INTERNET OMBUDSMANN

FAQ zur DSGVO

Häufige Fragen und Antworten zur Datenschutz-Grundverordnung

Wien, Mai 2018

Im Auftrag der Arbeiterkammern Österreich

AK ÖSTERREICH

Österreichisches Institut für angewandte Telekommunikation

Impressum

Österreichisches Institut für angewandte Telekommunikation

Ungargasse 64-66/3/404

1030 Wien

Inhalt

Einleitung

Die am 25.05.2018 in Geltung tretende Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtline 95/46/EG („***DS-GVO***“) stellt eine Weiterentwicklung des europäischen Datenschutzrechts dar und wird in Zukunft eine bessere Durchsetzung des Datenschutzrechts ermöglichen. Die folgenden FAQ und die entsprechenden Antworten sollen einen Überblick über das in Österreich geltend Datenschutzrecht ermöglichen und punktuell auftretende Fragen beantworten.
Da die DS-GVO einen gänzlich neuen Rechtsakt darstellt, sind viele Rechtsfragen in diesem Zusammenhang noch nicht gänzlich geklärt. Erst die zukünftige Rechtsprechung wird zeigen, wie die Bestimmungen im Detail auszulegen sind. Die nachfolgenden Ausführungen dürfen daher noch nicht als abschließende Antworten verstanden werden. Die Ausführungen dienen nur der Erstinformation und können keine rechtliche Beratung ersetzen. Es wird daher auch keine Haftung für allfällige Schadenersatzansprüche übernommen.

1. Was ist die Grundidee des Datenschutzrechts?

Das Datenschutzrecht bezweckt den Schutz natürlicher Personen in ihrer Privatsphäre. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Der Schutz personenbezogener Daten ist allerdings kein unbeschränktes Recht. Es muss Im Einzelfall gegen andere Grundrechte – zB das Grundrecht auf Meinungs- und Informationsfreiheit oder das Grundrecht auf freie Berufsausübung – abgewogen werden.

2. Wo ist das Datenschutzrecht geregelt?

Die zentrale Vorschrift des Datenschutzrechts ist die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtline 95/46/EG („**EU-*Datenschutz-Grundverordnung***“ oder „***DS-GVO***“), die am 25.05.2018 in Geltung tritt. Die DS-GVO löst die Richtline 95/46/EG („***EU-Datenschutz-Richtlinie***“) ab ist in allen EU-Mitgliedstaaten direkt anwendbar.
Die DS-GVO enthält die zentralen und grundsätzlichen Regelungen zum Datenschutzrecht; sie lässt den EU-Mitgliedstaaten allerdings die Möglichkeit, einzelne Bereiche der DS-GVO noch genauer zu regeln. Österreich hat davon teilweise Gebrauch gemacht und dazu das „Datenschutzgesetz“ (BGBl. I Nr. 120/2017) erlassen, das gemeinsam mit der DS-GVO anzuwenden ist. Das „Datenschutzgesetz“ löst das in Österreich davor geltende „Datenschutzgesetz 2000“ (mit dem die EU-Datenschutz-Richtline in nationales Recht umgesetzt wurde) ab.

3. Wer unterliegt den Verpflichtungen des Datenschutzrechts?

Grundsätzlich unterliegt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle den Verpflichtungen des Datenschutzrechts.
Das Datenschutzrecht unterscheidet einerseits zwischen dem „Verantwortlichen“, d.h. derjenigen natürlichen oder juristischen Person, die eine Datenverarbeitung durchführt sowie über die Zwecke und Mittel der Datenverarbeitung entscheidet, und andererseits der „betroffenen Person“, d.h. jener natürlichen Person, deren personenbezogene Daten verarbeitet werden. Der Verantwortliche ist der primäre Adressat des Datenschutzrechts.
Sobald eine Person, Behörde, Einrichtung oder andere Stelle (der Verantwortliche) personenbezogene Daten einer natürlichen Person (der betroffenen Person) verarbeitet, unterliegt der Verantwortliche dem

Datenschutzrecht und muss die sich daraus ergebenden Verpflichtungen einhalten.

