Eine Praxiseinführung in die Datenschutz-Grundverordnung

1. Einleitung

Die Datenschutz-Grundverordnung (DSGVO) stellt eines der ambitioniertesten legistischen Projekte der Europäischen Union der vergangenen Jahre dar. Sie wird mit 25. Mai 2018 die EU-Datenschutzrichtlinie ersetzen und die nationalen Datenschutzgesetze der 28 Mitgliedstaaten weitgehend obsolet machen. Nur Organisationen, die frühzeitig beginnen, ihre Verträge, Geschäftsprozesse und IT-Lösungen an die DSGVO anzupassen, werden mit Geltungsbeginn am 25. Mai 2018 ein vertretbares Compliance-Niveau erreicht haben.

Dass die DSGVO ernst zu nehmen ist, verdeutlichen nicht zuletzt die harschen Strafen von bis zu 20 Millionen Euro oder 4 % des weltweiten Konzernjahresumsatzes. Datenschutz wird so zu einem der größten Compliance-Risikofelder und damit notwendigerweise zu einer Priorität für jede Geschäftsleitung.

Die vorliegende Praxiseinführung dient dazu, sich rasch einen Überblick über die DSGVO oder einzelne ihrer Bereiche zu verschaffen. Hinsichtlich der Details verweist sie durch Angabe der entsprechenden Norm der DSGVO bzw einer Randziffer der Kommentierung des jeweiligen Artikels auf den Kommentarteil des vorliegenden Werkes.

2. Die wichtigsten Compliance-Schritte bis zum Geltungsbeginn am 25. Mai 2018

Die Geltung der DSGVO beginnt am **25. Mai 2018** (Art 99 Abs 2). Um bis dahin ein Mindestmaß an Compliance mit der DSGVO herzustellen, müssen Verantwortliche und Auftragsverarbeiter bereits frühzeitig Compliance-Schritte setzen.

Für Verantwortliche lassen sich die wichtigsten bis zum 25. Mai 2018 umzusetzenden ersten Compliance-Schritte wie folgt zusammenfassen:

1) Implementierung der Grundlagen eines **Datenschutz-Compliance-Programms** (siehe Kap 11) einschließlich der Bestellung eines **Daten-**

schutzbeauftragten, soweit dies im konkreten Fall zweckmäßig oder verpflichtend ist (siehe Kap 14),
2) Erstellung eines **Verzeichnisses der Verarbeitungstätigkeiten** (siehe Kap 12),
3) Prüfung der Rechtsgrundlage der jeweiligen Datenverarbeitung (siehe Kap 7), insbesondere der neuen Anforderungen an eine wirksame Einwilligung (siehe Kap 7.1),
4) Entwicklung DSGVO-konformer **Datenschutzerklärungen** (siehe Kap 8) und
5) Prüfung der Rechtsgrundlage für **internationale Datenübermittlungen** (siehe Kap 18).

Für Auftragsverarbeiter sind die wichtigsten ersten Compliance-Schritte bis zum 25. Mai 2018:
1) Bestellung eines **Datenschutzbeauftragten**, soweit dies im konkreten Fall verpflichtend oder zweckmäßig ist (siehe Kap 14),
2) Erstellung eines **Verzeichnisses von Verarbeitungstätigkeiten** (siehe Kap 12),
3) Implementierung **angemessener Sicherheitsmaßnahmen** (siehe Kap 15.1),
4) Sicherstellung, dass **Subauftragsverarbeiter** nur mit der vorherigen gesonderten oder allgemeinen, schriftlichen Genehmigung des Verantwortlichen herangezogen werden (Art 28 Abs 2) und
5) Sicherstellung, dass **internationale Datenübermittlungen** nur unter Einhaltung der Voraussetzungen der DSGVO erfolgen (siehe Kap 18).

Die oben genannten Maßnahmen werden keine vollständige Compliance mit der DSGVO garantieren, helfen jedoch, die personellen und finanziellen Ressourcen eines Verantwortlichen oder Auftragsverarbeiters auf zentrale Aspekte zu fokussieren.

Für größere Organisationseinheiten wird es zudem vorab erforderlich sein, eine grundsätzliche Bewertung der regulatorischen Risiken nach der DSGVO vorzunehmen, um einen effizienten Ressourceneinsatz zu ermöglichen.

3. Grundlegende Begriffe der DSGVO

Die DSGVO findet ausschließlich auf **personenbezogene Daten** Anwendung (siehe Kap 4.1). Diese sind definiert als alle Informationen, die sich

auf eine identifizierte oder identifizierbare **natürliche** Person beziehen, welche wiederum als **betroffene Person** bezeichnet wird (Art 4 Nr 1).

