Grundprinzipien des Datenschutzes nach der DSGVO und DSG

dataprotect it-recht

Grundprinzipien des Datenschutzes nach der DSGVO und DSG

Datenschutz ist **Schutz personenbezogener Daten natürlicher Personen**.

Ab **25.5.2018** tritt die **Datenschutz-Grundverordnung (DSGVO)** in Geltung und mit diesem Zeitpunkt müssen „**Verantwortliche**“ und „**Auftragsverarbeiter**“ sich an die Bestimmungen sowie die Ausführungsbestimmungen im **Datenschutzgesetz** (veröffentlicht am 31.7.2017 im BGBl I 120/2017) halten.

Eine „Übergangsfrist“ wird es nicht geben, da die Unternehmen, Behörden und öffentlichen Stellen bereits seit April 2016 (Veröffentlichung der VO 679/2016 im Amtsblatt) Zeit haben, sich intensiv vorzubereiten.

Was ändert sich ab 25.5.2018?

Derzeit sind auch juristische Personen im Schutzbereich des österreichischen DSG; ab 25.5.2018 ist nur mehr der **Schutz personenbezogener Daten natürlicher Personen** im Fokus der DSGVO („betroffene Person“ = natürliche Person; DSGVO regelt nur den Schutz natürlicher Personen.

Dennoch ist auch die juristische Person in Österreich aufgrund der unveränderten Geltung des § 1 (1) DSG („Jedermann“) im Schutzbereich des DSG, wobei dies keine zu großen Auswirkungen auf die Regelungen hat.

Die **Registrierungs- und Anmeldungspflicht** beim Datenverarbeitungsregister entfällt. Nach (us-amerikanischem Vorbild) wird dies von „**accountability**“ (**Rechenschaftspflicht**) abgelöst, die auch mit einer **Nachweispflicht** (siehe Art. 5 (2) DSGVO) verbunden ist.

„**Compliance**“ wird das Gebot im Datenschutz und „**Risiko**“ für Freiheiten und Rechte natürlicher Personen ist der Ausgangspunkt für viele Betrachtungen.

Werden die Regelungen nicht eingehalten, dann drohen den Unternehmen (siehe § 30 DSG) **hohe Geldstrafen** (siehe insbes. Art. 83 DSGVO; bis zu 4 % des Gesamtumsatzes bzw. EUR 20 Mio als maximaler Rahmen).

Welche Maßnahmen können jetzt gesetzt werden?

Es ist notwendig

1. ein **Commitment der Unternehmens- oder Behördenleitung** einzuholen, Datenschutz nach den Prinzipien der DSGVO als Prinzip der Organisation zu verankern,

2. eine/n **Verantwortliche/n („Data-Manager“)** in der Organisation zu bestellen, der das Projekt übernimmt, und steuert,

3. die **Gesamtsituation** in Bezug auf die **personenbezogenen Daten natürlicher Personen zu analysieren**,

4. **Abweichungen vom Standard**, den das Gesetz vorschreibt, **festzustellen**,

5. **Maßnahmen festzulegen** und gegebenenfalls zu **priorisieren**,

6. sowie die **technischen, organisatorischen und rechtlichen Maßnahmen** zu setzen, um die **bestehenden Defizite aufzuarbeiten**.

Welche Grundprinzipien normiert die DSGVO?

Folgende **Grundprinzipien** der DSGVO sind jedenfalls zu beachten:

Rechtmäßigkeit

Die **Verarbeitung von personenbezogenen Daten natürlicher Personen** ist **grundsätzlich verboten**, außer der Verantwortliche (derjenige, der die Daten für die eigenen Zwecke verarbeitet) kann sich auf eine gültige Rechtsgrundlage berufen.

Die Verarbeitung der Daten muss „**rechtmäßig**" sein, dh es muss **mindestens eine der Rechtsgrundlagen iSd Art. 6** oder **Art 9** (besondere Datenkategorien) oder **Art 10** (strafrechtlich relevante Daten) **DSGVO** gegeben sein. Diese sind z.B.

1. die (**freiwillige, informierte, jederzeit widerrufliche) Einwilligung** (z.B. beim Newsletter),

2. ein **Vertrag**, der zwischen den Parteien abgeschlossen ist/wird bzw. dessen Anbahnung (mit Kunden, Lieferanten, Beschäftigten, Bewerbern),

3. eine **rechtliche (gesetzliche) Verpflichtung** des Verarbeiters (z.B. steuerliche Aufbewahrungspflichten),

4. **lebenswichtige Interessen** der betroffenen Person oder eines Dritten (z.B. im Katastrophenfall),

5. **öffentliche Interessen** bzw. die **Ausübung öffentlicher Gewalt**,

6. oder ein **berechtigtes Interesse** an der Verarbeitung (z.B. bei Werbemaßnahmen per Post (beachte: absolutes Widerspruchsrecht; Videoüberwachung).

