WIRTSCHAFTSKAMMER WIEN
Werbung · Marktkommunikation

DATENSCHUTZ-GRUNDVERORDNUNG

„Fragen & Antworten mit dem Focus auf die Markt- und Meinungsforschung“

Marco Schreuder

Dr. Bertram Barth

Liebes Mitglied,

die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) und das daraus resultierende Datenschutzgesetz 2018 (DSG 2018) haben umfassende Änderungen für die Verarbeitung personenbezogener Daten gebracht. Im Zuge dessen wurden im Forschungsorganisationsgesetz (FOG) spezielle Datenschutzbestimmungen für den Bereich Wissenschaft und Forschung niedergeschrieben.

Durch diese Gesetzesänderungen ergeben sich neue Herausforderungen für Markt- und Meinungsforschungsinstitute, deren täglich Brot es ist, personenbezogene Daten zu verarbeiten. Dementsprechend groß war die Verunsicherung aufseiten unserer Mitglieder.

Die am häufigsten gestellten Fragen beantworten wir in dieser Broschüre, die als Kooperationsprojekt der Fachgruppe Werbung und Marktkommunikation Wien und dem Verband der Markt- und Meinungsforschungsinstitute Österreichs entstanden ist.

Wir hoffen, mit diesen FAQ Unklarheiten beseitigen und Ihnen die Arbeit etwas erleichtern zu können.

Mit den besten Grüßen

Marco Schreuder
Obmann
Fachgruppe Werbung und
Marktkommunikation Wien

Dr. Bertram Barth
Vorstandsvorsitzender
Verband der Markt- und Meinungsforschungsinstitute Österreichs

INHALTSVERZEICHNIS

Einleitung

Seit 25. Mai 2018 gilt in Österreich die Datenschutz-Grundverordnung (DSGVO).

Gleichzeitig mit der Datenschutz-Grundverordnung wurde in Österreich das Datenschutzgesetz 2018 (DSG 2018) erlassen, welches zusätzliche Regelungen für den österreichischen Datenschutz enthält. Bereits im Zuge des Gesetzgebungsverfahrens zum DSG 2018 zeichnete sich ab, dass nicht nur eine Anpassung bzw. Präzisierung der allgemeinen Bestimmungen des Datenschutzes, sondern auch hinsichtlich der speziellen Bestimmungen etwa für den Bereich Wissenschaft und Forschung notwendig ist.

Diese datenschutzrechtlichen Spezialbestimmungen haben Eingang in das Forschungsorganisationsgesetz (FOG) gefunden, welches ebenfalls seit 25.05.2018 in Österreich gilt.

Diese umfassenden Gesetzesänderungen stellen Markt- und Meinungsforschungsinstitute, welche naturgemäß sehr viele personenbezogene Daten verarbeiten, vor neue Herausforderungen. Vor diesem Hintergrund hat der Verband der Markt- und Meinungsforschungsinstitute Österreichs (VdMI) in Kooperation mit der Wirtschaftskammer Wien häufig gestellten Fragen einer Beantwortung zugeführt.

PERSONENBEZOGENE DATEN UND ANWENDUNGSBEREICH DER DSGVO

(ART 2,3 UND 4 DSGVO)

1) Wo ist der Datenschutz in Österreich geregelt?

Der Kern des Datenschutzrechtes in Österreich findet sich in der EU-Datenschutzgrundverordnung (DSGVO) und im Datenschutzgesetz 2018 (DSG 2018). Weitere datenschutzrechtliche Einzelbestimmungen finden sich in zahlreichen Materiengesetzen. Für Markt- und Meinungsforschung sind zusätzlich die Datenschutzbestimmungen im Forschungsorganisationsgesetz (FOG) relevant.

2) Was sind personenbezogene Daten?

Die DSGVO definiert personenbezogene Daten als Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen. Personenbezogene Daten sind daher sämtliche Informationen, die sich mit einer bestimmten Person eindeutig in Verbindung bringen lassen (wobei die Person dem Verantwortlichen der Datenverarbeitung nicht bekannt sein muss).

Personenbezogene Daten sind beispielsweise der Name, das Geburtsdatum, die Adresse des Wohn- oder Arbeitsortes, eine Telefonnummer oder eine E-Mail-Adresse. Aufgrund des weiten Begriffs der personenbezogenen Daten fallen darunter aber beispielsweise auch Tonaufnahmen, die einer Person zugeordnet werden können, die Einkaufshistorie in einem Onlineshop oder persönliche Präferenzen.

Ob ein Personenbezug vorliegt ist von hoher Relevanz, weil davon die Anwendung der datenschutzrechtlichen Gesetze (insb DSGVO und DSG 2018) abhängt. Daten, die keinen Personenbezug aufweisen, unterliegen nicht dem Datenschutz.

3) Ich verarbeite Daten von Personen, ohne deren Namen zu kennen. Sind das personenbezogene Daten?

Daten sind dann personenbezogen, wenn sie auf eine identifizierte oder identifizierbare Person beziehen, wobei es nicht erforderlich, ist, dass die Person dem Verantwortlichen tatsächlich bekannt ist.

Ein Personenbezug kann daher grundsätzlich auch bei der Verarbeitung von Daten bestehen, obwohl dem Verantwortlichen die betroffene Person, wie etwa der Inhaber der Nummer, namentlich nicht bekannt ist. Auch auf solche Daten sind die Datenschutzgesetze anwendbar. (Für weitere Informationen siehe auch Fragen 4 und 5)

4) Ab wann liegt ein Personenbezug vor, wenn ich den Namen des Betroffenen nicht kenne?

Die Frage hängt maßgeblich davon ab, wann die Identifizierbarkeit einer Person anzunehmen ist. Pseudonymisierte Daten (vgl Frage 10) gelten jedenfalls als personenbezogene Daten. In anderen Bereichen ist die Abgrenzung schwieriger und durchaus umstritten.

Grundsätzlich kommt es auf die Möglichkeit des Verantwortlichen an, von der Identität der betroffenen Person Kenntnis zu erlangen. Verfügt er über technische, finanzielle oder organisatorische Möglichkeiten, eine Information einer bestimmten Person zuzuordnen, ist er in der Lage die Person zu identifizieren. In diesem Fall liegt ein Personenbezug vor. Ob eine Zuordnung tatsächlich erfolgt ist, ist nicht ausschlaggebend. Es kommt bloß auf die entsprechende Möglichkeit an.
Deshalb kann aufgrund unterschiedlicher Möglichkeiten eine Information für den einen Verantwortlichen personenbezogen sein, für einen anderen hingegen nicht.

Vor diesem Hintergrund ist beispielsweise für den Betreiber einer Website eine dynamische IP-Adresse regelmäßig kein personenbezogenes Datum, weil dieser mit vernünftigen Mitteln keine Zuordnung der IP-Adresse zu einer Person vornehmen kann. Für den Anbieter des Internet-Dienstes (Service-Provider) sind dynamische IP-Adressen hingegen schon personenbezogene Daten, weil dieser über Informationen verfügt, um die dynamischen IP-Adressen einzelnen Rechnern und damit deren Inhaber zuzuordnen.

5) Sind im RLD-Verfahren generierte Telefonnummern personenbezogene Daten?

Eine künstlich generierte Telefonnummer stellt grundsätzlich noch kein personenbezogenes Datum dar, wenn der Verantwortliche mit vernünftigen technischen, finanziellen oder organisatorischen Möglichkeiten nicht in der Lage ist, den Inhaber des Anschlusses festzustellen. Dies wäre beispielsweise der Fall, wenn er für die Herstellung eines Personenbezuges die Hilfe eines Dritten benötigt, wie etwa des Anschlussinhabers oder des Telefondienst-Anbieters.

Zu berücksichtigten ist allerdings, dass viele Telefonnummern bereits online abgerufen werden können und deshalb für solche Telefonnummern mit einfachen Mitteln ein Personenbezug herstellt werden kann, weshalb in solchen Fällen auch die DSGVO zu berücksichtigen ist.

Vor dem Hintergrund, dass eine Überprüfung, ob ein Personenbezug im Einzelfall, dh für jede Telefonnummer, gegeben ist, nicht tunlich ist, sollten solche Telefonnummern grundsätzlich als personenbezogene Daten behandelt werden.

6) Gilt die DSGVO auch für handschriftliche Aufzeichnungen oder Aktenordner?

Die DSGVO gilt
(1) für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten
(2) sowie für die nichtautomatisierte („händische") Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

„Dateisystem" ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird, wobei die Ordnungskriterien, nach welchen die Strukturierung des Dateisystems erfolgt, personenbezogen sein muss und die personenbezogenen Daten im Dateisystem über eine bestimmte Person leicht wiederauffindbar sein müssen.

Die DSGVO wäre beispielsweise auf einen Ordner, der nach Nachnamen strukturiert ist, anwendbar, nicht aber auf einen Ordner der chronologisch sortiert ist, sofern keine zusätzlichen Hilfsmittel vorhanden sind, die eine leichte Auffindbarkeit gewährleisten, wie etwa eine Liste, auf der vermerkt ist, bei welchem Datum sich Informationen über bestimmte Personen befinden.

7) Was sind besondere Datenkategorien?

Besondere Datenkategorien wurden, bevor die DSGVO in Geltung trat, als „sensible Daten" bezeichnet.

Darunter versteht man personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Unter politischen Meinungen fallen zum Beispiel neben offensichtlichen Informationen, wie etwa die ausdrückliche Nennung der Parteizugehörigkeit, auch jene Informationen, aufgrund derer auf eine besondere Datenkategorie (sensibles Datum) geschlossen werden kann, wie die Teilnahme an einer Demonstration oder Wahlkundgebung. Unter religiöse oder weltanschauliche Überzeugungen können auch die Mitgliedschaft in einer Organisation oder die Verweigerung bestimmter Nahrungsmittel (aus religiösen Gründen) oder die Teilnahme an bestimmten Veranstaltungen fallen.

Keine besonderen Datenkategorien sind all jene, die nicht eingangs aufgezählt wurden, wie etwa das Geburtsdatum, Bankdaten, oder auch Passwörter für das Online-Banking. Dass für den Betroffenen im Fall der unbefugten Verarbeitung/Verwendung solcher Daten durch Dritte ein wesentlich höheres Risiko bestehen kann, bleibt bei der Beurteilung, ob besondere Datenkategorien vorliegen, unberücksichtigt.

8) Ist auch eine Sozialversicherungsnummer ein Datum der besonderen Kategorie und warum wird diese so oft in der Datenverarbeitung verwendet?

Die Sozialversicherungsnummer ist ein Personenkennzeichen. Personenkennzeichen sind alphanumerische Zeichen, die einer Person eindeutig (ähnlich wie eine „Nummern-Tafel" bei einem PKW) zugeordnet sind. Solche Personenkennzeichen erlauben in einer Datenbank, das einfache Auffinden von redundanten Einträgen („Datenzwillinge") und ermöglichen die Zusammenführung unterschiedlicher Datenbanken und daher die Erstellung umfassender Persönlichkeitsprofile. Aufgrund dieser Eigenschaften findet die Sozialversicherungsnummer oftmals Anwendung in der Datenverarbeitung.