> *Beispiel:* *Der Student S. gibt im Zuge seiner Anmeldung beim Fitnesscenter F. seinen Namen, seine Adresse, seine E-Mail-Adresse, seinen Body-Mass-Index und seine Bankverbindung bekannt. Das Fitnesscenter F. verarbeitet die personenbezogenen Daten des S. und ist daher „Verantwortlicher" im datenschutzrechtlichen Sinn. Der Student S., dessen personenbezogene Daten von F. verarbeitet werden, ist hingegen die „betroffene Person" im datenschutzrechtlichen Sinn. Das Fitnesscenter F. unterliegt als „Verantwortlicher" den datenschutzrechtlichen Verpflichtungen und darf die personenbezogenen Daten der „betroffenen Person" S. nur im Einklang mit der Datenschutz-Grundverordnung (DS-GVO) und dem österreichischen Datenschutzgesetz (DSG) verarbeiten. Der Student S. kann hingegen seine Rechte als „Betroffener" gemäß DS-GVO und DSG (Recht auf Auskunft, Recht auf Löschung etc.) in Anspruch nehmen.*

4. Gilt das Datenschutzrecht auch für meine rein privaten Datenverarbeitungen (private Telefonlisten, Facebook, WhatsApp am Privathandy etc.)

Die Datenschutz-Grundverordnung gilt nicht für Datenverarbeitungen durch natürliche Personen bei der Ausübung rein persönlicher und familiärer Tätigkeiten („Haushaltsausnahme" oder „Household exemption"). Es darf kein Bezug zu einer beruflichen und wirtschaftlichen Tätigkeit bestehen.
Als solchermaßen private Tätigkeiten gilt nach überwiegender Meinung etwa das Führen einer Kontaktliste auf dem Handy oder die Nutzung sozialer Online-Netzwerke wie Facebook. Das Datenschutzrecht gilt aber natürlich sehr wohl für jene Unternehmen, die die sozialen Online-Netzwerke oder technischen Dienstleistungen zur Verfügung stellen; diese müssen ihrerseits die sie treffenden datenschutzrechtlichen Pflichten einhalten.

5. Unterliegen auch Verantwortliche mit Sitz außerhalb der EU dem europäischen Datenschutzrecht?

Ja, wenn die Datenverarbeitung damit im Zusammenhang steht, Personen in der EU Waren oder Dienstleistungen anzubieten (sei es auch kostenlos) oder das Verhalten betroffener Personen in der EU zu beobachten, ist die DSGVO auch für Unternehmen mit Sitz außerhalb der EU anwendbar. Daher müssen sich auch Unternehmen mit Sitz in den USA an das europäische Datenschutzrecht halten.

> *Beispiel:* *Der Suchmaschinen-Betreiber M. mit Sitz in den USA bietet seine Dienstleistungen auch Personen in der EU an. Der Suchmaschinen-Betreiber M. unterliegt den Verpflichtungen der Datenschutz-Grundverordnung (DS-GVO) auch, wenn er über keine Niederlassung in der EU verfügt und sich seine gesamte Infrastruktur außerhalb der EU befindet. Die Aufsichtsbehörden in den EU-Mitgliedstaaten können auch Strafen gegen den US-amerikanischen Suchmaschinen-Betreiber M. verhängen.*

6. Wen schützt das Datenschutzrecht?

Die Datenschutz-Grundverordnung (DS-GVO) schützt alle natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten. Auch Unternehmer oder Arbeitgeber, soweit es sich dabei um natürliche Personen handelt, werden durch die DS-GVO geschützt. Die DS-GVO ist also nicht bloß Verbraucher- oder Arbeitnehmerschutzrecht, sondern schützt alle natürlichen Personen. Juristische Personen (zB eine GmbH) werden vom Schutzbereich des Datenschutzrechts nicht erfasst. Soweit der Firmenwortlaut einer juristischen Person den Namen natürlicher Personen enthält, findet das Datenschutzrecht aber wiederum Anwendung.

7. Unter welchen Voraussetzungen ist das Datenschutzrecht (DS-GVO und DSG) überhaupt anwendbar?

Das Datenschutzrecht ist anwendbar, wenn personenbezogene Daten zumindest teilweise automatisiert (d.h. grundsätzlich IT-unterstützt) verarbeitet werden. Es reicht aus, wenn personenbezogene Daten erhoben oder auch nur gespeichert werden. Die Anwendung des Datenschutzrechts setzt nicht voraus, dass personenbezogene Daten zusätzlich auch noch analysiert oder zu bestimmten Zwecken verwendet werden.