Eine Teilmenge der personenbezogenen Daten sind **sensible Daten** (auch „besondere Kategorien personenbezogener Daten"). Hierbei handelt es sich nach Art 9 Abs 1 um personenbezogene Daten betreffend die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, das Sexualleben oder die sexuelle Orientierung sowie Gesundheitsdaten iSd Art 4 Nr 15 und genetische Daten iSd Art 4 Nr 13. Darüber hinaus zählen auch Sozialversicherungsnummern (vgl Art 4 Rz 35) sowie biometrische Daten (zB Fingerabdrücke oder Gesichtsbilder), die zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden (Art 9 Rz 3), zu den sensiblen Daten.

Normadressaten der DSGVO sind Verantwortliche und Auftragsverarbeiter (vgl Art 3 Rz 4). Die DSGVO definiert den Begriff des **Verantwortlichen** als natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art 4 Nr 7).

Auftragsverarbeiter ist demgegenüber eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet, dh selbst nicht über Zwecke und Mittel der Datenverarbeitung entscheidet (Art 4 Nr 8). Lagert beispielsweise ein Unternehmen den Betrieb seiner Kundendatenbank an einen IT-Dienstleister aus, so agiert das Unternehmen weiterhin als Verantwortlicher, während der IT-Dienstleister als Auftragsverarbeiter fungiert.

Das **Verarbeiten** personenbezogener Daten ist denkbar weit definiert und umfasst jegliche Handhabung personenbezogener Daten, beginnend mit ihrer Erhebung, über das Ordnen, Verändern, Auswerten, Abfragen, Übermitteln und Gespeichert-Halten bis hin zum Löschen oder Vernichten (Art 4 Nr 2).

Der Begriff **Übermitteln** wird in der DSGVO häufig gebraucht, jedoch nicht definiert. Es kann hierunter die Offenlegung gegenüber einem anderen Verantwortlichen oder einem Auftragsverarbeiter bzw Subauftragsverarbeiter verstanden werden (siehe Art 44 Rz 1).

Der Begriff **Aufsichtsbehörde** bezeichnet die Datenschutzbehörde in jedem Mitgliedstaat.

Für jene Leser, welche nach Übersetzungen der Rechtsbegriffe des DSG 2000 in die Terminologie der deutschen und englischen Fassung der DSGVO suchen, wird auf das **DSG 2000–DSGVO Mini-Wörterbuch** am Anfang dieses Werkes (Seite XXIII) verwiesen.

4. Der Geltungsbereich der DSGVO

Im Folgenden wird beschrieben, für welche Tätigkeiten die DSGVO gilt (Kap 4.1), für wen die DSGVO gilt (Kap 4.2) und wo sie gilt (Kap 4.3).

4.1. Der sachliche Anwendungsbereich – Welche Datenverarbeitungen sind erfasst?

Grundsätzlich gilt die DSGVO für jegliche Verarbeitung personenbezogener Daten. Wie oben unter Punkt 3 ausgeführt, sind personenbezogene Daten alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen. Ob eine natürliche Person identifizierbar ist, muss **objektiv** beurteilt werden, sodass nicht nur auf die rechtlichen und tatsächlichen Möglichkeiten des Verantwortlichen, sondern auch auf die Möglichkeiten Dritter abzustellen ist (Art 4 Rz 3). So ist eine IP-Adresse eines Nutzers für den Betreiber einer Website auch dann ein personenbezogenes Datum, wenn zwar nicht der Betreiber, jedoch der Internet-Access-Provider des Nutzers einen Personenbezug herstellten könnte (so auch die Ansicht des Generalanwalts zur Rechtslage vor der DSGVO, vgl EuGH, C-582/14 – *Breyer*; die Entscheidung des Gerichtshofs steht derzeit noch aus).

Beziehen sich die Daten auf **juristische Personen**, sind sie nur dann personenbezogen iSd DSGVO, wenn der Firmenwortlaut der juristischen Person den Namen einer natürlichen Personen enthält (Art 4 Rz 1). Daten, welche sich auf verstorbene Personen beziehen, sind ebenso wenig personenbezogen iSd DSGVO (Art 4 Rz 2).