Die Verarbeitung der Sozialversicherungsnummer ist aber nur zu bestimmten Zwecken erlaubt, nämlich für die Verwaltung personenbezogener Daten für Zwecke der Sozialversicherung. Aus dieser gesetzlichen Zweckvorgabe ist abzuleiten, dass jede rechtmäßige Verwendung dieser Nummer für andere Zwecke auf einer gesetzlichen Ermächtigung beruhen muss.

Unter dem mittlerweile außer Kraft getretenen Datenschutzgesetz 2000 stellte Sozialversicherungsnummer keine besondere Datenkategorie dar. Anders ist diese Frage nunmehr unter der DSGVO zu beurteilen, weil gemäß den Erwägungen zur DSGVO zu den besonderen Datenkategorien auch Nummern gehören, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren. Die Sozialversicherungsnummer weist all diese Eigenschaften auf. Daher ist von einer besonderen Datenkategorie auszugehen.

9) Sind personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten besondere Datenkategorien?

Die DSGVO unterscheidet besondere Datenkategorien (gemäß Art 9 DSGVO) und Daten über strafrechtliche Verurteilungen und Straftaten besondere Datenkategorien (gemäß Art 10 DSGVO). Folglich sind – entgegen der landläufig oftmals anzutreffenden Meinung – Daten über strafrechtliche Verurteilungen und Straftaten keine besonderen Datenkategorien, aber unterliegen ebenfalls einem besonderen Schutz gemäß DSGVO und DSG 2018.

Beispiele für Daten über strafrechtliche Verurteilungen und Straftaten sind: Einträge aus dem Strafregisterauszug über gerichtliche Verurteilungen in Form von bedingten und unbedingten Haftstrafen, bereits verbüßte Haftstrafen, vorbeugende Maßnahmen (wie etwa die Unterbringung einer Anstalt für geistig abnorme oder entwöhnungsbedürftige Rechtsbrecher), Bewährungsauflagen, Weisungen etc.

Für weitere Informationen zur Verarbeitung solcher Daten, siehe Frage: 17).

10) Was sind pseudonymisierte Daten und ist die DSGVO auf diese Daten anwendbar?

Unter Pseudonymisierung versteht man die Verarbeitung von personenbezogenen Daten in der Weise, dass die Person, auf die sich diese personenbezogenen Daten beziehen, ohne zusätzliche Information nicht mehr identifiziert werden kann.
Ein einfaches Beispiel ist die Verwendung von Nummern (oder eines anderen beliebigen „Pseudonyms") anstatt des vollständigen Namens in einer Datenbank.

Die Zusatzinformation, welcher Name welcher Nummer zugeordnet ist, unterliegt in der Regel besonderen technischen und organisatorischen (Schutz-)Maßnahmen, wie etwa einer stark eingeschränkten Zugriffs- oder Zugangsbefugnis einer Verschlüsselung etc. Der Verantwortliche einer solchen Datenbank ist daher in der Lage die Pseudonymisierung aufzuheben.

Die Pseudonymisierung ist einerseits eine Maßnahme, um sicherzustellen, dass nicht mehr Daten verarbeitet werden, als für die Zweckerreichung notwendig ist (in vielen Fällen ist etwa der Name des Befragten für die Durchführung einer Umfrage irrelevant) und dient andererseits zur Erhöhung des Schutzes der personenbezogenen Daten, weil eine Identifikation der einzelnen Personen ohne der Zusatzinformation nicht möglich ist.

Solche Daten sind trotz Pseudonymisierung weiterhin als personenbezogene Daten anzusehen, weshalb die Vorschriften der DSGVO und des DSG 2018 uneingeschränkt auf pseudonymisierte Daten zur Anwendung gelangen.

Eine Pseudonymisierung kann zur Vermeidung von Risiken für die betroffenen Personen erforderlich sein. Unabhängig davon erlaubt die DSGVO unter gewissen Voraussetzungen Verarbeitungen für pseudonymisierte Daten, die für nicht pseudonymisierte Daten unzulässig sein können, wie etwa

- Weiterverarbeitung zu einem anderen Zweck oder
- Zulässigkeit der Verarbeitung für im öffentlichen Interesse liegende Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken.

11) Was sind anonymisierte Daten und ist die DSGVO auf diese Daten anwendbar?

Bei der Anonymisierung werden personenbezogene Daten in der Form verändert, dass die Person, auf die sich die personenbezogenen Daten beziehen, nicht (bzw nicht ohne unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft) mehr identifiziert werden kann.

Eine Anonymisierung kann durch schlichtes endgültiges Vernichten des Personenbezuges erfolgen (etwa durch das Löschen von Name und Geburtsdatum aus einer Datenbank) oder durch das Aggregieren von Daten zu einer Information, die keinen Personenbezug mehr zulässt (wie etwa „Das Medianeinkommen in Österreich beträgt EUR xy“) und Löschen jener personenbezogenen Daten, aus denen die Information abgeleitet wurde. Sie kann ferner auch dadurch erfolgen, dass die für die Pseudonymisierung erforderliche Zusatzinformation (vergleiche Frage 10) endgültig vernichtet wird.

Zu beachten ist in diesem Zusammenhang, dass je mehr Informationen über eine bestimmte Person vorhanden sind (beispielsweise Einkommen, Auflistung der Hauptwohnsitze, Krankheitsgeschichte, körperliche Merkmale etc), die theoretische Möglichkeit steigt, dass ein Personenbezug hergestellt werden kann. Welche Schritte für eine Anonymisierung erforderlich sind, muss daher im Einzelfall beurteilt werden.

Auf anonymisierte Daten ist weder die DSGVO noch das DSG 2018 anwendbar, weshalb bei der Verarbeitung solcher Daten keine datenschutzrechtlichen Aspekte zu berücksichtigen sind.

12) Gibt es einen besonderen Schutz für Minderjährige?

Die DSGVO nimmt an mehreren Stellen Bezug auf „Kinder“ und sieht diese als schutzbedürftigen natürlichen Personen an, weshalb unter anderem bei der Interessensabwägung, die schutzwürdigen Interessen von Kindern eine besonderes Gewicht haben, und bei der Erfüllung der Informationspflicht durch den Verantwortlichen einer Datenverarbeitung die Information, die sich speziell an Kinder richtet, in

einer besonders klaren und einfachen Sprache zu erfolgen hat. Auch bei der Datenschutz-Folgenabschätzung sind die Risiken, die Kinder betreffen, besonderes zu berücksichtigen.

Die DSGVO (in Verbindung mit dem DSG 2018) enthalten darüber hinaus eine spezielle Bestimmungen für die wirksame Einwilligung eines Kindes/Minderjährigen, der das 14. Lebensjahr noch nicht vollendet hat. In Bezug auf Dienste der Informationsgesellschaft benötigen die Kinder/Minderjährigen zusätzlich die Einwilligung ihres Erziehungsberechtigen.

Unter Dienste der Informationsgesellschaft versteht man Dienste, die in der Regel gegen Entgelt, ausschließlich elektronisch, im Fernabsatz und auf individuellen Abruf erbracht werden, wie etwa Online-Shops aber auch Video-on-Demand-Dienste etc.

GRUNDSÄTZE DER DATENVERARBEITUNG

(ART 5 UND 6 DSGVO)

13) Was ist bei jeder Datenverarbeitung zu beachten (Grundsätze der Datenverarbeitung)?

Im Zusammenhang mit jeder Datenverarbeitung müssen die nachstehenden Grundsätze eingehalten werden, andernfalls eine unzulässige Datenverarbeitung vorliegt, wofür hohe Strafen durch die Datenschutzbehörde verhängt werden können.

Die Grundsätze für die Verarbeitung von personenbezogenen Daten lauten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Die Verarbeitung ist nur aufgrund einer Rechtsgrundlage und in transparenter Weise zulässig, wobei die Prinzipien von Treu und Glauben anzuwenden sind; für weitere Informationen siehe Frage 14).
- Zweckbindung (Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden).
- Datenminimierung (Beschränkung der Datenerhebung und -verarbeitung auf das notwendige Maß).
- Richtigkeit (Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein).
- Speicherbegrenzung (Speicherung der Daten nur solange, wie es für die Zweckerreichung erforderlich ist; für weitere Informationen siehe Frage 18).
- Integrität und Vertraulichkeit (Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung/Veränderung).

Jede Datenverarbeitung ist in regelmäßigen Abständen zu überprüfen, ob die oben genannten Grundsätze (noch) eingehalten werden.

14) Wir verarbeiten Daten, die zu keiner besonderen Datenkategorie gehören. Welche Rechtsgrundlagen gibt es für eine solche Verarbeitung?

Jede Datenverarbeitung muss sich auf eine gültige Rechtsgrundlage stützen können (Rechtmäßigkeit der Verarbeitung).

Eine Verarbeitung von Daten, die keine besonderen Datenkategorien sind, ist aufgrund folgender Rechtsgrundlagen zulässig:

- Einwilligung des Betroffenen;
- Erfüllung eines Vertrages, dessen Vertragspartei der Betroffene ist (einschließlich vorvertraglicher Maßnahmen, die auf Anfrage des Betroffen erfolgen);
- Erfüllung einer rechtlichen Verpflichtung, die der Verantwortliche unterliegt;
- zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person;
- Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen der betroffenen Person, überwiegen;

Für besondere Datenkategorien besteht ein eigener Katalog an Rechtsgrundlagen. Für weitere Informationen siehe Frage 16).

15) Brauche ich in jedem Fall eine Einwilligung des Betroffenen für meine Datenverarbeitung?

Nein, wie unter Frage 14) dargestellt, gibt es mehrere Rechtsgrundlagen, aufgrund derer eine Verarbeitung zulässig ist.

In Fällen, in denen eine andere Rechtsgrundlage zur Anwendung gelangt, ist es nicht notwendig und oftmals auch nicht zielführend, zusätzlich eine Einwilligung einzuholen, weil die Einholung und Verwaltung von Einwilligungen regelmäßig mit einem hohen Verwaltungsaufwand verbunden ist. Ferner kann eine Einwilligung jederzeit durch den Betroffenen widerrufen werden.
Beruft sich der Verantwortliche nach dem Widerruf einer Einwilligung auf eine (ohnehin vorhandene) alternative Rechtsgrundlage, kann dies zu Irritationen beim Betroffenen führen, weil dieser aufgrund der eingeholten Einwilligung davon ausgeht, dass die Verarbeitung nur mit seiner Zustimmung erlaubt sei.

Einwilligungen sollten daher nur in jenen Fällen eingeholt werden, in denen sie mangels alternativer Rechtsgrundlage erforderlich sind sowie möglicherweise vorsichtshalber in Fällen, bei denen nicht eindeutig feststeht, ob eine alternative Rechtsgrundlage gegeben ist, wie etwa im Fällen bei denen die Interessensabwägung für das überwiegende berechtigte Interesse nicht eindeutig zugunsten des Verantwortlichen ausschlägt.