> *Beispiel:* *Der Händler H. führt in einem Textdokument fortlaufende ungeordnete Notizen zu seinen Kunden. Sobald H. diese personenbezogenen Notizen auf seinem Computer eingibt, ist das Datenschutzrecht anwendbar, weil personenbezogene Daten automationsunterstützt (bzw. IT-unterstützt) verarbeitet werden.*

Darüber hinaus ist das Datenschutzrecht auch dann anwendbar, wenn personenbezogene Daten rein manuell (d.h. nicht automatisiert) verarbeitet werden und nachfolgend in einem Dateisystem (d.h. in einer nach bestimmten Kriterien zugänglichen und durchsuchbaren Kartei) gespeichert werden.

> *Beispiel:* *Der Privatdetektiv P. hat den Auftrag, den G. zu observieren. Bei seiner Überwachung notiert sich P. handschriftlich, dass G. jeden Abend in die Eden-Bar geht. Außerdem geben ihm Angestellte der Eden-Bar über die sexuellen Vorlieben des G. Auskunft, was P. wiederum in seinem Notizblock notiert. Die handschriftlichen Notizen des P. unterliegen nicht dem Datenschutzrecht. Erst wenn P. seine Notizen in einer nach Namen geordneten Kartei oÄ ablegt, kommt das Datenschutzrecht zur Anwendung.*

8. Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Eine Person ist identifiziert, wenn sie durch bestimmte Merkmale unverwechselbar als genau diese Person gekennzeichnet ist. Identifizierbar ist eine Person dann, wenn sie aufgrund der Zuordnung zu einer Kennung (zB einer Kennnummer, Standortdaten, einer Online-Kennung etc.) und einem entsprechenden Zusatzwissen bestimmt werden kann.
Der Name einer Person ist das gängigste Kriterium, um eine Person zu identifizieren. Tragen mehrere Personen den gleichen Namen, müssen zusätzliche Identifizierungsmerkmale (zB Geburtsdatum, Wohnort etc.) herangezogen werden, um eine Person eindeutig zu identifizieren. Der Name ist allerdings nicht das einzige Kriterium, um eine Person zu identifizieren. So kann eine Person auch über eine Kombination verschiedener Informationen, die für sich allein keine Identifizierung zulassen, identifiziert werden.

> *Beispiel:* *Über das Attribut „derzeitiger Präsident der USA“ lässt sich eine bestimmte Person identifizieren. Ebenso könnte eine bestimmte Person über die Schnittmenge*

unterschiedlicher Informationen, zB „Mitglied des Schützenvereins Hohenems, der in der Postgasse wohnt und mit einer Ehefrau namens Gerda verheiratet ist" (fiktives Beispiel) identifiziert werden.

Personenbezogene Daten müssen nicht unbedingt Zahlen (Sozialversicherungsnummer, Kreditkartennummer, etc.) oder typische Formularangaben (Adresse, Geburtsort etc.) sein. Es kann sich bei personenbezogenen Daten auch um ganz allgemeine Informationen (Charaktereigenschaften, Freizeitverhalten etc.) handeln. Auch subjektive Meinungen („komplett inkompetent" oder „zahlungsunfähig") können personenbezogene Daten sein, egal ob diese Aussagen tatsächlich zutreffen oder unrichtig sind.

Beispiel: *Die Aussage „A. mag Actionfilme lieber als romantische Komödien." enthält ebenso personenbezogene Daten wie die Aussage „A. kommt jeden Tag zu spät in die Arbeit.", weil sie jeweils Informationen über die Person A. enthalten.*

9. Wann liegt ein Personenbezug (personenbezogener Daten) vor?

Personenbezogene Daten müssen einen Bezug zu einer bestimmten oder zumindest bestimmbaren Person aufweisen, ansonsten würde es sich eben nicht um *personenbezogene* Daten handeln. Rein statistische Daten, Daten über eine bestimmte Maschinenleistung usw. sind in der Regel keine personenbezogenen Daten, weil diese Informationen nichts über eine bestimmte oder bestimmbare Person aussagen. Es handelt sich hier einfach nur um Daten, jedoch nicht um personenbezogene Daten.

