„Datenschutz & Datenschutzgrundverordnung“

Ziel und Zweck des Datenschutzrechts:

Funktion des Datenschutzrechts ist es personenbezogene Daten natürlicher Personen vor der unrechtmäßigen Verarbeitung zu schützen und sowohl Datensicherheit zu gewährleisten als auch unerwünschte und unzulässige Eingriffe in die Privatsphäre der betroffenen Person zu unterbinden.

Rechtsquellen:

Europarechtlich: Datenschutzgrundverordnung (DSGVO)

Österreich: Datenschutzgesetz (DSG); zu beachten ist jedoch, dass auch weitere Gesetze datenschutzrechtliche Bestimmungen enthalten, die im Einzelfall anwendbar sind (zB Psychologengesetz).

Auf das (verfassungsrechtlich gewährleistete) Grundrecht auf Datenschutz sei an dieser Stelle verwiesen. Es bezieht sich auf die Ermittlung und den Schutz vor der Weitergabe der ermittelten Daten; keinen Schutz gibt es hier, wenn die Daten allgemein verfügbar oder soweit anonymisiert sind, dass kein Rückschluss mehr auf das Rechtssubjekt gezogen werden kann.

Anwendungsbereich:

1. Zeitlich: ab dem 25. Mai 2018
2. Räumlich: generell gilt die DSGVO für die folgenden Datenverarbeitungen
    a. Datenverarbeitungen innerhalb des Unionsgebiets,
    b. Datenverarbeitungen, die von einem Verantwortlichen durchgeführt werden, der keine Niederlassung in der EU hat, sofern er Personen, die sich im Unionsgebiet aufhalten Waren/Dienstleistungen anbietet oder ihr Verhalten beobachtet. Auf Entgeltlichkeit kommt es dabei nicht an.
3. Sachlich: die (teilweise) automatisierte Verarbeitung personenbezogener Daten natürlicher Personen oder die nichtautomatisierte Verarbeitung personenbezogener Daten natürlicher Personen, die in einem Dateisystem gespeichert werden (sollen) sind erfasst. Ausgenommen vom Anwendungsbereich sind etwa Verarbeitungstätigkeiten zu ausschließlich persönlicher oder familiärer Tätigkeiten (zB die Erstellung von Geburtstagslisten). Ebenso sind die Daten verstorbener Personen nicht vom Anwendungsbereich erfasst.

Der Anwendungsbereich des DSG deckt sich weitestgehend mit dem Anwendungsbereich der DSGVO.

Einschlägige Begriffsdefinitionen (Auswahl):

Personenbezogene Daten/Betroffene Person:

Es handelt sich hier um jene Informationen mit denen man eine natürliche Person (**betroffene Person**) identifizieren kann (zB Name, Adresse, aber auch ein Bild kann genügen).

Die DSGVO kennt spezielle Kategorien innerhalb der personenbezogenen Daten, die besonders schutzwürdig sind (zB Gesundheitsdaten, genetische Daten, Daten aus denen die ethnische Herkunft, politische Meinung, Gewerkschaftsangehörigkeit hervorgehen), die nur in bestimmten Fällen verarbeitet werden dürfen.

ADVM-Code: R185706
UID: ATU 68592613
Erste Bank IBAN AT57 2011 1285 3751 0106 BIC: GIBAATWWXXX

RA Dr. Graciela Faffelberger LL.M.
Kärntner Ring 5-7, 7.Stock; 1010 Wien
office@legalmining.eu; www.legalmining.eu
+43 650 5107690

Verarbeitung:

Unter diesen Begriff werden viele Handlungen erfasst zB Erheben, Erfassen, Organisation, Speichern, Verwenden, Löschen.

Verantwortlicher:

Das ist die natürliche oder juristische Person, Behörde oder Einrichtung, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine Vielzahl der Bestimmungen der DSGVO/DSG ist an sie adressiert.