Transparenz & Information

Die **Verarbeitung** personenbezogener Daten hat **transparent** zu erfolgen. Die natürlichen Personen, deren Daten verarbeitet werden, sollen Kenntnis darüber haben, welche konkreten Datenkategorien von welchem Verarbeiter für welchen Zweck verarbeitet werden.

Daher sind umfassende **Informationspflichten** bei der Erhebung und Verwendung von Daten normiert, und ist z.B. bei der Einwilligung darauf hinzuweisen, dass die betroffene Person das Recht hat, die Einwilligung zu widerrufen, und es ist über die Rechte der betroffenen Personen (z.B. Auskunft, Löschung, Data Portability) zu informieren.

In diesem Rahmen ist es notwendig, dass Bewerber, Beschäftigte, Kunden, Lieferanten, Interessenten, Personen, die über die Website Kontakt haben, Besucher, Personen, die von Videoüberwachung betroffen sind, bei der Erhebung der Daten (dh dort wo sie in den ersten Kontakt mit der Organisation, die Daten verarbeitet, treten) über den Zweck einer Verarbeitung und die Identität des Verarbeiters informiert werden, und auf weitergehende (sehr detaillierte) Informationen und den Zugang zu diesen hingewiesen werden.

Es ist zulässig, dass die betroffenen Personen mit einem allgemeinen Hinweis auf die Identität des Verantwortlichen (Verarbeiter) sowie den Zweck der Verarbeitung hingewiesen werden, und dann die Möglichkeit haben, die restlichen Informationen zum Datenschutz zu erhalten (z.B. über eine Link auf der Website).

Bei einer Newsletter-Anmeldung wäre es daher zulässig, folgenden Hinweis zu setzen:

> ***Wir verarbeiten die Daten zu Werbezwecken. Weitere Informationen dazu finden Sie unter www.domain.at/Newsletter-Info.***

Zweckbindung

Die Verarbeitung der Daten muss einem **eindeutigen, festgelegten Zweck (Zweckfestlegung)** dienen, und die Daten dürfen nur für diesen konkreten Zweck verwendet werden **(Zweckbindung ieS)**.

Datenminimierung

Datenminimierung bedeutet, dass **nur diejenigen Daten verarbeitet werden dürfen**, die für den (definierten) Zweck **notwendig** sind und nicht darüber hinausgehen. Eine andere Verwendung ist nicht ohne eine weitere Rechtsgrundlage zulässig. Daten, die zB im Rahmen eines Kundenverhältnisses (Vertrag) erhoben werden, und in der Kundenverwaltung gespeichert sind, werden aufgrund des Vertrages (Rechtsgrundlage) verwendet. Wenn man damit auch einen anderen Zweck verfolgen will, zB Marketing, dann benötigt man dazu eine andere Rechtsgrundlage, nämlich entweder eine gültige Einwilligung (freiwillig, informiert, jederzeit widerrufbar) oder das berechtigte Interesse (Kundengewinnung, wobei dann ein Widerspruchsrecht besteht, auf das der Kunden bei der ersten Verwendung für diesen Zweck zu informieren ist). Bitte beachten Sie, dass Kundendaten nur bei einer Einwilligung oder unter den Voraussetzungen des § 107 Abs 3 TKG für die Zusendung von Direktwerbung per elektronischer Post (z.B. Newsletter per Email) oder SMS verwendet werden dürfen, sodass das „berechtigte Interesse“ für Marketingzwecke nur für Zusendungen per Post verwendet werden kann.

Richtigkeit

Die verwendeten Daten müssen sachlich richtig sein (und auch auf dem neuesten Stand, wenn dies für den Verarbeitungszweck erforderlich ist).

Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, als dies für den Zweck erforderlich ist. Die Speicherbegrenzung schreibt vor, dass jeder Verarbeiter festlegen muss (im Rahmen der gesetzlichen Anforderungen) zu welchem Zeitpunkt er die Daten löscht (oder anonymisiert).

Integrität & Vertraulichkeit

Dieses Prinzip erfordert, dass die Integrität der Daten und auch deren Vertraulichkeit zu schützen sind.

Was sind die konkreten Regelungen in der DSGVO und im DSG?