Beispiel: *Die Aussage „353.320 Pkw-Neuzulassungen im Jahr 2017" enthält keine personenbezogenen Daten, auch wenn 353.320 oder weniger konkrete Personen einen Pkw zugelassen haben mögen. Sie enthält nämlich keine Information über eine identifizierte oder identifizierbare Person.*

Allerdings können sich auch Daten, die auf den ersten Blick keinen Personenbezug aufweisen, als personenbezogene Daten herausstellen. So handelt es sich beispielsweise bei dynamischen IP-Adressen um personenbezogene Daten, wenn der Verantwortliche (zB ein Website-Betreiber, der die IP-Adressen seiner Besucher speichert) über rechtliche Möglichkeiten verfügt, um mit Hilfe Dritter (zB mit der Hilfe von Strafverfolgungsbehörden) die betroffene Person anhand der dynamischen IP-Adresse bestimmen zu lassen. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.
Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden. Ein ursprünglich nicht vorliegender Personenbezug kann auch erst im Nachhinein mit dem Lauf der Zeit entstehen. Somit sind bei der Erhebung von Daten auch absehbare zukünftige technologische Entwicklungen zu berücksichtigen und zu prüfen, ob sich aufgrund dieser Entwicklungen in absehbarer Zukunft ein Personenbezug herstellen lassen wird.

Beispiel: *Technologische Entwicklungen wie der Abgleich zwischen umfangreichen Datensätzen lassen mittlerweile eine Identifizierung von Personen zu, die vor einigen Jahren noch nicht möglich gewesen wäre. Es ist also denkbar, dass ein per se nicht einer bestimmten Person zuordenbarer Datensatz (zB ein Datensatz über bestimmte Aufenthaltsorte zu einer bestimmten Zeit) in Kombination mit weiteren Datensätzen (zB Facebook-Fotos, Aufzeichnung über Zahlungsvorgänge etc.)*

letztlich eine Identifizierung einer bestimmten Person zulässt und die in dem Datensatz enthaltenen Daten als personenbezogene Daten zu qualifizieren sind.

10. Was sind „sensible Daten“?

Die DS-GVO spricht nicht von sensiblen Daten, sondern von „besonderen Kategorien personenbezogener Daten“. Dabei handelt es sich um folgende Arten von personenbezogenen Daten:

- Daten über die rassische und ethnische Herkunft
- Daten über politische Meinungen
- Daten über religiöse oder weltanschauliche Überzeugungen
- Daten über die Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (zB Fingerabdruck, Gesicht etc.)
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Die Verarbeitung dieser „kategorisierten“ Daten ist grundsätzlich untersagt. Die Verarbeitung ist nur in speziell aufgezählten Fällen zulässig (zB zur Erfüllung arbeitsrechtlicher Pflichten; aufgrund ausdrücklicher Einwilligung; zum Zweck einer medizinischen Behandlung; Verarbeitung durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Organisation ohne Gewinnerzielungsabsicht u.a.)

11. Was sind pseudonymisierte Daten?

Pseudonymisierte Daten sind Daten, die ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen („Schlüssel“) müssen gesondert aufbewahrt werden. Außerdem müssen technische und organisatorische Maßnahmen ergriffen werden, damit dieser „Schlüssel“ dritten Personen nicht zugänglich ist.

Beispiel: *Der Pharmakonzern H. gibt eine klinische Studie in Auftrag. Der Studienleiter S. ordnet vor der Durchführung der medizinischen Studie den Studienteilnehmern eine Kennnummer zu, sodass die Identität der Studienteilnehmer nicht mehr eruiert werden kann. S. speichert den Zuordnungsschlüssel an einem eigenen Ort und trifft Maßnahmen, dass andere Personen (zB der Pharmakonzern H.) keinen Zugang zu dem Zuordnungsschlüssel haben. Die personenbezogenen Daten werden dadurch „pseudonymisiert“ und nur noch in „pseudonymisierter“ Form verarbeitet. Nur der Studienleiter S., der über den Zuordnungsschlüssel verfügt, kann die Zuordnung der Daten (mittels des Zuordnungsschlüssels) zu den konkreten Studienteilnehmern vornehmen und daher wieder den Personenbezug herstellen.*

Pseudonymisierte Daten sind trotz Pseudonymisierung immer noch personenbezogene Daten (weil der Personenbezug wiederhergestellt werden kann) und unterliegen daher auch dem Datenschutzrecht. Die Pseudonymisierung von Daten stellt allerdings ein geeignetes und gewünschtes Instrument dar, um die Datensicherheit zu erhöhen. Soweit ein Personenbezug für eine bestimmte Verarbeitung überhaupt erforderlich ist, sollten personenbezogene Daten nach Ihrer Erhebung daher nach Möglichkeit pseudonymisiert und in pseudonymisierter Form verarbeitet werden.