16) Was ist bei der Verarbeitung von Daten der besonderen Kategorie zu beachten?

Zu beachten ist, dass für besondere Datenkategorien ein eigener Katalog an Rechtsgrundlagen besteht.

Unter anderem ist gemäß DSGVO die Verarbeitung besonderer Datenkategorien aufgrund ausdrücklicher Einwilligung des Betroffenen, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, oder zum Schutz lebenswichtiger Interessen des Betroffenen zulässig.

Darüber hinaus können die Mitgliedstaaten im nationalen Recht zusätzliche gesetzliche Rechtsgrundlagen schaffen, wie etwa im Fall einer (erforderlichen) Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses oder für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

Der österreichische Gesetzgeber hat von dieser Möglichkeit Gebrauch gemacht, und mit dem Forschungsorganisationsgesetz (FOG) eine solche zusätzliche gesetzliche Rechtsgrundlage geschaffen, weshalb die Verarbeitung besonderer Datenkategorie im wissenschaftlichen Bereich bei Vorliegen der Voraussetzungen auf diese Rechtsgrundlage gestützt werden kann.

Das „überwiegende berechtigte Interesse des Verantwortlichen" ist als Rechtsgrundlage für die Verarbeitung von besonderen Datenkategorien nicht vorgesehen.

17) Was ist bei der Verarbeitung im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten zu beachten?

Eine Verarbeitung solcher Daten ist nur unter behördlicher Aufsicht oder auf Grundlage nationaler Erlaubnisbestimmungen zulässig. Der Österreichische Gesetzgeber hat von dieser Möglichkeit Gebrauch gemacht, allerdings ist die gesetzliche Bestimmung sehr vage:

Gemäß DSG 2018 ist die Verarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 lit. f DSGVO erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und dem DSG 2018 gewährleistet.

Vereinfacht gesagt, kann sich ein Verantwortlicher bei der Verarbeitung solcher Daten gegebenenfalls auf sein überwiegendes berechtigtes Interesse stützen und er entsprechende Vorkehrungen zum Schutz der Daten trifft.

In vielen Fällen ist mit einer solchen Verarbeitung allerdings die Pflicht zur Durchführung Datenschutz-Folgenabschätzung und zur Ernennung eines Datenschutz-Beauftragten verbunden. Ferner ist in diesem Fall die (unter bestimmten Voraussetzungen zur Anwendung gelangende) Ausnahmebestimmung zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten nicht anwendbar (für nähere Informationen zur Ausnahmebestimmung siehe Frage 51).

18) Wie lange dürfen Daten gespeichert werden?

Grundsätzlich gilt, dass personenbezogene Daten nur solange gespeichert werden dürfen, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Vor diesem Hintergrund kann eine Beurteilung für jede Datenkategorie nur im Einzelfall erfolgen.

Personenbezogene Daten, die für die Abwicklung eines Vertrages gespeichert werden, können beispielsweise bis zur Durchführung des Vertrages und darüber hinaus solange gespeichert werden, wie die Vertragspartner Rechtansprüche aus dem Vertrag geltend machen können.

Darüber hinaus kann der Verantwortliche einer Datenverarbeitung besonderen gesetzlichen Vorschriften unterliegen, die eine Aufbewahrung über den Verarbeitungszweck hinaus erforderlich machen. Steuerrechtliche und Unternehmensrechtliche Vorschriften sehen unter bestimmten Voraussetzungen eine Aufbewahrungspflicht im Ausmaß von sieben Jahren vor.

Eine Beurteilung der Speicherdauer muss, falls erforderlich, im Einzelfall für jede Datenkategorie einzeln erfolgen. So wird nach der Auflösung eines Dienstverhältnisses mit einem Mitarbeiter in der Regel eine Löschung des Fotos des Mitarbeiters erforderlich sein. Hingegen sind jene Daten, die für die Ausstellung eines Dienstzeugnisses erforderlich sind, 30 Jahre zu speichern.

Eine besondere Ausnahme gilt gemäß § 2d Abs 5 Forschungsorganisationsgesetz (FOG). Aufgrund dieser Bestimmung dürfen personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken grundsätzlich unbeschränkt gespeichert und gegebenenfalls sonst verarbeitet werden, sofern dies für die Verarbeitungszwecke erforderlich ist soweit gesetzlich keine zeitlichen Begrenzungen vorgesehen sind. Zu berücksichtigen ist allerdings, dass es sich hierbei um eine „Zweifelsregelung" handelt. Dies bedeutet, dass personenbezogene Daten, sofern der Zweck der Verarbeitung erreicht wurde, zu löschen sind.

19) Wie lange darf ich die Daten von potentiellen Kunden und/oder Interessenten aufbewahren?

Unter Interessent wird eine Person verstanden, die Interesse an einem Unternehmen bekundet hat, ohne dass es zu einem Vertragsabschluss gekommen ist.

Grundsätzlich gilt auch in diesem Fall, dass die Speicherung von personenbezogenen Daten von potentiellen Kunden und Interessenten solange zulässig ist, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Die mittlerweile außer Kraft getretene Standard- und Musterverordnung 2004 führte für solche Fälle als Höchstdauer der zulässigen Datenaufbewahrung bei Interessenten eine Dauer von drei Jahren nach dem letzten Kontakt mit dem Verantwortlichen durch den Interessenten an. Die Orientierung an diesem Zeitraum wird (trotz des Umstandes, dass die Standard- und Musterverordnung nicht mehr in Kraft ist) zulässig sein.

Der Fall von potentiellen Kunden oder Interessenten darf nicht mit Fällen gleichgesetzt werden, bei denen aus dem potentiellen Kunden bzw. Interessenten tatsächlich ein Vertragspartner wurde,

weil sich in diesem Fall, die Zwecke der Datenverarbeitung maßgeblich ändern und darüber hinaus gesetzliche Aufbewahrungspflichten zum Tragen kommen können. Für weitere Informationen vergleiche Frage 18).

20) Müssen personenbezogene Daten auch aus Backup-Datenträger und Sicherungskopien gelöscht werden?

Grundsätzlich gilt, dass personenbezogene Daten auch aus Backup-Datenträgern und Sicherungskopien zu löschen sind.

Das Problem, das sich für viele Verantwortliche in diesem Zusammenhang stellt, ist, dass zwar personenbezogene Daten aus dem aktiven System vergleichsweise einfach gelöscht werden können, allerdings die Daten sich mehrfach kopiert auf Backup-Datenträgern und Sicherungskopien befinden. Die Löschung solcher Backup-Datenträger und Sicherungskopien ist oftmals mit einem erheblichen technischen Aufwand verbunden.

Das DSG 2018 erlaubt eine Löschung zu einem späteren Zeitpunkt, falls die Löschung nicht unverzüglich erfolgen kann, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann. Dies kann bei sogenannten „Abbildungen (images)" von Festplatten der Fall sein, welche nicht einfach verändert werden können, sondern es zuerst einer Übertragung der gesamten Sicherungskopie in das operative System bedarf.

Unter bestimmten Voraussetzungen – unter anderem, dass die Sicherungskopien regelmäßig gelöscht werden – ist es nicht erforderlich, die Daten gesondert aus den Sicherungskopien zu löschen, sondern kann mit der Löschung zugewartet werden, bis die gesamte Sicherungskopie routinemäßig gelöscht oder überschrieben wird.

21) Ist eine Übermittlung von personenbezogenen Daten außerhalb des EWR-Raumes (Geltungsbereiches der DSGVO) zulässig und was muss dabei beachtet werden?

Für die Übermittlung von personenbezogenen Daten außerhalb des EWR-Raumes (oder an eine internationale Organisation) geltend besondere Vorschriften, weil außerhalb des EWR-Raumes die DSGVO nicht unmittelbar anwendbar ist.

Eine Übermittlung ist nur zulässig, wenn durch den Verantwortlichen oder den Auftragsverarbeiter geeignete Garantien getroffen wurden, dass das durch die DSGVO gewährleistete Schutzniveau nicht untergraben wird. In der Praxis werden regelmäßig sogenannte „Europäische Standard-Vertragsklauseln" abgeschlossen, mit welchem der Datenimporteuer, dh der Empfänger im Drittland oder die internationale Organisation, sich vertraglich verpflichtet, ein mit der DSGVO vergleichbares Datenschutzniveau einzuhalten.

Weitere geeignete Garantien können im Einzelfall von der Datenschutzbehörde bewilligte Vertragsklauseln oder verbindliche interne Datenschutzvorschriften (sogenannte „binding corporate rules") sein.

Darüber hinaus kann die europäische Kommission – wenn sie der Auffassung ist, dass das Datenschutz-Niveau in einem Drittland (dh außerhalb des EWR-Raumes) mit dem Schutzniveau der DSGVO vergleichbar ist – einen Angemessenheitsbeschuss fassen. In einem solchen Fall, sind keine weiteren Garantien für die Datenübermittlung in ein solches Land erforderlich.
Jene Länder, in denen nach Ansicht der Kommission ein angemessenes Datenschutzniveau gegeben ist sind die Staaten Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay sowie für die USA das Privacy Shield.

WISSENSCHAFT UND FORSCHUNG

22) Inwiefern sind Wissenschaft und Forschung (wissenschaftliche Forschungszwecke) in der DSGVO und nach nationalem Recht privilegiert?

Die DSGVO privilegiert wissenschaftliche Forschungszwecke an mehreren Stellen:

- Art 5 Abs 1 lit b DSGVO – Erleichterung der Weiterverarbeitung;
- Art 5 Abs 1 lit e DSGVO – Lockerung der Speicherbegrenzung;
- Art 9 Abs 2 lit. j DSGVO – Möglichkeit Verarbeitung von sensiblen Daten auf Grundlage des Rechts der Union oder der Mitgliedsstaaten (in Österreich insbesondere aufgrund des Forschungsorganisationsgesetzes);
- Art 14 Abs 5 lit b DSGVO - Keine Auskunftspflicht bei Erhebung von Daten von Dritten, wenn sich die Erteilung der Information als unmöglich oder unverhältnismäßig erweist; dies gilt insbesondere bei Verarbeitungen für wissenschaftliche Forschungszwecke;
- Art 17 Abs 3 lit d DSGVO – Einschränkung des Rechts auf Löschung, soweit diese für die Verarbeitung für Forschungszwecke erforderlich ist;
- Art 21 Abs 6 DSGVO – spezielles Widerspruchsrecht gegen die Verarbeitung für wissenschaftliche Forschungszwecke;

23) Fallen Markt- und Meinungsforschungsinstitute unter den Wissenschaftsbegriff der DSGVO?

Art 89 DSGVO sieht Garantien und Ausnahmen in Bezug auf die Verarbeitung zu wissenschaftlichen Forschungszwecken vor. Umfasst vom Begriff wissenschaftliche Forschungszwecke sind beispielsweise die technologische Entwicklung und deren Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung, wie etwa die industrielle Forschung.