Die Bestimmungen der **DSGVO**, die durch das **DSG** ab 25.05.2018 (dann nicht mehr Datenschutzgesetz 2000 oder DSG 2000, sondern nur mehr Datenschutzgesetz oder DSG) ergänzt bzw. präzisiert werden, regeln diese Grundprinzipien im Detail.

Einige wesentliche Punkte daraus sind:

Datenschutzerklärung / Texte für Informationen an betroffene Personen (Art. 13 und 14 DSGVO):

Eine **Datenschutzerklärung**, die uU auch auf der Website notwendig sein könnte (z.B. bei Webshops, Anmeldungen für Newsletter, etc…), ist auf den aktuellen Stand der Informationsverpflichtungen nach der DSGVO anzupassen. Auch bei anderen Arten der Erhebung von Daten sind die betroffenen Personen ausreichend iSd Art. 13 und 14 DSGVO zu informieren, und die notwendige Texte sind zu erstellen bzw. die bestehenden Texte zu überarbeiten.

Ein „Medienbruch" ist zulässig, sodass die betroffenen Personen (zB Kunden, Lieferanten) im Rahmen der üblichen Korrespondenz auf die Verarbeitung ihrer Daten für die Geschäftsabwicklung hingewiesen werden können, und Ihnen eine Zugangsmöglichkeit auf die Datenschutzerklärung (Datenschutz-Information) auf der Website gegeben wird. Dies ist jedoch nur dann zulässig, wenn man annehmen kann, dass die betroffenen Personen tatsächlich auch die Möglichkeiten haben, über das Internet auf diese Daten zugreifen zu können, sodass zB bei einer Seniorenresidenz dies eher nicht möglich sein wird.

Rechte der betroffenen Personen (Art. 15 ff. DSGVO):

In der Organisation ist organisatorisch, technisch und auch rechtlich sicherzustellen, dass den Rechten der betroffenen Person (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Datenübertragbarkeit, Recht nicht einer automatischen Entscheidungsfindung unterworfen zu sein) rechtzeitig und vollumfänglich bei der Ausübung nachgekommen werden kann.

Es ist daher zu empfehlen, alle möglichen anwendbaren Szenarien in einem konkreten Rollenspiel durchzuspielen, den jeweiligen Prozess bei einem Ersuchen einer betroffenen Person mit den entsprechenden Verantwortlichkeiten zu definieren und damit auf die möglichen Ausübung der Betroffenenrechte vorbereitet zu sein.

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO):

Verantwortliche sind verpflichtet, selbst ein Dokument zu erstellen.

Der Inhalt umfasst: den **Zweck** der Verarbeitung, die **Kategorien der betroffenen Personen**, die **Kategorien der personenbezogenen Daten**, **Kategorien von Empfängern**, **Fristen für die Löschung** und die **technischen und organisatorischen Maßnahmen** zur Sicherheit der Verarbeitung. Es ist auch sinnvoll, die **Rechtsgrundlage** und die **Quelle** der Daten in diesem Dokument aufzunehmen, obwohl dies gesetzlich nicht gefordert ist.

Ausgangspunkt für dieses Verzeichnis von Verarbeitungstätigkeiten kann die (aktuelle) Meldung beim Datenverarbeitungsregister sein, wobei zu empfehlen ist, dasselbe nicht in der Detailliertheit wie dies

üblicherweise bei DVR-Meldungen erfolgte, zu erstellen. Ausgangspunkt für unterschiedliche Kategorien (von Personen, Daten oder Empfängern) sollte das Risiko sein, welches damit aus Sicht der betroffenen Person verbunden ist.

Meldung bei Datenschutzverletzungen (Data Breach Notification) (Art. 33 und 34 DSGVO):

Kommt es zu einer Datenschutzverletzung, dann ist eine Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und an die betroffenen Personen (Art. 34 DSGVO) zu erstatten.

Die **Meldung bei der Datenschutzbehörde** kann entfallen, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Meldung an die Aufsichtsbehörde ist unverzüglich und möglichst binnen 72 Stunden durchzuführen.

Überdies sind auch die **betroffenen Personen** unverzüglich von einer Datenschutzverletzung zu informieren, wenn die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen zur Folge hat.

Aus der kurzen Frist für die Meldung bei der Behörde ist ersichtlich, dass in der jeweiligen Organisation proaktiv ein Prozess zur Meldung von Datenschutzverletzungen zu implementieren ist; wenn sich eine Organisation mit den potentiellen Verletzungen des Datenschutzes nicht vorab befasst, und die Abläufe definiert, wird es vermutlich die Fristen der Art. 33 oder 34 DSGVO nicht einhalten können, und setzt sich einer potentiellen Geldbuße aus.