Auftragsverarbeiter:

Es ist die natürliche oder juristische Person, Behörde oder Einrichtung, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (zB Provider).

Datenschutzbeauftragter:

Aus österreichischer Sicht handelt es sich um eine Neuerung, da diese Rechtsfigur dem österreichischen Recht bisher fremd war.

Rechte und Pflichten der Hauptakteure des Datenschutzrechts:

Der Verantwortliche: Er ist für die Einhaltung der datenschutzrechtlichen Grundsätze verantwortlich und hat diese Einhaltung auch nachweisen (sog Rechenschaftspflicht). Die DSGVO geht somit von einem risikobasierten Ansatz aus, dh der Verantwortliche hat bei der Durchführung von Datenverarbeitungen eigenständig zu prüfen, ob er und gegebenenfalls in welchem Ausmaß er sich an die datenschutzrechtlichen Normen zu halten hat.

Die datenschutzrechtlichen Grundsätze sind die Folgenden:

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
2. Zweckbindung (Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden)
3. Datenminimierung (Datenspeicherungen dürfen nicht im großen Stil geschehen. Sie müssen jeweils dem Zweck angemessen sein)
4. Richtigkeit (Sachliche Richtigkeit der Daten)
5. Speicherbegrenzung (Daten sollen nur so lange als notwendig gespeichert werden)
6. Integrität und Vertraulichkeit (Schutz vor unbefugter oder unrechtmäßiger Verarbeitung/Verlust durch geeignete technische und organisatorische Maßnahmen)

Als praktische Beispiele dienen hier etwa Verschlüsselungsmechanismen bei der Datenaufbewahrung und auch das Ergreifen einfache Maßnahmen (zB versperrbare Räumlichkeiten).

Die Rechtmäßigkeit einer Verarbeitung gründet sich auf mindestens einer der folgenden Bedingungen:

- Einwilligung durch die betroffene Person zur Verarbeitung für einen oder mehreren bestimmten Zweck. Diese Einwilligung muss nachweisbar sein, dh am besten ist sie schriftlich zu erteilen. Die betroffene Person ist von ihrem Widerrufsrecht vor Abgabe der Einwilligung zu belehren. Das Einwilligungsersuchen muss in einer einfachen und klaren Sprache abgefasst werden. Weiters ist das Koppelungsverbot zu beachten, dh ein Vertragsabschluss darf nicht von der Zustimmung zur Datenverarbeitung abhängen. Bis zum Widerruf der Einwilligung wird die Rechtmäßigkeit der Verarbeitung nicht berührt. Die Einwilligungsfähigkeit ist in Österreich ab der Vollendung des 14. Lebensjahres gegeben (davon unberührt ist aber eine allfällige zusätzlich erforderliche Geschäftsfähigkeit).
- Vertragserfüllung
- Erfüllung einer rechtlichen Verpflichtung
- Lebenswichtige Interessen der betroffenen Personen oder einer anderen natürlichen Person sind betroffen
- Wahrnehmung einer Aufgabe im öffentlichen Interesse

RA Dr. Graciela Faffelberger LL.M.
Kärntner Ring 5-7, 7.Stock; 1010 Wien
office@legalmining.eu; www.legalmining.eu
+43 650 5107690

- Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen/Grundrechte/Grundfreiheiten der betroffenen Person überwiegen

Sollte der Verantwortliche Daten bei der betroffenen Person erheben, so unterliegt er Informationspflichten, wie etwa die Bekanntgabe von Namen und Kontaktdaten des Verantwortlichen (gegebenenfalls seines Vertreters und Datenschutzbeauftragten); Zwecke und die Rechtsgrundlage für die Verarbeitung; Empfänger und die Absicht der Übermittlung in ein Drittland/Internationale Organisation; Speicherdauer; Bestehen des Beschwerderechts an die Aufsichtsbehörde;