Darüber hinaus soll die DSGVO dem in Artikel 179 Absatz 1 AEUV festgeschriebenen Ziel, einen europäischen Raum der Forschung zu schaffen, Rechnung tragen.

Das DSG 2018 nimmt in diesem Zusammenhang eine weitere Präzisierung vor: Wissenschaftliche Einrichtungen sind natürliche Personen, Personengemeinschaften sowie juristische Personen, die Zwecke gemäß Art. 89 Abs. 1 DSGVO verfolgen, d.h. insbesondere Tätigkeiten der Forschung und experimentellen Entwicklung vornehmen.

Tätigkeiten der Forschung und experimentellen Entwicklung sind
a) neuartig,
b) schöpferisch,
c) ungewiss in Bezug auf das Endergebnis,
d) systematisch und
e) übertrag- oder reproduzierbar.

Verarbeitungen, bei denen das Markt- und Meinungsforschungsinstitut diese Grundsätze einhält, sind als Verarbeitung für wissenschaftliche Forschungszwecke im Sinne der DSGVO zu qualifizieren.

24) Haben Marktforschungsinstitute Zugang zu öffentlichen Registern?

Unter „Registerforschung“ versteht man die Bereitstellung von personenbezogenen Daten aus staatlichen Registern, auch nicht-öffentlichen Registern, wie zum Beispiel, das Melderegister, für die Verarbeitung zu wissenschaftlichen Forschungszwecken. Eine solche Registerforschung ist unter bestimmten Voraussetzungen zulässig.

Die Registerforschung ist grundsätzlich nur für wissenschaftliche Einrichtungen erlaubt, die gleichzeitig auch zur Verwendung von bereichsspezifischen Personenkennzeichen befugt sind.

Die Registerforschung ist auch Markt- und Meinungsforschungsinstituten zugänglich, soweit sie wissenschaftlich tätig sind. Diese haben beim Bundesminister für Verkehr, Innovation und Technologie, eine Bestätigung einzuholen, dass sie Tätigkeiten der Forschung und experimentellen Entwicklung durchführen.

Dieser entscheidet über den Antrag mit Bescheid, wobei der Bescheid maximal fünf Jahre gültig ist.

Darüber hinaus besteht die Pflicht, einen Datenschutzbeauftragten zu bestellen, um Registerforschung durchführen zu können.

Sind die vorgenannten Voraussetzungen gegeben, dürfen wissenschaftliche Einrichtungen die Bereitstellung von Daten aus bestimmten Registern in elektronischer Form zu wissenschaftlichen Forschungszwecken verlangen, wobei Namensangaben durch Bereichsspezifische Personenkennzeichen zu ersetzen sind.

Die Daten werden daher grundsätzlich nur pseudonymisiert an die wissenschaftliche Einrichtung übermittelt. Unter bestimmten Voraussetzungen ist allerdings auch eine Übermittlung einschließlich der Namensangaben möglich.

25) Dürfen Marktforschungsinstitute Archive mit personenbezogenen Daten („Repositories") anlegen?

Unter „Repositories" versteht man unter anderem die Sammlung, Archivierung und systematische Erfassung von Forschungsmaterial sowie die Verarbeitung von Daten in diesem Zusammenhang für wissenschaftliche Forschungszwecke, um einen optimalen Zugang zu den Daten und dem Forschungsmaterial zu gewährleisten.

Das Anlegen von Repositories ist nur wissenschaftlichen Einrichtungen erlaubt.

Das Forschungsorganisationsgesetz ermächtigt den Verantwortlichen eines Repositories Daten in umfangreichem Ausmaß zu verarbeiten, beispielsweise Namensangaben (Vorname(n), Familienname bzw. Bezeichnung, Geburtsname, akademischer Grad, Titel, Ansprache) Personenmerkmale (Geburtsdatum, Geburtsort, soweit verfügbar, Geschlecht, Staatsangehörigkeit) sowie insbesondere Zugehörigkeit zu einer sozialen, ethnischen oder kulturellen Gruppe, (soziale Stellung, Beruf, Sprachkenntnisse und sonstige, besondere Kenntnisse, Angaben hinsichtlich der Vorfahren, bereichsspezifisches Personenkennzeichen), Adress- und Kontaktdaten (Adressdaten und Angaben zur elektronischen Erreichbarkeit) sonstige Daten, die für die Archivierung und Klassifikation erforderlich sind, wie etwa Fundortdaten oder spezifische Angaben zu Personen, die das Forschungsmaterial zur Verfügung gestellt haben sowie weitere Angaben über politische, religiöse, rechtliche, traditionelle oder andere gruppenspezifische Hintergrundinformationen sowie Hintergrundinformationen betreffend Gesundheit, Gesundheitsdaten oder genetische Daten.

Darüber hinaus dürfen wissenschaftliche Einrichtungen als Verantwortliche solcher Repositories, anderen wissenschaftlichen Einrichtungen unter bestimmten Voraussetzungen direkt personenbezogene Daten bereitstellen.

26) Ein Markt- und Meinungsforschungsinstitut möchte die Einwilligung von betroffenen Personen für mehrere wissenschaftliche Projekte einholen, wobei die einzelnen Projekte noch nicht feststehen. Wie ist in solchen Fällen vorzugehen und was ist zu beachten?

Eine wirksame Einwilligungserklärung muss hohen Anforderungen entsprechen. Insbesondere sind „Pauschaleinwilligungen" grundsätzlich unzulässig, weil der Betroffene in diesem Fall nicht genau weiß, wofür er seine Einwilligung erteilt.

Für Datenverarbeitungen zu Zwecken der wissenschaftlichen Forschung ist hingegen ein „broad consent“ zulässig. Das bedeutet, dass es nicht erforderlich ist, den Zweck genau zu beschreiben (dh Angabe eines konkret beschriebenen Forschungsprojektes) sondern die Angabe des Zweckes durch Angaben eines Forschungsbereiches, mehrerer Forschungsbereiche, von Forschungsprojekten oder von Teilen von Forschungsprojekten erfolgen darf.

Durch den „broad consent“ wird daher die Verarbeitung von Forschungsdaten für zukünftige, zum Zeitpunkt der Erhebung nicht bekannte Zwecke, ermöglicht.

27) Ist die teilweise Aufnahme von Interviews via Tablet zulässig oder darf der Supervisor zu Qualitätssicherungszwecken Teile des Telefon-Interviews mithören?

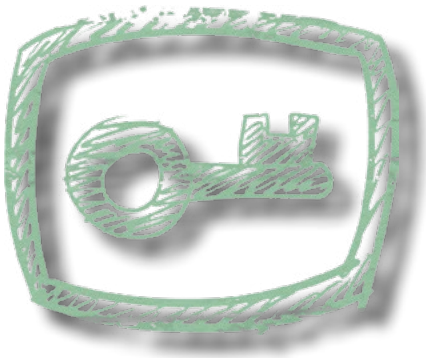
Aus datenschutzrechtlicher Sicht ist die Aufnahme von Interviews (oder Teilen desselben) eine Verarbeitung von personenbezogenen Daten des Interviewers als auch des Befragten, weil jeweils deren Stimme als auch die jeweiligen Gesprächsinhalte aufgezeichnet werden. Eine solche Verarbeitung unterliegt– wie das Abhören eines Telefonats - die dem Datenschutz.

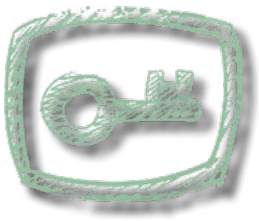
Grundsätzlich ist eine solche Datenverarbeitung (wie jede andere Datenverarbeitung auch) nur zulässig, wenn eine entsprechende Rechtsgrundlage vorliegt.

Die einschlägige Rechtsgrundlage ist die Einwilligung sowohl des Interviewers als auch des Befragten, weil andere Rechtsgrundlagen nicht in Frage kommen. Die Einwilligung kann auch telefonisch eingeholt werden, wobei eine technische Protokollierung der Einwilligung jedenfalls ratsam ist.

Hinsichtlich der Formulierung einer solchen Einwilligungserklärung sind besondere Anforderungen einzuhalten, da der Betroffene freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich seine Einwilligung erteilen muss, andernfalls eine unwirksame Einwilligung vorliegt. Eine solche Einwilligungserklärung sollte daher für den jeweiligen Einzelfall angepasst werden.

Das überwiegende berechtigte Interesse scheidet als Rechtsgrundlage in der Regel aus, weil je nach Inhalt des Interviews die Interessen der befragten Person in sehr intensiver Weise beeinträchtigt sein können, sodass dieses in vielen Fällen nicht zugunsten des Verantwortlichen (dh des Markt- und Meinungsforschungsinstituts) ausschlägt, insbesondere dann, wenn die Aufzeichnung ohne Wissen der betroffenen Person erfolgt.





INFORMATIONSPFLICHTEN DES VERANTWORTLICHEN

(ART 12, 13 UND 14 DSGVO)

28) Was ist eine Datenschutzerklärung und ist eine solche notwendig?

Mit der Datenschutzerklärung erfüllt der Verantwortlichen seine Informationspflicht gemäß DSGVO, betroffenen Personen Informationen über die Verarbeitung ihrer personenbezogenen Daten zu Verfügung zu stellen. Dadurch soll die vom Verantwortlichen vorgenommene Verarbeitung für die betroffenen Personen nachvollziehbar und transparent werden und diese in die Lage versetzen, gegebenenfalls entsprechende Maßnahmen zu ergreifen, wenn sie der Meinung sind, dass die Verarbeitung ihrer personenbezogenen Daten rechtswidrig erfolgt.

Die Datenschutzerklärung enthält wichtige Informationen in welchem Umfang und wofür die personenbezogenen Daten verarbeitet werden. Sie gibt darüber hinaus Auskunft, wem die Daten offengelegt wurden und informiert über die Rechte der Betroffenen. Für weitere Informationen siehe Frage 29.

29) Über was muss ein Verantwortlicher die betroffenen Personen informieren und zu welchem Zeitpunkt? Macht es einen Unterschied ob die Daten von Dritten stammen?