Datenschutz-Folgenabschätzung (Art. 35 DSGVO):

Sofern eine Datenverarbeitung, insbes. bei **Verwendung neuer Technologien**, aufgrund der **Art, des Umfanges, der Umstände** und **der Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen** haben kann, ist eine Datenschutz-Folgenabschätzung durchzuführen. Es ist zu dokumentieren, welche Risiken für die betroffene Person (nicht für die Organisation) durch die Datenverarbeitung gegeben sind.

Datenschutzbeauftragter (Art. 37 ff DSGVO):

In Art. 37 DSGVO wird für **Behörden und öffentliche Stellen** (Abs 1 lit a DSGVO) sowie für **Unternehmen** (Abs 1 lit b und c DSGVO) **unter bestimmten Voraussetzungen** die Bestellung eines Datenschutzbeauftragten (DSB) verpflichtend vorgeschrieben. Unternehmen müssen dann einen DSB bestellen, wenn mit der **Datenverarbeitung ein Risiko** verbunden ist, und zwar dann, wenn die Kerntätigkeit des Unternehmens bestimmte umfangreiche Datenverarbeitungen (regelmäßige und systematische Überwachung von betroffenen Personen ist erforderlich) in der Kerntätigkeit des Unternehmens umfasst oder bestimmte Datenarten (Art. 9/10-Daten) im Rahmen der Kerntätigkeit umfangreich verarbeitet werden.

Datenverarbeitung im Beschäftigungskontext (Art. 88 DSGVO, § 11 DSG):

Die DSGVO gibt den **Mitgliedsstaaten** die Möglichkeit, die **Datenverarbeitung von HR-Daten speziell zu regeln**. In Österreich finden sich diesbezügliche **Regelungen für Unternehmen**, in denen ein Betriebsrat besteht, in **§§ 96 und 96a ArbeitsverfassungsG (Betriebsvereinbarungen)**, und

Unternehmen, bei denen ein Betriebsrat nicht besteht, in **§ 10 (1) ArbeitsvertragsrechtsanpassungsG (Einzelvereinbarung)**. In diesen Bestimmungen wird den Unternehmen die Möglichkeit gegeben, außerhalb der Verarbeitung der personenbezogenen Daten im Arbeitsverhältnis, die zur (wechselseitigen) Erfüllung des Arbeitsvertrages notwendig sind oder die gesetzlich vorgeschrieben sind (z.B. Arbeitsunfälle, Arbeitszeitaufzeichnungen …), **Regelungen auf genereller Basis für die Verarbeitung von personenbezogenen Daten** (z.B. Videoüberwachung, whistleblowing-Hotline, Zeiterfassungssysteme, Zugangskontrollsysteme für bestimmte Bereiche …) mit den Mitarbeitern zu **vereinbaren**.

Durch den Verweis in (§ 11 DSG) auf das ArbVG soll klargestellt werden, dass diese Systematik auch den Bestimmungen der DSGVO Rechnung trägt, wobei mE noch Klarstellungen für betriebsratslose Betriebe oder leitende Angestellte mit maßgeblichem Einfluss auf die Betriebsführung oder freie Dienstnehmer, die an sich von Betriebsvereinbarungen iSd ArbVG nicht erfasst werden, im Gesetz notwendig gewesen wären.

Geldbußen (Art. 83 DSGVO, § 30 DSG):

Wie bereits aus den Medien zu entnehmen war, werden die Geldbußen erheblich steigen, und bis zu **EUR 20.000.000,--** bzw. 4 % des weltweiten Gesamtumsatzes betragen können (es zählt die Grenze, die höher ist).

Die Geldbußen sollen in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend sein** (siehe Art 83 (1) DSGVO). Die Geldbuße soll nach der neuen österreichischen Rechtslage primär die **juristische Person treffen**, und **nicht** den **Vorstand, Geschäftsführer** oder **den verantwortlich Beauftragten** gem. § 9 VStG. Die juristische Person ist insbesondere dann der Adressat der Geldbuße, wenn ein **Internes Kontrollsystem** fehlt, und dies die Begehung der Tat durch MitarbeiterInnen ermöglicht hat.

