersichtlich, sind auf dem Weg zur Datenschutz-Compliance eine Vielzahl von Entscheidungen zu treffen und unterschiedliche Aktivitäten zu setzen. Ihnen gemein ist, dass die Entscheidungsfindung durch den Verantwortlichen bzw Auftragsverarbeiter selbst erfolgen muss und kein Auslagern an Dritte möglich ist. Weiters ist jeder Verantwortliche und Auftragsverarbeiter für sich selbst verpflichtet, angemessene technische und organisatorische Maßnahmen zu implementieren und nachzuweisen, welche die Einhaltung der DSGVO sicherstellen. Diese Grundregeln ergeben sich als Auswirkung der Rechenschaftspflicht.

Demnach ist es wichtig, die Umsetzung der DSGVO als Projekt zu verstehen und in Summe eine gesamthafte Darstellung der Datenschutzaktivitäten unter Berücksichtigung der Risiken für Freiheit und Rechte der betroffenen Personen zu entwickeln. Vor diesem Hintergrund wird auch von der Ausarbeitung eines Datenschutz-Managementsystems (DSMS) gesprochen. Grundlegende Elemente einer Projektsteuerung sowie des Qualitätsmanagements, wie zB der PDCA-Zyklus („Plan-Do-Check-Act"), sollten aufgenommen werden.

Weiters ist zu beachten, dass ein DSGVO-Projekt nicht am 25.5.2018 enden wird, sondern an diesem Tag lediglich von der Implementierungsphase in die operative Phase übergeht. Ab diesem Tag müssen sich die gesetzten Tätigkeiten in der täglichen Unternehmenspraxis bewähren und der Erfüllung der datenschutzrechtlichen Ziele dienen. Auch hier ist wieder der laufende Verbesserungsgedanke verinnerlicht, da die Wirksamkeit der Maßnahmen in kontinuierliche Evaluierungs- und Prüfungsschleifen zu testen ist. Dies kann sowohl durch unternehmensinterne Maßnahmen als auch durch externe Prüfungen mit anschließender Zertifizierung erfolgen.