Der Verantwortliche muss der betroffenen Person folgende Informationen zur Verfügung stellen (Art 13 DSGVO):

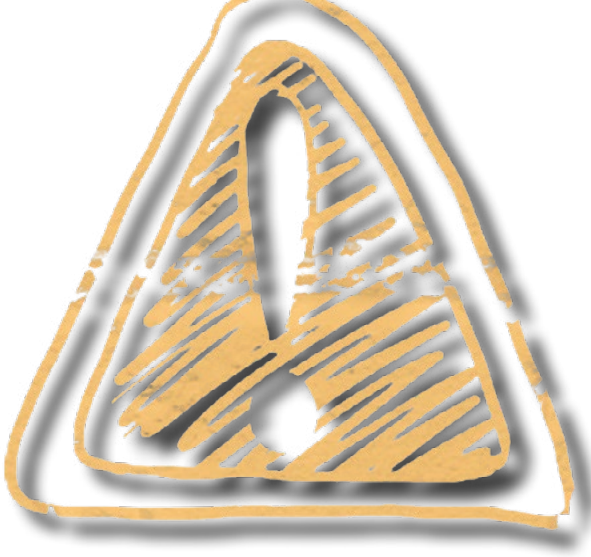
- Name und Kontaktdaten des Verantwortlichen und gegebenenfalls seines Vertreters;
- Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtgrundlage der Verarbeitung;
- das berechtigte Interesse, aufgrund dessen die Verarbeitung erfolgt;
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- die Absicht die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln;
- die Dauer der Speicherung der Daten;
- das Recht auf Auskunft über die betreffenden personenbezogenen Daten;
- das Recht auf Berichtigung der personenbezogenen Daten;
- das Recht auf Löschung der personenbezogenen Daten;
- das Recht auf Einschränkung der Verarbeitung der personenbezogenen Daten;
- ein Widerspruchsrecht gegen die Verarbeitung der personenbezogenen Daten;
- das Recht auf Datenübertragbarkeit;
- das Recht eine Einwilligung zur Verarbeitung jederzeit zu widerrufen;
- das Beschwerderecht bei der Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben, oder für einen Vertragsabschluss erforderlich ist;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling;
- gegebenenfalls Informationen über die Weiterverarbeitung zu einem anderen Zweck;

Die genannten Informationen müssen der betroffenen Person zum Zeitpunkt der Erhebung zur Verfügung gestellt werden.

Wenn die Daten nicht bei der betroffenen Person erhoben wurden – dies ist etwa auch dann der Fall, wenn personenbezogene Daten aus einem Telefonbuch erhoben werden - sind folgende Informationen zusätzlich zu erteilen:

- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Quelle, aus der die personenbezogenen Daten stammen;

Darüber hinaus sind in einem solchen Fall der betroffen Person die erforderlichen Informationen innerhalb einer angemessene Frist nach Erhebung der Daten, längstens innerhalb eines Monats, zu



erteilen oder spätestens bei Eintritt der nachstehenden Fälle.

Wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, erfolgt die Information spätestens zum Zeitpunkt der ersten Mitteilung an sie und falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

30) In welcher Form hat die Informationserteilung stattzufinden und wie sind die Informationen den Betroffenen zur Verfügung zu stellen.

In der Regel wird die Datenschutzerklärung, insbesondere im „Online-Bereich", leicht auffindbar auf der Website des Verantwortlichen platziert. Notwendig ist es, allfällige Verlinkungen direkt auf die Datenschutzerklärung zu setzen und nicht bloß auf die Website, auf welcher die Datenschutzerklärung möglicherweise erst gesucht werden muss.

Es sind aber auch andere Formen denkbar, wie der Verantwortliche dem Betroffenen die notwendigen Informationen zur Verfügung stellen kann. Im „Offline-Bereich" wird eine auf der Website befindliche Datenschutzerklärung unter Umständen nicht ausreichend sein. Werden Daten im Zuge einer Befragung von Passanten in personenbezogener Form erhoben (dh die Rückführbarkeit der Antworten auf den Befragten ist gegeben), wäre eine Datenschutzerklärung auf der Website des Markt- und Meinungsforschungsinstituts deshalb nicht ausreichend, weil dem Betroffenen im Zeitpunkt der Erhebung die Informationen nicht zur Verfügung stehen.

In diesem Fall ist der Betroffene zumindest über die Identität des Verantwortlichen, die Verarbeitungszwecke und die Identität von weiteren Verantwortlichen zu informieren, denen die Daten übermittelt werden sollen, und auf die Datenschutzerklärung auf der Website des verantwortlichen hinzuweisen.

Werden die Daten nicht in personenbezogener Form erhoben, weil beispielsweise nur Alter und Geschlecht des Betroffenen verarbeitet werden, liegen anonyme Daten vor, auf die die DSGVO und damit die Informationspflicht des Verantwortlichen keine Anwendung finden.

31) Wie kann ich am Telefon die Informationen zur Verfügung stellen?

Es kann Situationen geben, in denen eine Informationserteilung am Telefon zu erfolgen hat, etwa, weil der Betroffene diese Vorgehensweise ausdrücklich wünscht oder weil personenbezogen Daten im Zuge eines Telefonats erhoben werden.

In solchen Fällen können vorerst nur die wesentlichen Punkte der Datenverarbeitung unmittelbar im Gespräch offengelegt werden. Diese Eckpunkte sind die Identität des Verantwortlichen, die Verarbeitungszwecke und die Identität jener Verantwortlichen, an welche die Daten übermittelt werden sollen. Für die Erteilung der übrigen Informationen kann durch Verweis auf eine online leicht zugängliche Datenschutzmitteilung erfolgen bzw. durch postalische Zusendung der Datenschutzerklärung, sofern dies die betroffene Person wünscht.

Eine andere Möglichkeit wäre, ein Tonband abzuspielen, welches die geforderten Informationen enthält, wobei der Betroffene mittels Wähltasten am Telefon die einzelnen Kapitel der Erklärung (wie etwa Namen, Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters, Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung etc) ansteuern kann.

BETROFFENENRECHTE

(ART 15 – 22 DSGVO, EXKL. ART 22 DSGVO)

32) Welche Rechte haben Personen, deren Daten verarbeitet werden (Betroffene)?

Schon nach der alten Rechtlage (DSG 2000) hatte der Betroffene das Recht auf Auskunft (nunmehr Art 15 DSGVO), das Recht auf Berichtigung (nunmehr Art 16 DSGVO) und Löschung (nunmehr Art 17 DSGVO) und ein Widerspruchsrecht (nunmehr Art 21 DSGVO). Durch das Inkrafttreten der DSGVO wurden die Rechte der Betroffenen um das Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO) und um das Recht auf Datenübertragbarkeit (Art 20 DSGVO) erweitert. Darüber hinaus stehen dem Betroffenen spezielle Rechte im Fall der automatischen Entscheidungsfindung (einschließlich Profiling) zu.

33) Kann der Antrag eines Betroffenen auch abgelehnt werden?

Grundsätzlich muss der Verantwortliche den Anträgen der Betroffenen im Zusammenhang mit der Ausübung ihrer Rechte innerhalb der dafür vorgesehen Frist nachkommen.

Für diese Grundregel sieht die DSGVO mehrere Ausnahmen vor. So kann der Antrag eines Betroffenen abgelehnt werden, wenn der Betroffene solche Anträge offenkundig unbegründet oder in exzessiver Weise stellt.

Ein Antrag ist offenkundig unbegründet, wenn die Voraussetzungen des Antrags offensichtlich nicht erfüllt sind (zB wenn eine unberechtigte Person die Betroffenenrechte geltend machen will). Ein exzessiver Antrag liegt unter anderem bei häufiger Wiederholung der Antragstellung vor.

Von der Möglichkeit der Ablehnung sollte jedoch nur restriktiv Gebrauch gemacht werden, insbesondere weil Rechtsprechung, wann eine solche häufige Wiederholung vorliegt, fehlt und die unberechtigte Weigerung einem Antrag eines Betroffenen nachzukommen zu einer Strafe der Datenschutzbehörde führen kann.

Wird ein Antrag durch den Verantwortlichen abgelehnt, ist der Betroffene über die Gründe, warum dem Antrag nicht entsprochen wird und über die Möglichkeit, bei der Datenschutzbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, zu informieren.

34) Bis wann ist ein Antrag eines Betroffen zu erledigen?

Die Information ist dem Betroffenen unverzüglich, aber jedenfalls innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl der Anträge erforderlich ist (Art 12 Abs 3 DSGVO).

Das bedeutet, dass die Mitteilung ohne unbillige bzw. schuldhafte Verzögerung erfolgen muss. Für wie lange dieser Zeitraum wirklich zu bemessen ist, ist nach dem Einzelfall zu beurteilen. Die Erteilung von sehr einfachen Auskünften am letzten Tag der Frist könnte möglicherweise eine solche schuldhafte Verzögerung darstellen, weil diese auch schon früher erfolgen hätte können.

35) Wie ist vorzugehen, wenn der Verantwortliche Zweifel an der Identität des Betroffenen hat?

Der Verantwortliche einer Datenverarbeitung hat sich von der Identität eines Betroffenen, der ein Recht ausüben möchte zu vergewissern, wenn er begründete Zweifel an dieser hat.

Zweifel an der Identität bedeutet, dass der Verantwortliche sich nicht sicher ist, ob es sich bei dem Antragsteller tatsächlich um jene Person handelt, für die sie sich ausgibt.

In diesem Fall hat der Verantwortliche die Identität zu prüfen, indem er zusätzliche Informationen anfordert.

Das Anfordern von zusätzlicher Information ist nur zulässig, wenn begründete Zweifel bestehen, etwa wenn ein Antrag von einer E-Mailadresse stammt, die dem Verantwortlichen bisher unbekannt war oder der Antrag mündlich per Telefon gestellt wird.

Dies kann etwa durch Anforderung einer Ausweiskopie erfolgen, um die Unterschriften auf dem Antrag und auf dem Ausweis abzugleichen oder durch eine Zwei-Faktoren-Authentisierung. Der Verantwortliche ist verpflichtet, die Ausübung der Rechte von Betroffenen möglichst zu erleichtern, weshalb er ein möglichst gelindes Mittel zu wählen hat, um seine Zweifel auszuräumen.

Kommt der Verantwortliche mangels ausreichender Identitätsprüfung einem Antrag nach, der nicht von der betroffenen Person gestellt wurde, riskiert er eine Datenschutzverletzung, weil er beispielsweise im Falle eines Auskunftsbegehrens personenbezogene Daten an einen unbefugten Dritten offenlegt.

Kann der Verantwortliche die Identität des Betroffenen nicht authentisieren, beispielsweise weil dieser keine zusätzlichen Informationen zur Verfügung stellt, so kommt er dem Antrag nicht nach und hat darüber hinaus die entsprechenden Umstände, warum eine Authentifizierung nicht möglich war, zu dokumentieren.

36) Was versteht man unter dem Recht auf Auskunft?

Das Auskunftsrecht dient der betroffenen Person in einem ersten Schritt zur Klärung der Frage, ob überhaupt ihre personenbezogenen Daten, verarbeitet werden. Der Betroffene hat das Recht eine Bestätigung zu verlangen, ob seine personenbezogenen Daten verarbeitet werden.

Werden keine personenbezogenen Daten verarbeitet, ist dies vom Verantwortlichen zu bestätigen (sog „Negativ-Bestätigung"). Werden personenbezogene Daten verarbeitet, hat der Verantwortliche Auskunft über die verarbeiteten personenbezogenen Daten zu erteilen, wobei nicht neben den Datenkategorien (wie etwa „Geburtsdatum", „Vorname", „Nachname" etc) auch die konkret verarbeiteten Daten dem Betroffenen zur Verfügung zu stellen sind.