Der Verantwortliche wird in der Regel auch verpflichtet sein ein Verarbeitungsverzeichnis zu führen, das etwa die Zwecke der Verarbeitung, Beschreibung der Kategorien betroffener Personen und personenbezogener Daten, Name und Kontaktdaten des Verantwortlichen und etwaige Aufbewahrungsfristen zu enthalten hat. Generell gilt, dass es auch hier wieder auf den Einzelfall ankommen wird, wie detailliert das Verarbeitungsverzeichnis ausfallen wird. Das Verarbeitungsverzeichnis kann man sich auch selber in einer Excel-Tabelle erstellen. Wichtig ist, dass die Beschreibungen so gewählt werden, dass sich ein unbeteiligter Dritter ein Bild davon machen kann.

Exkurs: Newsletter und Ankündigungen

In diesem Zusammenhang ist auch auf die Regelungen des TKG zu verweisen. Telefonische Werbeanrufe sind ohne vorherige Zustimmung unzulässig. Die Zusendung von elektronischer Post, also auch Newslettern, ist grundsätzlich ohne Einwilligung des Empfängers unzulässig, wenn sie zu Zwecken der Direktwerbung erfolgt oder an mehr als 50 Empfänger gerichtet ist. Ausnahmen sind denkbar, wenn der Empfänger bereits Kunde ist und die Nachricht für eigene ähnliche Produkte oder Dienstleistungen erfolgt. Dem Empfänger muss weiters bei der Erhebung seiner E-Mail-Adresse und in jeder Mail eine kostenlose Widerrufsmöglichkeit geboten werden. Zu beachten ist auch, dass der Empfänger die Zusendung nicht von vornherein abgelehnt hat (vgl Robinson-Liste, Liste der RTR).

Auftragsverarbeiter:

Den Verantwortlichen trifft hinsichtlich der Person des Auftragsverarbeiters ein sogenanntes Auswahlverschulden; dh er muss sich vergewissern, dass er eine geeignete Person (hinsichtlich Fachwissens, Zuverlässigkeit und der Ressourcen) auswählt und hat dies auch fortlaufend zu überprüfen. Auch der Auftragsverarbeiter hat ein eigenes Verarbeitungsverzeichnis zu führen.

Datenschutzbeauftragter:

Sie können sowohl auf Seiten des Verantwortlichen als auch auf Seiten des Auftragsverarbeiters tätig sein. Sie sind als Kontaktstelle des Verantwortlichen zur Außenwelt konzipiert und unterliegen der Geheimhaltungspflicht. Innerhalb ihres Tätigkeitsradius sind sie weisungsfrei und unabhängig.

Die Ernennung eines Datenschutzbeauftragten kann **zwingend** (zB Verarbeitung wird von einer Behörde durchgeführt; oder die Kerntätigkeit besteht in umfangreichen, regelmäßigen und systematischen Überwachungen von betroffenen Personen bzw von besondere Datenkategorien gem Art 9) oder **fakultativ** sein. Er unterliegt einer erschwerten Kündigungsmöglichkeit und der Verantwortliche hat ihm die notwendigen Ressourcen (zB Weiterbildungen) zur Ausübung seiner Tätigkeit zur Verfügung zu stellen. Hervorzuheben ist, dass der Datenschutzbeauftragte nicht für die Einhaltung der Datenschutzbestimmungen verantwortlich gemacht werden kann, da er großteils nur beratende Funktionen hinsichtlich des Datenschutzrechts hat. Jedoch kann er sich gegenüber dem Verantwortlichen oder Auftragsverarbeiter für unzutreffende Beratung haftbar machen. Es empfiehlt sich entsprechendes vertraglich festzuhalten.