Kinder:

Bei einem **Angebot von Diensten der Informationsgesellschaft**, das einem **Kind direkt** gemacht wird, ist die Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das **vierzehnte Lebensjahr** vollendet hat (siehe § 4 (4) DSG). Die Öffnungsklausel des Art. 8 (1) DSGVO, nämlich dass ein Mitgliedsstaat ein niedrigeres Alter als DSGVO selbst (nämlich Vollendung des 16. Lebensjahres) festlegen kann, wurde ausgenützt.

Bildverarbeitung (Videoüberwachung) (§ 12 ff DSG):

Die **Bildverarbeitung (Videoüberwachung)** wird in Österreich **im Datenschutzgesetz näher präzisiert**, und z.B. eine Speicherdauer von 72 Stunden als Standard vorgesehen.

Die **Gründe für die Rechtmäßigkeit** sind speziell definiert und das überwiegende berechtige Interesse im Einzelfall unter Abwägung der Interessen im Sinne einer Verhältnismäßigkeit wird in einer demonstrativen Aufzählung näher definiert.

Weiters werden **Gründe für die Unzulässigkeit einer Bildverarbeitung** normiert, nämlich im höchstpersönlichen Lebensbereich ohne die ausdrückliche Einwilligung, zur Kontrolle von Arbeitnehmern, der automationsunterstützte Abgleich der Bildverarbeitung mit anderen personenbezogenen Daten sowie die Auswertung der Bildverarbeitung anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium.

Eine **Videoüberwachungsanlage ist gesondert zu kennzeichnen**, damit die Betroffenen erkennen können, wer die Videoüberwachung betreibt und ihre Rechte ausüben können.

Die Schlussfolgerung

Die **Datenschutz-Grundverordnung** ist seit mehr als einem Jahr in Geltung und tritt in weniger als 90 Arbeitstagen in Kraft. Es ist daher dringend geboten, dass Organisationen mit den Notwendigkeiten und Verpflichtungen, die sich daraus ergeben, auseinandersetzen.

Der erste Ansatzpunkt dafür wäre z.B. festzustellen, **welche Kategorien von betroffenen Personen es in der Organisation gibt** (Bewerber/innen, Mitarbeiter/innen, Kunden, Lieferanten, Abonnenten des Newsletters …) und **welche Datenarten** in Bezug auf diese Personen für welchen **konkreten, eindeutig definierten Zweck** verarbeitet werden.

Aus dieser ersten Analyse sollte das **Verzeichnis von Verarbeitungstätigkeiten** erstellt werden, wobei darin auch die **Kategorien der Empfänger** sowie die **Löschfristen** und auch die **technischen und organisatorischen Maßnahmen** zur Sicherheit der Verarbeitung zu dokumentieren sind.

Für interne Dokumentationszwecke kann das Verzeichnis auch um die **Gründe für die Rechtmäßigkeit** der Verarbeitung und eine **Einschätzung des potentiellen Risiko**, insbes. auch mit Hinblick darauf, ob ein hohes Risiko für Rechte und Freiheiten der natürlichen Personen besteht, ergänzt werden.

Weiters sollte dokumentiert werden, ob und weshalb ein **DSBA** bestellt wird, oder davon ausgegangen wird, dass ein DSB nicht verpflichtend zu bestellen ist.

Nach diesen Maßnahmen sollen die notwendigen **Prozesse** für die **Erfüllung der Rechte der betroffenen Personen** sowie die **Meldungen bei Datenschutzverletzungen** definiert werden.

Auch die Texte für eine **Data Privacy Policy** (Datenschutzerklärung) und auf den konkreten Zweck abgestimmte **Informationstexte** für die betroffenen Personen sollten an die Bestimmungen und Verpflichtungen der DSGVO angepasst werden.

Da Datenschutz nicht nur von Maßnahmen und Dokumentation abhängig ist, ist es auch notwendig, das Bewusstsein für den Schutz der personenbezogenen Daten natürlicher Personen bei den Mitarbeiter/innen der Organisation zu wecken bzw. anzuheben, und diese im Datenschutz zu schulen und zu trainieren, sowie diesen Ansprechpartner für Fragen im Anlassfall zu geben.

Version 1.1 (März 2018)
© Dr. Thomas Schweiger, LLM (Duke), CIPP/E
zertifizierter Datenschutzbeauftragter (DATB)
www.dataprotect.at
SMP Schweiger Mohr & Partner Rechtsanwälte OG
Huemerstraße 1 / Kaplanhofstraße 2, A-4020 Linz
ATU 40112014 Tel 0732/79 69 00 Fax 0732 796906
FN 37294w LG Linz / Österreich

Verfasser: RA Dr. Thomas Schweiger, LL.M. (Duke), CIPP/E