Die betroffene Person hat Anspruch auf eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Das bedeutet unter anderem, dass dem Betroffenen Kopien jener Dokumente zur Verfügung zu stellen ist, in denen seine personenbezogenen Daten vorkommen (wie etwa Auszüge aus Datenbanken, E-Mails etc).

37) Was versteht man unter dem Recht auf Berichtigung?

Die betroffene Person hat das Recht, von dem Verantwortlichen die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen (Art 16 DSGVO).

Unrichtig sind personenbezogene Daten dann, wenn sie nicht mit der Realität übereinstimmen, oder wenn sie irreführend, unklar oder missverständlich sind und nach der Zweckbestimmung ihrer Verarbeitung die betroffene Person „in ein falsches Licht" rücken und somit ihre Rechtsstellung beeinträchtigen können.

Ob personenbezogene Daten unrichtig sind, kann in manchen Fällen, insbesondere bei Werturteilen schwierig sein, weshalb diese nur in begrenztem Umfang einer Berichtigung zugänglich sind.

38) Was versteht man unter dem Recht auf Löschung?

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten gelöscht werden, wenn eine der folgenden Voraussetzungen gegeben ist: Wegfall der Notwendigkeit der Verarbeitung zur Zweckerreichung, der Widerruf der Einwilligung, der Widerspruch gegen die Verarbeitung, die Unrechtmäßigkeit der Verarbeitung, die Erfüllung einer Rechtspflicht oder die Verarbeitung mit Angebot eines Dienstes der Informationsgesellschaft.

Eine Ausnahme vom Recht auf Löschung besteht, wenn die Verarbeitung für die Ausübung des Rechts auf Meinungs- und Informationsfreiheit, die Erfüllung einer rechtlichen Verpflichtung, einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, ein überwiegendes öffentliches Gesundheitsinteresse, ein öffentliches Archivinteresse oder wissenschaftliche oder historischen Forschungs- und statistische Zwecke oder die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Unter Löschung ist die tatsächliche physische Löschung zu verstehen. Als Richtschnur für eine Löschung gilt, dass die Daten nicht ohne weiteres wiederherstellbar sein dürfen, weshalb logisches Löschen nicht ausreichend ist.

Unter logischem Löschen versteht man die Freigabe der betreffenden Speicherplätze in der entsprechenden Indexierung zum neuen Beschreiben, wobei die zu löschenden Informationen dadurch noch nicht verändert bzw. gelöscht werden. Da eine Großzahl der Betriebssysteme Löschbefehle in Form von logischem Löschen durchführen, genügen diese nicht den Maßstäben der DSGVO. Vielmehr ist eine Spezialsoftware erforderlich, die die Bezug habenden Speicherplätze tatsächlich (mehrfach) überschreibt und so die zu löschende Information tatsächlich vernichtet.

39) Müssen die Daten von betroffenen Personen in jedem Fall gelöscht werden?

Nein. Vielmehr muss der Verantwortliche genau überprüfen, welche personenbezogenen Daten er löschen muss und welche er weiterhin verarbeiten muss bzw darf.

So können beispielsweise unternehmensrechtliche oder steuerrechtliche Vorschriften den Verantwortlichen verpflichten, solche personenbezogene Daten für einen gewissen Zeitraum weiterhin aufzubewahren. Darüber hinaus können die personenbezogen Daten für bestimmte Zwecke, wie etwa die Erfüllung von vertraglichen Pflichten gegenüber dem Betroffenen oder zur Abrechnung eines solchen Vertrages noch benötigt werden.

Der Verantwortliche hat daher für jede Datenkategorie zu prüfen, ob die Voraussetzungen für eine Löschung vorliegen. Eine Löschung von personenbezogenen Daten „sicherheitshalber" bzw „im Zweifel" ohne genaue Abklärung, ob die Daten noch erforderlich sind, ist nicht ratsam.

40) Was versteht man unter dem Recht auf „Vergessenwerden"?

Das Recht auf „Vergessenwerden" ist eine Ausweitung des Rechts auf Löschung, um dem Problem zu begegnen, dass das Internet „nichts vergisst". Informationen sind selbst nach Jahrzehnten noch online abrufbar sind, was für die Betroffenen mit negativen Konsequenzen verbunden sein kann.

Aus diesem Grund, wurden dem Verantwortlichen durch die DSGVO zusätzliche Pflichten auferlegt, um die Entfernung persönlicher Daten aus dem Internet effektiver zu machen.

Der Verantwortliche ist verpflichtet, sofern er die personenbezogenen Daten öffentlich gemacht hat, durch technische und kostenmäßig angemessene Maßnahmen, andere Verantwortliche über das Verlangen der betroffenen Person, alle Links zu den

betroffenen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten zu löschen, zu informieren.

Im engeren Sinne handelt es sich hierbei um eine Informationspflicht des Verantwortlichen. Er schuldet nicht die Herbeiführung eines Löschungserfolges.

Der Betroffene muss das Recht nicht ausdrücklich geltend machen. Es ist ausreichend, wenn sich aus dem Antrag auf Löschung ergibt, dass eine weitergehende Löschung verlangt wird, als lediglich die Löschung der beim Verantwortlichen verarbeiteten Daten.

Das Recht auf „Vergessenwerden" besteht nur in dem Umfang, wie auch das Recht auf Löschung besteht. Ist daher kein Recht auf Löschung gegeben, ist auch die Ausübung des Rechtes auf „Vergessenwerden" nicht möglich.

41) Was versteht man unter dem Recht auf Einschränkung der Verarbeitung?

Das Recht auf Einschränkung der Verarbeitung bedeutet, die Verarbeitung der personenbezogenen Daten mit Ausnahme der Speicherung der Daten vollständig einzuschränken.

Das Recht auf Einschränkung der Verarbeitung besteht, wenn eine der folgenden Voraussetzungen erfüllt ist:

- Wenn die betroffene Person die Richtigkeit der Daten bestritten hat, für die Dauer der Berichtigungsprüfung durch den Verantwortlichen.
- Wenn die Verarbeitung unrechtmäßig ist und die betroffene Person eine Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung verlangt.
- Wenn der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht weiter benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.
- Wenn die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen des Betroffenen überwiegen.

42) Was versteht man unter dem Recht auf Datenübertragbarkeit?

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten ohne Behinderung durch den Verantwortlichen zu übermitteln. Voraussetzung für die Ausübung dieses Rechtes ist, dass die Verarbeitung auf einer Einwilligung oder einem Vertrag mit dem Betroffenen beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Die betroffene Person kann die Übertragung an sich selbst bzw an einen anderen Verantwortlichen verlangen, soweit dies technisch machbar ist. Zu beachten ist, dass mit einem Antrag auf Datenübertragbarkeit nicht automatisch ein Antrag auf Löschung verbunden ist. Daher darf der Verantwortliche, der die Daten an die betroffene Person oder einen dritten Verantwortlichen übertragen hat, die übertragenen Daten nicht automatisch aus seinen Systemen löschen.

Darüber hinaus soll das Recht auf Datenübertragbarkeit laut den Erwägungen zur DSGVO nicht die Pflicht für Verantwortliche begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten.

43) Was versteht man unter dem Widerspruchsrecht?

Das allgemeine Widerspruchsrecht ist das Recht gegen eine als solche möglicherweise rechtmäßige, weil auf einer zulässigen Interessensabwägung gestützte Verarbeitung personenbezogener Daten, vorzugehen.

Das Widerspruchsrecht gilt für den Fall, dass sich eine im Ausgangspunkt rechtmäßig erscheinende Datenverarbeitung im Nachhinein, im Hinblick auf eine Sondersituation einer betroffenen Person, als rechtswidrig erweist.

Eine besondere Situation ist gegeben, wenn sich die betroffene Person in außerordentlicher, spezifischer und individueller Weise von der Situation anderer Personen unterscheidet. Dies kann eine familiäre, gesellschaftliche, soziale, wirtschaftliche, rechtliche oder sonst wie faktische Sondersituation sein. Dadurch besteht die Möglichkeit für den Betroffenen, die generelle und vorab durchgeführte Interessensabwägung durch den Verantwortlichen durch eine konkret auf seinen spezifischen Fall angepasste Prüfung der Interessen zu ersetzen.

Ein Beispiel für eine solche Sondersituation wäre etwa ein Patient, dessen Gesundheitsdaten durch ein Krankenhaus verarbeitet werden, wobei ein naher Verwandter in diesem Krankenhaus in naher Zukunft eine Führungsposition einnehmen soll.

Liegen keine besonderen Gründe bzw eine Sondersituation des Betroffenen vor, sondern ist der Betroffene vielmehr der Meinung, dass die Interessensabwägung durch den Verantwortlichen generell unrichtig war, ist nicht mit dem Widerspruchsrecht sondern mit dem Recht auf Löschung vorzugehen, weil in diesem Fall in der Regel keine Rechtsgrundlage für die Datenverarbeitung besteht.

AUFTRAGSVERARBEITER
(ART 26 DSGVO)

44) Was ist ein Auftragsverarbeiter?
Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Das bedeutet, dass der Auftragsverarbeiter für den Verantwortlichen der personenbezogenen Daten eine konkrete Datenverarbeitung durchführt, wobei er strikt an die Weisungen des Verantwortlichen gebunden ist. Typische Beispiele für einen Auftragsverarbeiter sind: Anbieter von Cloud-Diensten, Dienstleister in der IT-Branche, externe Buchhalter oder auch Marketing-Unternehmen. Darüber hinaus sind noch unzählige weitere Fälle einer Auftragsverarbeitung denkbar.

Dem Auftragsverarbeiter kommt keine Entscheidungsbefugnis zu, zu welchem Zweck die Daten verarbeitet werden. Was mit den Daten geschieht, entscheidet daher alleine dem Verantwortlichen. Auch hinsichtlich rechtlicher Aspekte, beispielsweise wie lange die Daten gespeichert werden, wer Zugriff zu den Daten erhält oder welche Daten für die Zweckerreichung verarbeitet werden, obliegt die Entscheidung ausschließlich dem Verantwortlichen.

Dem Auftragsverarbeiter kann bloß ein gewisser Entscheidungsspielraum hinsichtlich technischen und organisatorischen Mittel überlassen werden, beispielsweise Details zu den Sicherheitsvorkehrungen, die für den Schutz der Daten konkret getroffen werden, oder welche Hard- oder Software konkret verwendet wird.

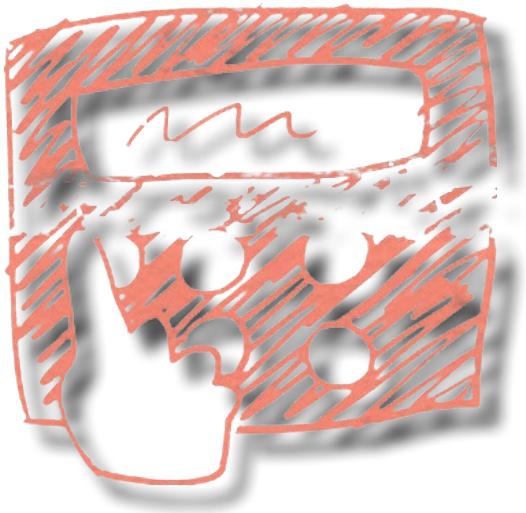
Die Berücksichtigung der oben genannten Aufgabenverteilung ist insbesondere für den Auftragsverarbeiter wichtig, weil ein Auftragsverarbeiter der seinen Auftrag überschreitet (und damit die Daten für eigene Zwecke verwendet) selbst zum Verantwortlichen.