Betroffene Person:

Die betroffene Person hat mehrere Rechte; das prominenteste ist wohl das Recht auf Auskunft iZm Datenverarbeitungen ihrer personenbezogenen Daten. Der Verantwortliche hat ihr Auskunftsbegehren unverzüglich zu beantworten, jedoch sieht die DSGVO Maximalfristen vor. Im Falle von offenkundig unbegründeten oder exzessiven Auskunftsbegehren besteht seitens des Verantwortlichen die Möglichkeit ein Entgelt für die Auskunft zu verlangen. Weitere Rechte sind etwa das Recht auf Berichtigung, auf Einschränkung der Verarbeitung, auf Löschung, Datenportabilität und das Widerspruchsrecht (zB iZm Direktmarketing).

Dropbox&Co - Datenübermittlungen und Datensicherheit:

Datenübermittlungen innerhalb der Union sind zulässig, sofern sie rechtmäßig erfolgen.

Datenübermittlungen in ein Drittland/Internationale Organisationen sind prinzipiell nur dann zulässig, wenn der Verantwortliche/Auftragsverarbeiter die Bestimmungen der DSGVO einhält. Dies gilt auch für etwaige Weiterübermittlungen an ein weiteres Drittland/Internationale Organisation. Generell gilt der Grundsatz, dass durch die Datenübermittlung das Schutzniveau für die betroffene Person unterlaufen wird. Es gibt verschiedene rechtliche Instrumentarien, die diesem Umstand Rechnung tragen, so gelten etwa die Schweiz und Kanada als gleichgestellte Drittländer, aber auch die Verwendung von Standarddatenschutzklauseln können ein gleichwertiges Schutzniveau bewerkstelligen. Es ist daher unerlässlich vor der Datenübermittlung von personenbezogenen Daten zu prüfen, wohin die Daten übermittelt werden.

Im Fall, dass ein Datenleck vorliegt, hat der Verantwortliche generell eine Maximalfrist von 72 Stunden innerhalb derer er dies der zuständigen Aufsichtsbehörde zu melden hat. Zusätzlich kann es auch erforderlich sein, dass er die betroffenen Personen davon in Kenntnis setzen muss.

Rechtsfolgen:

Rechtsfolgen iZm einem Verstoß gegen das Datenschutzrecht können einerseits zivilrechtlicher als auch verwaltungsrechtlicher Natur sein: Zivilrechtlich kann Schadenersatz geltend gemacht werden, der auf Ersatz des materiellen und des immateriellen Schadens lauten kann. Die betroffene Person hat zusätzlich ein Beschwerderecht. Geldbußen werden von der Datenschutzbehörde verhängt. Gem DSGVO hängt die Bemessung ihrer Höhe (von bis zu 10.000.000 bzw 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 2% bzw 4% des weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahres, je nachdem welcher der Beträge höher ist) von verschiedenen Faktoren ab, wie etwa die Art, Schwere, Dauer des Verstoßes, Verschuldensgrad und Wiedergutmachungsmaßnahmen ab. Subsidiär dazu können andere Verstöße, wie zB man verweigert der Datenschutzbehörde Einsicht in die Datenverarbeitungsunterlagen zu geben, eine Geldstrafe von bis zu 50.000 EUR auslösen.

Zusätzlich ist auch ein Verstoß gegen Wettbewerbsrecht denkbar, der Schadenersatz und Unterlassungsansprüche begründen kann.

Soweit in diesem Handout auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Das Handout wird der IG Bildenden Kunst zur Verfügung gestellt und ist in seiner Gesamtheit urheberrechtlich geschützt. Hingewiesen wird, dass nach derzeitigem Stand (Stichtag 19.6.2018) noch keinerlei Rechtsprechung zum neuen Datenschutzrecht existiert. Die folgenden Informationen verstehen sich als genereller Überblick über das Datenschutzrecht und stellen weder Rechtberatung dar noch ersetzen sie eine solche.

ADVM-Code: R185706
UID: ATU 68592613
Erste Bank IBAN AT57 2011 1285 3751 0106 BIC: GIBAATWWXXX

RA Dr. Graciela Faffelberger LL.M.
Kärntner Ring 5-7, 7.Stock; 1010 Wien
office@legalmining.eu; www.legalmining.eu
+43 650 5107690