Die DSGVO gilt grundsätzlich nur für **elektronisch verarbeitete Daten**. Für manuell (in der Regel auf Papier) verarbeitete Daten gilt die DSGVO nur, wenn die Daten in einem Dateisystem gespeichert sind oder dort gespeichert werden sollen (Art 2 Abs 1). Ein Dateisystem ist eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind (Art 4 Nr 6), wie zB eine nach Namen geordnete Personalaktenverwaltung. Einzelne Papierakten unterliegen jedoch nicht der DSGVO (Art 2 Rz 4).

Als Rechtsakt der Union findet die DSGVO außerhalb des Anwendungsbereichs des Unionsrechts (zB im Bereich der nationalen Sicherheit) keine Anwendung (Art 2 Abs 2 lit a). Weiters gilt die DSGVO nicht für den Bereich der Gemeinsamen Außen- und Sicherheitspolitik (GASP; Art 2 Abs 2 lit d) sowie für die Bereiche der Strafrechtspflege, des Strafvollzugs und der öffentlichen Sicherheit (Art 2 Abs 2 lit d; hier ist die

Richtlinie (EU) 2016/680 einschlägig, welche insbesondere in der StPO, dem SPG, dem PStSG und dem StVG umzusetzen sein wird).

Schließlich gilt die DSGVO nicht bei der Verarbeitung von personenbezogenen Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten („**Household Exemption**"; Art 2 Abs 2 lit c). Hierzu zählt insbesondere die zu privaten Zwecken erfolgende Nutzung sozialer Netzwerke (Art 2 Rz 7).

4.2. Der persönliche Anwendungsbereich – Für wen gilt die DSGVO?

Normadressaten der DSGVO sind sowohl Verantwortliche als auch Auftragsverarbeiter (siehe Kap 3 zur Definition dieser Begriffe).

Nach der DS-RL war die Rolle des Auftragsverarbeiters attraktiv, da diesen nur untergeordnete regulatorische Pflichten trafen. Der wirtschaftliche Nachteil der Rolle des Auftragsverarbeiters bestand und besteht freilich darin, die personenbezogenen Daten nicht für eigene Zwecke verwenden zu dürfen. Wer personenbezogene Daten zu eigenen Zwecken verwenden und so aus ihnen einen wirtschaftlichen Wert schöpfen wollte (Stichwort „**Dateneigentum**"), musste hingegen die Rolle des Verantwortlichen für sich beanspruchen, was mit erheblichen zusätzlichen Pflichten verbunden war.

Diese Gleichung ändert die DSGVO insofern, als Auftragsverarbeiter – ebenso wie Verantwortliche – nunmehr primäre Normadressaten sind, erheblichen regulatorischen Pflichten unterworfen werden (siehe einleitend Kap 2 oben) und insbesondere denselben Geldbußen ausgesetzt sind (siehe Kap 20). Durch diese tendenzielle Annäherung der Verantwortlichkeit von Verantwortlichen und Auftragsverarbeitern treten daher die wirtschaftlichen Vorteile der Verantwortlichenstellung in den Vordergrund. Viele Unternehmen, die sich bisher ausschließlich auf eine Auftragsverarbeiterstellung beschränkt haben, werden daher zunehmend versuchen, eine Stellung als Verantwortlicher zu erlangen. Dies bedeutet jedoch nicht nur, dass regulatorische Pflichten hinsichtlich der Rechtsgrundlage der Datenverarbeitung, wie insbesondere der Einwilligung der Betroffenen (siehe Kap 7) und der Transparenz (siehe Kap 8) einzuhalten sind, sondern auch, dass bestehende Verträge mit Kunden, Abnehmern und allenfalls Betroffenen zu überarbeiten sind, um diese neue regulatorische Realität zu reflektieren.

4.3. Der räumliche Anwendungsbereich – Wo gilt die DSGVO?

Die DSGVO findet jedenfalls auf Verantwortliche und Auftragsverarbeiter Anwendung, welche ihren **Sitz in der EU bzw dem EWR** (vgl Art 3 Rz 5) haben. Auftragsverarbeiter in der EU unterliegen sogar dann der DSGVO, wenn sie für Verantwortliche tätig sind, die nicht der DSGVO unterliegen (Art 3 Rz 4).

Weiters gilt die DSGVO auch dann, wenn der Verantwortliche bzw Auftragsverarbeiter seinen Sitz zwar nicht in der EU bzw dem EWR hat, jedoch eine Niederlassung (zB eine Tochtergesellschaft) in der EU oder dem EWR hat und die Datenverarbeitung **im Rahmen der Tätigkeiten dieser Niederlassung** erfolgt. Ein solcher Fall liegt zB vor, wenn die US-Konzernmutter die personenbezogenen Daten der Kunden einer österreichischen Tochtergesellschaft verarbeitet, um die Verkaufsaktivitäten der Tochtergesellschaft zu unterstützen (vgl Art 3 Rz 2).