Beispiel: Auch das Verpixeln von im Rahmen einer Videoüberwachung aufgenommenen Personen ist als eine Pseudonymisierung einzuordnen, wenn unter bestimmten Umständen das Entpixeln möglich bleibt.

Je größer Datenbestände sind, umso häufiger schützt Pseudonymisierung nicht verlässlich vor einer Identifizierung der Person. Anhand der Schnittmenge mehrerer pseudonymisierter Datensätze lässt sich nämlich oft bereits eine konkrete Person identifizieren.

12. Was sind anonymisierte Daten?

Anonyme Daten sind Daten, die sich überhaupt nicht auf eine identifizierte oder identifizierbare Person beziehen.
Anonymisierte Daten liegen vor, wenn personenbezogene Daten in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Der Verantwortliche und jede andere Person darf nicht mehr in der Lage sein, eine Person mittels dieser Daten zu (re-) identifizieren. Eine Anonymisierung muss Rückschlüssen auf eine bestimmte Person verlässlich entgegenwirken. Je größer die Datenmengen, desto leichter wird der Rückschluss auf eine bestimmte Person möglich.
Um festzustellen, ob Daten pseudonymisiert oder anonymisiert wurden, sind alle Mittel heranzuziehen, die von dem Verantwortlichen oder einer dritten Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die betroffene Person direkt oder indirekt zu identifizieren. Dabei sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.
Anonyme und anonymisierte Daten unterliegen nicht dem Datenschutzrecht.

13. Was ist unter einer „Datenverarbeitung“ zu verstehen?

Zunächst ist festzuhalten, dass bei einer Datenverarbeitung nicht eine Vielzahl von Daten verarbeitet werden muss. Es reicht bereits aus, wenn ein einzelnes personenbezogenes „Datum“ (Einzahl von „Daten“) verarbeitet wird.
Eine „Verarbeitung“ bezeichnet jeden 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.
Unter „Datenverarbeitung“ ist also nicht nur eine Analyse, eine Auswertung, ein Abgleich o. Ä. von Daten zu verstehen, sondern allein schon ein einfacher Vorgang wie das Erheben von personenbezogenen oder das bloße Speichern von personenbezogenen Daten an einem sicheren Ort. Selbst das Löschen oder Vernichtung von personenbezogenen Daten stellt eine Datenverarbeitung dar, die nur aufgrund einer bestimmten Rechtsgrundlage erfolgen darf.

Beispiel: Im Rahmen einer Telefon-Umfrage werden Personen zu Ihren Essgewohnheiten befragt. Bereits das automationsunterstützte Erheben dieser Daten stellt eine „Datenverarbeitung“ (Erheben von Daten) dar, soweit der Personenbezug dieser Informationen mittels Telefonnummer oÄ hergestellt werden kann.

14. Ist eine Videoaufnahme eine Datenverarbeitung?

Eine Videoaufnahme als eine Verarbeitung von Lichtbildern stellt dann eine Datenverarbeitung dar, wenn Lichtbilder von identifizierten oder identifizierbaren Personen, und damit personenbezogene Daten verarbeitet werden. Daher stellt eine Videoaufnahme von Personen grundsätzlich eine Datenverarbeitung dar, es sei denn die Personen auf der Videoaufnahme sind in keiner Weise erkennbar oder bestimmbar. Für Videoaufnahmen als „Bildverarbeitungen" bestehen in Österreich spezielle datenschutzrechtliche Vorschriften.

15. Ist die Übermittlung von Daten an andere Personen eine „Datenverarbeitung"?

Auch die Übermittlung/Weitergabe von personenbezogenen Daten (oder Offenlegung von personenbezogenen Daten) an Dritte stellt eine Datenverarbeitung dar. Der Verantwortliche darf personenbezogene Daten betroffener Personen nur dann an Dritte weitergeben, wenn es eine Rechtsgrundlage dafür gibt. Der Empfänger von personenbezogenen Daten wird mit dem Empfang der Daten selbst zum Verantwortlichen, sofern er die Daten bewusst weiter speichert. Der Empfänger darf die personenbezogenen Daten seinerseits nur verarbeiten, wenn er sich auf eine Rechtsgrundlage stützen kann.

