Grundlegendes zum Datenschutz für Immobilientreuhänder

© RA Dr. Thomas Schweiger, LL.M. (Duke)

Was ändert sich mit der Datenschutzgrundverordnung? (DSGVO und DSG)

Datenschutz ist der **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.

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.

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.

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).

Wer ist von der Datenschutzgrundverordnung betroffen?

Jeder Unternehmer, jede Firma und jedes Portal, welcher, welche oder welches in nur irgendeiner Art und Weise personenbezogene Daten erfasst oder verarbeitet, wird von der Datenschutzgrundverordnung 2018 erfasst. Das bedeutet vor allem mehr Verantwortung und ein sorgsamer Umgang mit allen personenbezogenen Daten, die das Unternehmen verarbeitet.

Was sind „personenbezogene“ Daten?

Geschützt ist die Verarbeitung von personenbezogenen Daten natürlicher Personen. Darunter sind all jene Angaben über Betroffene, auf deren Grundlage die Identität des Betroffenen bestimmt werden kann oder bestimmbar ist (z.B. Namen, Adressen, Geburtsdaten, Kontonummern, IP-Adressen etc.) zu verstehen. Unter „**Verarbeitung“** wird jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung verstanden (zB. die Erstellung einer Kundendatei, Aufnahme der Daten zur Erstellung einer Rechnung oder auch eine Mitarbeiterdatenbank, die Verwaltung der Newsletteradressen).

Unter welchen Voraussetzungen dürfen personenbezogene Daten verarbeitet werden?

Die Verarbeitung der Daten muss **„rechtmäßig“** sein, dh es muss mindestens eine der in der DSGVO genannten Rechtsgrundlagen gegeben sein. Entweder gibt es dafür eine (freiwillige, informierte) Einwilligung, einen Vertrag, der zwischen den Parteien abgeschlossen ist/wird, eine rechtliche/gesetzliche Verpflichtung des Verarbeiters, lebenswichtige Interessen der betroffenen Person, öffentliche Interessen oder ein überwiegend berechtigtes Interesse an der Verarbeitung der Daten. Die Verarbeitung der Daten muss einem **eindeutigen, festgelegten Zweck** (Zweckfestlegung) dienen, und die Daten dürfen nur für diesen konkreten Zweck verwendet werden (**Zweckbindung**). Im Sinne der Datenminimierung dürfen nur diejenigen Daten verarbeitet werden, die für den definierten Zweck notwendig sind und nicht darüber hinausgehen. Die verwendeten Daten müssen sachlich richtig sein (und auch auf dem neuesten Stand, wenn dies für den Verarbeitungszweck erforderlich ist).

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

- ### Rechtmäßigkeit
  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. die (freiwillige, informierte) Einwilligung, ein Vertrag, der zwischen den Parteien abgeschlossen ist/wird, eine rechtliche Verpflichtung des Verarbeiters, lebenswichtige Interessen der betroffenen Person, öffentliche Interessen oder ein überwiegend berechtigtes Interesse an der Verarbeitung.
- ### 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.

- Zweckbindung
  Die Verarbeitung der Daten muss einem **eindeutigen, festgelegten Zweck (Zweckfestlegung)** dienen, und die Daten dürfen nur für diesen konkreten Zweck verwendet werden **(Zweckbindung im eigentlichen Sinn)**.
- Datenminimierung
  Datenminimierung bedeutet, dass **nur diejenigen Daten verarbeitet werden dürfen**, die für den (definierten) Zweck **notwendig** sind und nicht darüber hinausgehen.
- 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.

Wann ist eine Einwilligung für die Datenverarbeitung notwendig?

Damit personenbezogene Daten verarbeitet werden dürfen, bedarf es **nur dann einer Einwilligung**, wenn die Verarbeitung **nicht zur Vertragserfüllung** notwendig, durch **berechtigte Interessen** gerechtfertigt, zur **Erfüllung einer gesetzlichen Verpflichtung** erforderlich oder im öffentlichen Interesse geboten ist. Für die gängige Datenverarbeitung, wie sie etwa in Hausverwaltungen im Rahmen der Miet- oder Wohnungseigentümerverwaltung erfolgt, wird – solange es sich nicht um sogenannte sensible Daten etwa zur Gesundheit, Religionsbekenntnis, Gewerkschaftszugehörigkeit etc. handelt – keine Einwilligung der Betroffenen erforderlich sein, da sich die Zulässigkeit der Datenverarbeitung auf den Rechtgrund der Vertragserfüllung der rechtlichen/gesetzlichen Verpflichtung stützt. Dies gilt ebenso für den Makler, der etwa allgemeine personenbezogene Daten von Interessenten zum Zweck der Interessentenverwaltung auf der Rechtsgrundlage der Vertragserfüllung bzw. der Anbahnung eines Vertrages verarbeitet.