In solchen Fällen liegt allerdings oftmals eine unzulässige Datenverarbeitung vor, sodass der Auftragsverarbeiter dem Risiko einer Strafe durch die Datenschutzbehörde ausgesetzt ist.

45) Wann sind Markt- und Meinungsforschungsinstitute als Auftragsverarbeiter anzusehen?
Markt- und Meinungsforschungsinstitute ist in der Regel dann als Auftragsverarbeiter anzusehen, wenn sie die personenbezogenen Daten entweder im ausdrücklichen Auftrag für einen Auftraggeber als Verantwortlichen erheben und diese in personenbezogener Form an den Verantwortlichen weitergeben, ohne dass das Markt- und Meinungsforschungsinstitut die Daten für eigene Zwecke verwendet, oder die Daten vom Auftraggeber direkt erhalten und ausschließlich der Auftraggeber als Verantwortlicher über die Zwecke der Datenverarbeitung bestimmt und auch sonst über die wesentlichen Mittel der Datenverarbeitung bestimmt (für nähere Informationen siehe Frage 44). Im Fall von Kundenzufriedenheitsumfragen fungieren Markt- und Meinungsforschungsinstitute oftmals als Auftragsverarbeiter.

Werden diese Grundsätze eingehalten, kann ein Markt- und Meinungsforschungsinstitut als Auftragsverarbeiter fungieren. Zu den Grundsätzen gehört allerdings auch, dass die Rohdaten und die Forschungsergebnisse nach Durchführung der Studie gelöscht und/oder dem Verantwortlichen zurückgestellt werden, andernfalls davon auszugehen ist, dass das Markt- und Meinungsforschungsinstitut die Daten für eigene Zwecke verarbeitet und damit als Verantwortlicher anzusehen ist.

Stammen die Rohdaten aus einer Datenverarbeitung des Markt- und Meinungsforschungsinstitutes ist dieses für diese Daten jedenfalls als Verantwortlicher und nicht als Auftragsverarbeiter anzusehen.



Im Fall von Kundenzufriedenheitsumfragen, bei denen das Markt- und Meinungsforschungsinstitut, die personenbezogenen Daten für die Durchführung der Umfrage regelmäßig vom Auftraggeber als Verantwortlichen erhält, ist in vielen Fällen eine Eigenschaft des Markt- und Meinungsforschungsinstitutes als Auftragsverarbeiter gegeben.

46) Wir machen eine Kundenzufriedenheitsumfrage für ein Unternehmen mit der Hauptniederlassung in Deutschland. Was ist zu beachten?

Wenn der Verantwortliche seinen Sitz in Deutschland hat und über keine Niederlassung in Österreich verfügt, ist auf seine Datenverarbeitungen deutsches Recht anzuwenden. Das gilt auch, wenn dieser Verantwortliche ein österreichisches Unternehmen als Auftragsverarbeiter beauftragt. In diesem Fall hat auch das österreichische Unternehmen deutsches Recht zu beachten.

Für Markt- und Meinungsforschungsinstitute sieht das Bundesdatenschutzgesetz (BDSG neu) ausdrücklich vor, dass ein Datenschutz-Beauftragter zu bestellen ist. In dem oben dargestellten Fall, gilt diese Pflicht auch für das österreichische Markt- und Meinungsforschungsinstitut.

47) In welchem Ausmaß muss der Umstand offengelegt werden, dass (Sub-)Auftragsverarbeiter an einer Datenverarbeitung beteiligt sind?

In diesem Zusammenhang ist zu unterscheiden zwischen der Pflicht des Verantwortlichen zur Offenlegung der Beiziehung von Auftragsverarbeitern gegenüber dem Betroffenen im Rahmen einer Datenschutzerklärung und der Pflicht zur Offenlegung (und Einholung einer Genehmigung) des Auftragsverarbeiters gegenüber dem Verantwortlichen zur Beiziehung von weiteren (Sub-)Auftragsverarbeitern im Rahmen eines Auftragsverhältnisses.

Die DSGVO verlangt vom Verantwortlichen, dass den betroffenen Personen sämtliche Empfänger von personenbezogenen Daten bekanntzugeben sind oder zumindest die Kategorien von Empfängern. Unter Empfänger sind gemäß Definition der DSGVO auch die Auftragsverarbeiter zu verstehen. Daher ist eine Offenlegung der Auftragsverarbeiter durch den Verantwortlichen gegenüber den Betroffenen Personen erforderlich.

Im Rahmen eines Auftragsverhältnisses dürfen sich Auftragsverarbeiter unter gewissen Voraussetzungen eines Sub-Auftragsverarbeiters bedienen. Wesentliche Voraussetzung hierfür ist die vorherige Zustimmung des für die Datenverarbeitung Verantwortlichen, welche in Form einer für jeden Subauftragsverarbeiter gesonderten oder allgemeinen schriftlichen Genehmigung erfolgen kann.

Allerdings ist selbst im Fall der allgemeinen schriftlichen Genehmigung der Auftragsverarbeiter verpflichtet, jede Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Subauftragsverarbeiter dem Verantwortlichen mitzuteilen, damit dieser die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Daraus kann geschlossen werden, dass auch sämtliche Sub-Auftragsverarbeiter dem Verantwortlichen offenzulegen sind.

48) Welche Pflichten muss ein Auftragsverarbeiter beachten?

Den Auftragsverarbeiter werden durch die DSGVO umfangreiche Pflichten auferlegt, die möglicherweise durch die Auftragsverarbeiter-Vereinbarung noch erweitert werden.

Der Auftragsverarbeiter ist unter anderem verpflichtet, die Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, Maßnahmen zur Sicherheit der Verarbeitung zu treffen, seine Mitarbeiter zur Vertraulichkeit im Hinblick auf die überlassenen Daten zu verpflichten, Subauftragsverarbeiter nur mit Einwilligung des Verantwortlichen hinzuziehen, den Verantwortlichen bei seinen Pflichten gegenüber Betroffenen zu unterstützen

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

(beispielsweise bei der Ausübung des Rechtes auf Löschung oder auf Auskunft etc.) sowie gegebenenfalls ein Auftragsverarbeiterverzeichnis zu führen. Ferner ist er verpflichtet, sämtliche Informationen zum Nachweis der Einhaltung seiner Pflichten gemäß DSGVO bei Bedarf dem Verantwortlichen zur Verfügung zu stellen, wozu eine entsprechende Dokumentation erforderlich ist. Darüber hinaus gibt es noch weitere Pflichten, die ein Auftragsverarbeiter je nach Situation z berücksichtigen hat.

Ein Verstoß eines Auftragsverarbeiters gegen seine Pflichten kann zu einer Strafe der Datenschutzbehörde führen aber auch dazu, dass er als Verantwortlicher einer Datenverarbeitung angesehen wird (wodurch ebenfalls eine Strafe durch die Datenschutzbehörde aufgrund einer unzulässigen Datenverarbeitung drohen kann).

49) Was ist ein Verzeichnis von Verarbeitungstätigkeiten?

Das Verzeichnis von Verarbeitungstätigkeiten ist grundsätzlich von jedem Verantwortlichen zu führen.

Auch der Auftragsverarbeiter muss ein Verzeichnis von Verarbeitungstätigkeiten führen, das sich allerdings inhaltlich vom Auftragsverarbeiterverzeichnis des Verantwortlichen unterscheidet.

Die Pflicht für den Verantwortlichen bzw für den Auftragsverarbeiter entfällt unter bestimmten Umständen (für weitere Informationen siehe Frage 51).

Mit dem Verzeichnis von Verarbeitungstätigkeiten werden die vom Verantwortlichen oder Auftragsverarbeiter vorgenommen Verarbeitungen dokumentiert. Sie bieten daher eine Übersicht, welche Verarbeitungen von einem Verantwortlichen bzw einem Auftragsverarbeiter vorgenommen werden.

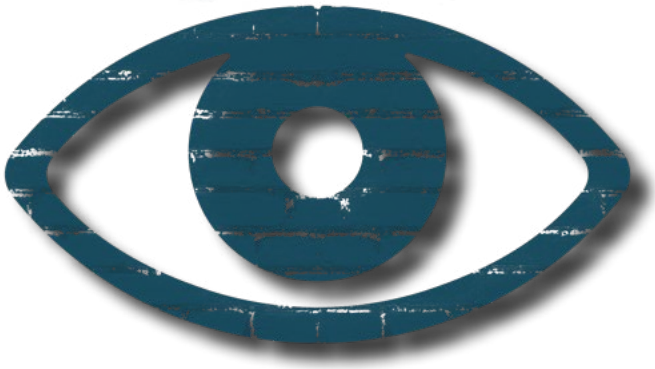
Diese Verzeichnisse müssen der Datenschutzbehörde auf Anfrage vorgelegt werden. Es ist daher nicht auszuschließen, dass die Behörde solche Verzeichnisse als Anknüpfungspunkt für weitergehende Kontrollen verwendet, insbesondere, wenn solche Verzeichnisse mangelhaft geführt werden.

50) Wie muss das Verzeichnis von Verarbeitungstätigkeiten aussehen?

Das Verzeichnis von Verarbeitungstätigkeiten, das der Verantwortliche zu führen hat, weicht inhaltlich von jenem, das der Auftragsverarbeiter zu führen hat ab, wobei die DSGVO an das Verarbeitungsverzeichnis des Auftragsverarbeiters geringere Anforderungen stellt.

Gemäß DSGVO hat das Verzeichnis des Verantwortlichen Namen und Kontaktdaten des Verantwortlichen, die Zwecke der Verarbeitung, die Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, die Kategorien von Empfängern bzw. geplanten Empfängern (einschließlich Übermittlungen an ein Drittland oder eine internationale Organisation samt entsprechender Garantie für eine Übermittlung in ein Drittland), die Fristen für die Löschung der verschiedenen Datenkategorien sowie die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen zu enthalten.

Das Verzeichnis des Auftragsverarbeiters hat Namen und Kontaktdaten des Auftragsverarbeiters sowie von jedem Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden, Übermittlung von personenbezogenen Daten an ein Drittland (einschließlich Übermittlungen an ein Drittland oder eine internationale Organisation samt entsprechender Garantie für eine Übermittlung in ein Drittland) sowie die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu enthalten.



51) Welche Ausnahmebestimmungen für das Führen des Verzeichnisses von Verarbeitungstätigkeiten gibt es?