> *Beispiel:* *Der Arbeitgeber A. übermittelt aufgrund seiner arbeitsrechtlichen Verpflichtung personenbezogene Daten des Arbeitnehmers T. an die Finanzbehörden weiter. Die Finanzbehörde wird mit dem Empfang selbst zum Verantwortlichen hinsichtlich der personenbezogenen Daten des T. Sie verarbeitet die personenbezogenen Daten des T. zur Berechnung von dessen Steuerpflicht.*

16. Was ist ein Auftragsverarbeiter?

Einen speziellen Fall der Datenübermittlung stellt die Übermittlung bzw. die Offenlegung von personenbezogenen Daten an einen sogenannten Auftragsverarbeiter dar.
Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Auftragsverarbeiter wird sozusagen als „verlängerter Arm" des Verantwortlichen tätig. Er darf die personenbezogenen Daten nur im Rahmen des Auftrags des Verantwortlichen verarbeiten. Zwischen dem Verantwortlichen und dem Auftragsverarbeiter muss eine Vereinbarung bestehen, wonach der Auftragsverarbeiter personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeitet und in welcher noch einige andere Pflichten des Auftragsverarbeiters festgelegt sind.
Ein Auftragsverarbeiter, der die ihm überlassenen personenbezogenen Daten pflichtwidrig entgegen den Weisungen des Verantwortlichen Daten für eigene Zwecke verarbeitet, gilt in Bezug auf diese Verarbeitung dann selbst als Verantwortlicher.
Die Weitergabe von personenbezogenen Daten an einen Auftragsverarbeiter ist grundsätzlich zulässig, ohne dass eine gesonderte Einwilligung eingeholt werden muss. Der Betroffene ist allerdings über den Einsatz von Auftragsverarbeitern zu informieren (siehe Frage 38).

> *Beispiel:* *Der Verantwortliche speichert personenbezogene Daten beim Cloud-Anbieter C.. Der Cloud-Anbieter C. ist als Auftragsverarbeiter anzusehen, weil er die personenbezogenen Daten nur im Auftrag des Verantwortlichen verarbeitet (in der Regel lediglich speichert).*

Wenn der Cloud-Anbieter C. die bei ihm gespeicherten Daten allerdings für eigene Zwecke (zB Analyse der personenbezogenen Daten zu Werbezwecken oder zur Erstellung von Nutzerprofilen) verarbeitet, gilt er nicht mehr als Auftragsverarbeiter, sondern wird selbst zum Verantwortlichen, der die personenbezogenen Daten nur aufgrund einer eigenen Rechtsgrundlage verarbeiten dürfte. Im konkreten Fall wäre die Verarbeitung durch den Cloud-Anbieter unrechtmäßig.

17. Welche Grundsätze sind bei der Datenverarbeitung einzuhalten?

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn eine bestimmte Rechtsgrundlage dafür besteht. Allgemein darf eine Datenverarbeitung nur im Einklang mit den folgenden Grundsätzen erfolgen:

a. „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“
   - Eine Datenverarbeitung ist grundsätzlich verboten, außer es liegt eine Rechtsgrundlage für die Datenverarbeitung vor.
   - Die betroffene Person muss über sie betreffende Datenverarbeitungen und ihre Rechte klar und verständlich informiert werden.

b. „Zweckbindung“
   - Personenbezogene 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.

c. „Datenminimierung“
   - Eine Datenverarbeitung muss dem Zweck der Verarbeitung angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

d. „Richtigkeit“
   - Personenbezogene Daten sollen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

e. „Speicherbegrenzung“
   - Personenbezogene Daten sollen grundsätzlich nur solange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

f. „Integrität und Vertraulichkeit“
   - Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.

Jede Person, die personenbezogene Daten verarbeitet, muss sicherstellen, dass diese Grundsätze eingehalten werden und muss die Einhaltung dieser Grundsätze auch nachweisen können (Grundsatz der „Rechenschaftspflicht“).

18. Unter welchen Bedingungen dürfen meine personenbezogenen Daten verarbeitet werden bzw. darf ich personenbezogene Daten verarbeiten?

Eine Datenverarbeitung zu einem bestimmten Zweck darf nur durchgeführt werden, wenn es zumindest einen Rechtfertigungsgrund bzw. eine bestimmte Rechtsgrundlage dafür gibt. Entgegen zahlreicher Annahmen ist eine Zustimmungs- bzw. Einwilligungserklärung nicht die einzige Rechtsgrundlage für eine Datenverarbeitung.