Um sicherzustellen, dass Wirtschaftsakteure ohne Niederlassung in der EU bzw dem EWR, welche auf dem europäischen Markt tätig werden, denselben Wettbewerbsbedingungen wie europäische Unternehmen unterliegen, gilt die DSGVO auch für Verantwortliche und Auftragsverarbeiter ohne Niederlassung in der Union, wenn diese ihre **Waren oder Dienstleistungen entgeltlich oder unentgeltlich in der EU bzw dem EWR anbieten** (Art 3 Abs 2 lit b).

Weiters findet die DSGVO auch auf Verantwortliche und Auftragsverarbeiter ohne Niederlassung in der Union Anwendung, die das Verhalten betroffener Personen in der Union **beobachten** (Art 3 Abs 2 lit b). Dies gilt insbesondere für sog Online-Advertising-Networks, welche das Surf-Verhalten von Internetnutzern protokollieren, um personenbezogene Online-Werbung ausliefern zu können.

5. Das Verhältnis zu nationalen Datenschutzgesetzen

Grundsätzlich gilt, dass die DSGVO wie jede EU-Verordnung unmittelbar anwendbar ist und daher nicht durch nationales Recht umgesetzt werden darf. Das DSG 2000 wird daher in seiner jetzigen Form nach dem 25. Mai 2018 nicht fortbestehen.

Außerhalb des Anwendungsbereichs der DSGVO (siehe Kap 4) bleibt es dem nationalen Gesetzgeber jedoch überlassen, Regelungen zu treffen. Bei der Frage des Datenschutzes für juristische Personen ist allerdings zu hoffen, dass der österreichische Gesetzgeber von dieser

Möglichkeit nicht Gebrauch machen wird. Denn der ohnedies bereits gegebene (§§ 123 f StGB, §§ 11 f UWG) und in Umsetzung der Geschäftsgeheimnis-RL (2016/943/EU) noch zu präzisierende Schutz von Geschäftsgeheimnissen stellt bereits ein hinreichendes Regelungsinstrument dar, sodass es eines nationalen Sonderwegs mit zweifelhafter systematischer Einordnung des auch datenschutzrechtlichen Schutzes juristischer Personen nicht bedarf.

Hiervon unabhängig gibt es zahlreiche Regelungsfragen im Anwendungsbereich der DSGVO, für welche die DSGVO keine oder keine abschließende Antwort vorsieht, sondern durch **Öffnungsklauseln** bewusst und kompromisshaft eine legislative Zuständigkeit der Mitgliedstaaten begründet und damit Unterschiede innerhalb der Mitgliedstaaten zulässt. Dies ist insbesondere bei folgenden Regelungsfragen der Fall (vgl Art 92 Rz 4):

- Ab welchem Alter kann ein Minderjähriger wirksam in die Verarbeitung seiner personenbezogenen Daten einwilligen? (Art 8 Abs 1 UAbs 2)
- Wann ist eine wirksame Einwilligung in die Verarbeitung sensibler Daten ausgeschlossen? (Art 9 Abs 2 lit a)
- Unterliegt die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten zusätzlichen Beschränkungen? (Art 9 Abs 5)
- Dürfen personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten überhaupt verarbeitet werden? (zB im Rahmen einer Whistleblowing-Hotline; Art 10)
- Sind automatisierte Entscheidungen und Profiling, welche für den Abschluss oder die Erfüllung eines Vertrages mit der betroffenen Person nicht erforderlich sind, auch ohne Einwilligung der betroffenen Person zulässig? (Art 22 Abs 2 lit b)
- Unterliegen die Betroffenenrechte zusätzlichen Beschränkungen? (Art 23)
- Müssen nur bestimmte oder alle Verantwortlichen und Auftragsverarbeiter einen Datenschutzbeauftragten bestellen? (Art 37 Abs 4)
- Können gegen Behörden und öffentliche Stellen Geldbußen verhängt werden? (Art 83 Abs 7)
- Können Datenschutzorganisationen im Namen der Betroffenen Schadenersatz begehren? (Art 80 Abs 1)
- Können Datenschutzorganisationen auch ohne Auftrag eines Betroffenen gegen einen Verantwortlichen oder Auftragsverarbeiter mit Klage vorgehen? (Art 80 Abs 2)