Eine Pflicht zur Führung des Verzeichnisses von Verarbeitungstätigkeiten entfällt sowohl für den Auftragsverarbeiter als auch für den Verantwortlichen, wenn diese weniger als 250 Mitarbeiter beschäftigen, die vorgenommenen Verarbeitungen kein Risiko für die betroffenen Personen bergen und die Verarbeitung nur gelegentlich vorgenommen sowie keine personenbezogenen Daten oder Daten über strafrechtliche Verurteilungen verarbeitet werden.

Vor dem Hintergrund, dass nur in sehr wenigen Fällen von einer Datenverarbeitung kein Risiko für die betroffenen Personen ausgeht und Markt- und Meinungsforschungsinstitute oftmals besondere Datenkategorien verarbeiten, wird für diese die Ausnahmebestimmung regelmäßig nicht in Betracht kommen.

DATENSCHUTZ-BEAUFTRAGTER

(ART 37 - 39 DSGVO)

52) Was ist eine Datenschutz-Folgenabschätzung?

Mit der DSGVO wurde die Pflicht zur sogenannten Datenschutz-Folgenabschätzung eingeführt, die bei Vorliegen von bestimmten Voraussetzungen verpflichtend vom Verantwortlichen durchzuführen ist.

Bei einer Datenschutz-Folgenabschätzung beleuchtet der Verantwortliche eine Datenverarbeitung und beurteilt das potentielle Risiko, das durch die Datenverarbeitung für betroffene Personen entstehen kann.

Unterschiedliche Risikofaktoren sind beispielsweise die Anzahl der Datenkategorien, die pro betroffene Person verarbeitet werden, welche Rückschlüsse sich aus den Informationen ziehen lassen, ob besondere Datenkategorien („sensible Daten") verarbeitet werden, um welche Art von Verantwortlichen es sich handelt (beispielsweise um ein Inkassobüro oder bloß einem örtlichen Sportverein) und viele andere mehr.

Diese Risikofaktoren werden anhand unterschiedlicher Beurteilungssysteme quantifiziert, wobei die Quantifizierung in vielen Beurteilungssystemen anhand der Eintrittswahrscheinlichkeit des Risikos und der Schwere des Schadens für die Betroffen erfolgt das Risiko in die Klassen „gering", „mittel" und „hoch" eingeteilt wird.

In der Folge werden technische und organisatorische Maßnahmen getroffen, um die Risiken für die betroffenen Personen zu reduzieren. Für den Fall, dass trotz solcher Maßnahmen ein „hohes" Risiko für die betroffen Personen verbleibt, siehe Frage 54).

Die Datenschutz-Folgenabschätzung ist daher eine systematische Evaluierung einer (oder mehrerer ähnlicher) Datenverarbeitungen hinsichtlich der Risiken für die Betroffenen.

53) Wann ist eine Datenschutz-Folgenabschätzung erforderlich bzw wie erkenne ich die Erforderlichkeit?

Die Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung entsteht, sobald voraussichtlich ein hohes Risiko für die betroffenen Personen aufgrund der beabsichtigten Datenverarbeitung vorliegt.

Ob ein hohes Risiko vorliegt, kann nur im Einzelfall beurteilt werden. Die DSGVO zählt beispielhaft Fälle auf, wie etwa die umfangreiche Verarbeitung besonderer Datenkategorien oder personenbezogene Daten über strafrechtliche Verurteilungen.

Darüber hinaus ist möglicherweise die Erforderlichkeit einer Datenschutz-Folgenabschätzung gegeben, wenn zwei oder mehr der nachstehenden Faktoren zutreffen:

1. Evaluierung oder Scoring, inklusive Profilbildung und Vorhersagen
2. Automatisierte Entscheidungen mit rechtlicher oder ähnlich beeinträchtigender Wirkung
3. Systematische Beobachtung
4. Vertrauliche oder höchstpersönliche Daten
5. In großem Umfang verarbeitete Daten
6. Datensätze, die abgeglichen oder kombiniert wurden
7. Daten, die verletzliche Datensubjekte betreffen
8. Innovative Nutzung oder Verwendung von technologischen und organisatorischen Lösungen
9. Datenübermittlung in Drittstaaten außerhalb der EU
10. Datenverarbeitungen, die den Betroffenen davon abhalten, ein Recht geltend zu machen odereinen Dienst oder Vertrag zu nutzen

Ferner kann die Datenschutzbehörde eine Liste von Datenverarbeitungen erstellen, bei denen eine Datenschutz-Folgenabschätzung jedenfalls notwendig ist („Black-List") bzw. in keinem Fall erforderlich ist („White-List").

Eine gültige „Black-List“ existiert derzeit (Stand 25.09.2018) (noch) nicht. Die Datenschutzbehörde plant allerdings, eine solche Black-List zu erstellen und hat bereits einen entsprechenden Entwurf verfasst. Nach derzeitigem Wissensstand wird diese Black-List keine Liste von Datenverarbeitungen enthalten, sondern nur Kriterien, bei deren Vorliegen jedenfalls eine Datenschutz-Folgenabschätzung vorzunehmen ist.

Die „White-List“ ist in der konsolidierten Fassung im Rechtsinformationssystem unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010206 abrufbar.

54) Was ist zu tun, wenn ich bei einer Datenschutz-Folgenabschätzung trotz Berücksichtigung sämtlicher Maßnahmen der Auffassung bin, dass ein hohes Risiko für die Betroffenen verbleibt bzw ich ein solches nicht ausschließen kann?

Für den Fall, dass trotz entsprechender Maßnahmen des Verantwortlichen ein hohes Risiko für die betroffenen Personen nicht ausgeschlossen werden kann, ist die Datenschutz-Behörde zu informieren, wobei es ratsam aber nicht verpflichtend ist, dies vor Aufnahme der Datenverarbeitung zu tun.

Die Behörde kann in der Folge dem Verantwortlichen eine schriftliche Empfehlung unterbreiten, wie etwa die Umsetzung einer oder mehrerer konkreter technischer Maßnahmen. Sie kann aber auch ihre Befugnisse gemäß DSGVO ausüben, was von einer Verwarnung, dass die Datenverarbeitung die Datenschutz-Grundverordnung verletzt bis zur vorübergehenden oder endgültigen Beschränkung der Verarbeitung, einschließlich eines Verbots, reichen kann.
Der Verantwortliche hat allerdings den Vorteil, dass er nach erfolgreicher Durchführung eines solchen Konsultierungs-Verfahrens davon ausgehen darf, dass seine Datenverarbeitung im Einklang mit der Datenschutz-Grundverordnung steht.

55) Wer muss und wer kann einen Datenschutzbeauftragten bestellen?

Behörden und öffentliche Stellen müssen in jedem Fall einen Datenschutz-Beauftragten benennen. Verantwortliche aus dem privaten Bereich (dh insbesondere Unternehmer) können freiwillig immer einen Datenschutzbeauftragten benennen und müssen dies verpflichtend in folgenden Fällen tun:

- Die Kerntätigkeit des Verantwortlichen besteht aus Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder

- die Kerntätigkeit des Verantwortlichen besteht in der umfangreichen Verarbeitung besonderer Datenkategorien oder von Daten über strafrechtliche Verurteilungen und Straftaten.

56) Müssen Markt- und Meinungsforschungsinstitute einen Datenschutzbeauftragten bestellen?

Weder die Datenschutz-Grundverordnung noch nationale Vorschriften wie etwa das Datenschutzgesetz 2018 sehen eine ausdrückliche Pflicht für Markt- und Meinungsforschungsinstitute zur Ernennungen eines Datenschutz-Beauftragten vor. Anders ist beispielsweise die Situation in Deutschland, wo gesetzlich die Ernennung eines Datenschutzbeauftragten vorgeschrieben ist, sobald Daten für Zwecke der Markt- und Meinungsforschung verarbeitet werden.

Daher kommen die allgemeinen Grundsätze gemäß DSGVO für die Ernennung eines Datenschutz-Beauftragten zum Tragen (für weitere Informationen siehe Frage 55).

Markt- und Meinungsforschungsinstitute. die umfangreiche Verarbeitungen besonderer Datenkategorien oder von Daten über strafrechtliche Verurteilungen und Straftaten als Kerntätigkeit durchführen müssen einen Datenschutzbeauftragten bestellen. Ob die Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, ist allerdings immer im Einzelfall zu prüfen.

Die Bestellung eines Datenschutzbeauftragten ist darüber hinaus eine Voraussetzung für den Zugang zu öffentlichen Registern zu wissenschaftlichen Forschungszwecken („Registerforschung"). (für weitere Informationen siehe Frage 24).

57) Was ist die Funktion eines Datenschutz-Beauftragten?

Der Datenschutzbeauftragte berät den Verantwortlichen und dessen Mitarbeiter über die anwendbaren Datenschutzvorschriften und überwacht die Einhaltung dieser datenschutzrechtlichen Bestimmungen und Strategien. Er unterstützt den Verantwortlichen bei der Einhaltung von dessen datenschutzrechtlichen Pflichten. Er ist des Weiteren die informierte Ansprechperson für die Datenschutzbehörde, aber auch betroffene Personen können sich an ihn wenden, wenn sie Fragen über die Verarbeitung ihrer personenbezogenen Daten haben oder ihre Betroffenenrechte wahrnehmen möchten. Ferner ist er im Falle einer Datenschutz-Folgenabschätzung vom Verantwortlichen zu konsultieren.

58) Haftet der Datenschutzbeauftragte für Verstöße gegen die DSGVO?

Der Datenschutzbeauftragte unterstützt den Verantwortlichen bei der Einhaltung seiner datenschutzrechtlichen Pflichten. Er „übernimmt" diese allerdings nicht. Daher ist jede Pflichtverletzung dem Verantwortlichen einer Datenverarbeitung zuzurechnen, weshalb ausschließlich dieser auch einer Strafe der Datenschutzbehörde bzw. Schadenersatzforderung von betroffenen Personen ausgesetzt ist.

Es kann allerdings Fälle geben, in denen der Datenschutzbeauftragte gegenüber dem Verantwortlichen eine Haftung trifft, weil er beispielsweise gegen seine Pflichten in grob fahrlässiger Weise verstoßen hat, wodurch dem Verantwortlichen ein Schaden entstanden ist. Inwiefern ein solcher Schadenersatzanspruch des Verantwortlichen tatsächlich gegeben bzw durchsetzbar ist, muss jeweils im Einzelfall geprüft werden.

WIRTSCHAFTSKAMMER WIEN
Werbung · Marktkommunikation

IMPRESSUM

Fachgruppe Werbung und Marktkommunikation Wien
Schwarzenbergplatz 14 | 1041 Wien
T +43 1/514 50-3512
E werbungwien@wkw.at
W wko.at/wien/werbung | **W** werbungwien.at

Texterstellung: Mag. Dietmar Huemer, LL.M.; Mag. Stefan Winroither
Diese FAQ-Sammlung ist ein Kooperationsprojekt der Fachgruppe Werbung und Marktkommunikation Wien mit dem VdMI.
Grafik&Layout: Ref. Organisationsmanagement | Fotorechte: Shutterstock/Maksim Kabakou
Stand: 10/2018