Ein typisches Beispiel, das eine Einwilligung für die Datenverarbeitung erfordert, ist im Bereich des Marketings das »Newsletter-Abo«. Schon aus dem Telekommunikationsgesetz (§ 107) ergibt sich, dass für die Zusendung von Newslettern die Zustimmung notwendig ist, aber auch aus datenschutzrechtlicher Sicht ist dies erforderlich. Es kann kein anderer Grund für die Rechtmäßigkeit gem. Art. 6 (1) lit a bis f DSGVO beim „Newsletterversand“ herangezogen werden. Der »Hauptvertrag« (z.B. Alleinvermittlungsauftrag, Verwaltungsvertrag) selbst reicht nicht aus, denn bei Einwilligung muss das sogenannte Kopplungsverbot beachtet werden, d.h. die Einwilligung für Marketingmaßnahmen darf nicht im Hauptvertrag selbst (versteckt) enthalten sein, sondern der Kunde muss die Möglichkeit haben, den Hauptvertrag auch ohne den Zusatz „Marketingmaßnahmen“ abzuschließen. Die Einwilligung ist vom Verantwortlichen nachzuweisen, wenn er sich auf diese Art der Rechtsmäßigkeit

stützt, und der Kunde muss freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich in die Verarbeitung seiner Daten einwilligen. Der Kunde ist vor der Einwilligung über den Zweck derselben zu informieren und über seine Rechte nach der DSGVO (z.B. Auskunft, Löschung) und auf die Widerrufsmöglichkeit hinzuweisen. Der Widerruf muss so einfach möglich sein wie die Erteilung selbst. Die Anforderungen an die Einwilligung als Grundlage für die Verarbeitung von personenbezogenen Daten sind daher sehr hoch.

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO):

Mit dem in Kraft treten der DSGVO obliegt es den jeweiligen „Verantwortlichen" selbst, ein sogenanntes Verarbeitungsverzeichnis aller Verarbeitungen personenbezogener Daten zu führen, das auf Anfrage der Datenschutzbehörde vorzulegen ist. Um die Führung eines sogenannten Verarbeitungsverzeichnisses wird wohl kaum ein Unternehmen herumkommen, es sei denn, es verarbeitet personenbezogener Daten nur gelegentlich.

Der Mindestinhalt dieses Verzeichnisses entspricht, abgesehen von der Speicherdauer, im Wesentlichen dem Inhalt der bisherigen Meldung an das DVR. Das Verzeichnis soll die betreffenden Verarbeitungsvorgänge dokumentieren und der Aufsichtsbehörde als Ausgangspunkt für ihre Kontrollmaßnahmen dienen. Umgekehrt kann es in Anbetracht der hohen Strafen bei der Beweisführung helfen, um nachzuweisen, dass die Verarbeitung rechtmäßig erfolgte.

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. 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.

Wann ist ein Datenschutzbeauftragter zu bestellen?

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) umfasst oder bestimmte Datenarten (Art. 9/10-Daten) im Rahmen der Kerntätigkeit umfangreich verarbeitet werden.

Die große Mehrzahl der Immobilienmakler als auch Verwalter wird keinen DSB benötigen. Das Datenschutzgesetz sieht keine Ausweitung der Verpflichtung zur Bestellung eines Datenschutzbeauftragten vor. Dennoch kann es sinnvoll sein, dass ein Unternehmen eine oder mehrere Personen im Unternehmen benennt, die sich um die Angelegenheiten des Datenschutzes als »Daten-Manager«, d.h. zentrale Schnittstelle für personenbezogene Daten kümmern.

Wann ist eine Datenschutz-Folgenabschätzung notwendig?

Eine Datenschutzfolgeabschätzung (Art. 35 DSGVO oder englisch: DPIA oder PIA) ist dann erforderlich, wenn mit der Verarbeitung der Daten (insbes. bei der Verwendung neuer Technologien) ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen verbunden** ist. Hier ist zu dokumentieren, welche Risiken für die betroffene Person (nicht für die Organisation) durch die Datenverarbeitung gegeben sind. Diese Voraussetzungen wird bei der überwiegenden Zahl von Verarbeitungsvorgängen bei Immobilienmaklern (Kundeninformationssystem, Auftraggeberdatenverwaltung, Newslettertool, Bewerberverwaltung, Personalverwaltung) oder auch Verwaltern nicht der Fall sein. Die Datenschutzbehörde wird noch eine Liste von Verarbeitungen erstellen, bei denen eine DSFA notwendig bzw. nicht notwendig ist.

Informationspflichten: Worüber müssen Betroffene informiert werden?

(Datenschutzerklärung gem. Art. 13 und 14 DSGVO)

Die Personen, deren Daten verarbeitet werden, sollen Kenntnis darüber haben, welche konkreten Datenkategorien von welchem Verarbeiter für welchen Zweck wie lange verarbeitet werden. Daher sind umfassende Informationspflichten bei der Erhebung und Verwendung von Daten normiert.

Auch wenn vielfach keine Einwilligung in die Datenverarbeitung erforderlich sein wird, schreibt die DSGVO vor, dass der Verantwortliche den Betroffenen dennoch gewisse Informationen über die Datenanwendungen zur Verfügung zu stellen hat. Diese Datenschutzinformation hat den Namen und die Kontaktdaten des Verantwortlichen (und ggf. seiner Vertreter), Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung, die Kategorien personenbezogener Daten, die verarbeitet werden und ggf. Empfänger der Daten zu enthalten. Die Informationen sind den Betroffenen zum Zeitpunkt der Erhebung der Daten zur Verfügung zu stellen. Es empfiehlt sich daher, eine Datenschutzinformation anzufertigen, die bereits beim ersten Kontakt dem Kunden bzw. betroffenen Vertragspartner (z.B. beim Abschluss des Vermittlungsauftrags, Mietvertragsabschluss etc.) ausgehändigt werden kann oder zumindest einen Hinweis zu erteilen, dass personenbezogene Daten verarbeitet werden und wo allenfalls weitere Datenschutzinformationen etwa auf der Website abgerufen werden können (z.B.: *[Firmenwortlaut] verarbeitet personenbezogene Daten nach den datenschutzrechtlichen Bestimmungen. Weitergehende Informationen sind unter … zu finden.*)

Ein Hinweis auf die Datenschutzinformation könnte ebenso in der Korrespondenz (etwa im email-Footer, Briefpapier etc.) oder allenfalls auch in den jeweiligen Verträgen implementiert werden.

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. Die Informationspflicht trifft nach der DSGVO immer den **datenschutzrechtlichen Verantwortlichen.**

Rechte von betroffenen Personen

Die DSGVO räumt Betroffenen auch das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung sowie das Recht auf Datenübertragbarkeit ein. Betroffene (z.B. Interessenten, Mieter oder Wohnungseigentümer) könnten Auskunft darüber verlangen, ob bzw. welche personenbezogenen Daten von ihm/ihr gespeichert werden, was die Rechtsgrundlage der Verarbeitung ist und an wen gegebenenfalls diese Daten übermittelt wurden.

Die Informationen sind grundsätzlich kostenlos binnen eines Monats zu erteilen. Fraglich ist, wie weit diese Auskunftspflicht reicht? Gem. Art 15 DSGVO hat der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Hierbei kann es sich um emails, Briefe, Auszüge aus Datenbanken, Befunde etc. handeln. Zu hinterfragen ist, ob dies auch für Dokumente und Korrespondenz gilt, von denen der Betroffene bereits Kenntnis hat (etwa emails, die der Betroffene selbst an das Unternehmen geschickt hat oder Dokumente, die ihm bereits einmal ausgehändigt wurden).

Im Unternehmen ist organisatorisch, technisch und auch rechtlich sicherzustellen, dass den Rechten der betroffenen Person (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Datenübertragbarkeit) 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 mögliche Ausübung der Betroffenenrechte vorbereitet zu sein.

Was ist bei einer Datenschutzverletzung zu tun? (Data Breach Notification)

Eine Datenschutzverletzung liegt z.B. dann vor, wenn personenbezogene Daten an unbefugte Personen zu gelangen drohen, so z.B. wenn ein USB-Stick mit Daten über Kunden verloren geht, oder auch bei einem Hackerangriff über die Website auf eine Datenbank mit personenbezogenen Daten oder einem fehlgeleiteten Email oder der Versendung eines Newsletters oder einer Einladung zu einer Veranstaltung ohne Verwendung der bcc-Funktion im Email.

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. Diese 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.

Datenverarbeitung im Beschäftigungskontext

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

Geht man von den derzeitig verhängten Geldstrafen (z.B. EUR 700,00 für eine nicht registrierte Videoüberwachung) aus, dann sind die potentiellen Geldbußen, die Unternehmern gem. der DSGVO (Art. 83 DSGVO, § 30 DSG) nach dem 25. Mai 2018 drohen, wesentlich höher und können bis zu **EUR 20.000.000** bzw. 4 % des weltweiten Gesamtumsatzes betragen (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.
Festzuhalten ist, dass es nicht darauf ankommt, dass es zu einer konkreten Datenschutzverletzung kommt, damit eine Geldbuße verhängt werden kann. Die DSGVO geht davon aus, dass sich die Unternehmen an die Bestimmungen halten, dies auch dokumentieren und dann gegenüber der Behörde im Rahmen der Nachweisverpflichtung auch Rechenschaft ablegen. Wenn ein Unternehmen daher den Verpflichtungen, die sich aus der DSGVO ergeben, nicht nachkommt, und z.B. kein Verzeichnis von Verarbeitungstätigkeiten führt, die Informationsverpflichtungen bei der Datenerhebung vernachlässigt oder keine Einwilligungen zur Verarbeitung personenbezogener Daten nachweisen kann, sofern diese notwendig sind, dann wird es erhebliche Geldbußen geben, die nicht nur spezialpräventiven, sondern auch generalpräventiven Charakter haben sollen, um andere Unternehmen dazu anzuhalten, die Verantwortung nach der DSGVO für die Verarbeitung personenbezogener Daten ordnungsgemäß wahrzunehmen.

Bildverarbeitung (Videoüberwachung)

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 berechtigte 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.

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.

Welche Maßnahmen sollten gesetzt werden?

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 Risikos**, 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 **DSB** 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.