Es muss also nicht immer notwendigerweise eine Zustimmungs- bzw. Einwilligungserklärung eingeholt werden, damit personenbezogene Daten rechtmäßig verarbeitet werden dürfen. Soweit die Datenverarbeitung auf eine andere Rechtsgrundlage gestützt werden kann, darf sie rechtmäßig vorgenommen werden.
Personenbezogene Daten dürfen nur dann verarbeitet, wenn zumindest eine der nachstehenden Bedingungen erfüllt ist.

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

   Beispiel: *Der Kunde K. erteilt beim Antrag auf Ausstellung einer O.-Kundenkarte seine Einwilligung, dass das Unternehmen O. Daten betreffend die Einkäufe von K. zum Zweck der Analyse von dessen Einkaufsverhalten verarbeitet werden dürfen.*

b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

   Beispiel: *Der Kunde K. gibt im Rahmen seiner Online-Bestellung beim Unternehmen U. seinen Namen, seine Adresse und seine Kreditkartennummer bekannt. Die Verarbeitung dieser Daten durch das Unternehmen U. ist zur Erfüllung des Kaufvertrags erforderlich und daher zulässig, weil ohne Verarbeitung dieser Daten der Vertrag zwischen K. und U. nicht erfüllt werden und die Ware nicht an die Adresse von K. geliefert werden könnte. Das Unternehmen U. muss für die Verarbeitung der Daten des K. daher nicht zusätzlich auch eine Einwilligungserklärung von K. einholen.*

   Beispiel: *Das Reisebüro R. erhebt personenbezogene Daten, um dem Kunden K. ein individualisiertes Vertragsangebot zu unterbreiten. Die Datenverarbeitung durch R. ist zulässig, auch wenn K. das Angebot letztlich nicht annehmen und daher kein Vertrag zwischen R. und K. zustande kommen sollte.*

c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

   Beispiel: *Der Arbeitgeber U. ist gesetzlich zur Anmeldung seines Arbeitnehmers C. beim zuständigen Sozialversicherungsträger verpflichtet. Daher ist auch die Verarbeitung und Übermittlung der personenbezogenen Daten des C. an den Sozialversicherungsträger durch den Arbeitgeber U. im gesetzlich vorgegebenen Rahmen zulässig.*

d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

   Beispiel: *Die Person H. wird nach einem Unfall bewusstlos angetroffen. Die Verarbeitung von H.‘s personenbezogenen Daten zur Erlangung von weiteren medizinischen Informationen über H. ist zum Schutz der lebenswichtigen Interessen von H. erforderlich und daher zulässig.*

e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

Beispiel: *Der Polizeibeamte P. erfasst im Zuge einer Fahrzeugkontrolle die personenbezogenen Daten des Lenkers L. und verarbeitet dessen Daten zum Zweck einer polizeilichen Abfrage.*

f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Beispiel: *Der Betreiber einer Website X. speichert kurzfristig Daten von Besuchern der Website, um externe Angriffe auf die Funktionalität der Website abwehren zu können und die IT- und Netz-Sicherheit zu gewährleisten.*

Beispiel: *Der Journalist J. erhebt und analysiert personenbezogene Daten von M. und N. zum Zweck der Recherche und der Veröffentlichung eines Zeitungsartikels über M. und N..*

Beispiel: *Ein Suchmaschinenbetreiber O. verarbeitet personenbezogene Daten, um bei Eingabe eines bestimmten Suchbegriffs (zB eines Namens) relevante Suchergebnisse im Zusammenhang mit eingegeben Suchbegriffen anzeigen zu können.*

19. Unter welchen Bedingungen dürfen sensible Daten verarbeitet werden?

Besondere Kategorien von personenbezogenen Daten („sensible Daten“) dürfen ausschließlich in folgenden Fällen verarbeitet werden:

a. Verarbeitung erfolgt aufgrund ausdrücklicher Einwilligung der betroffenen Person;
b. Verarbeitung ist zur Erfüllung (Ausübung) arbeits- oder sozialrechtlicher Pflichten (Rechte) erforderlich;
c. Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich;
d. Verarbeitung erfolgt durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht;
e. Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat;
f. Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich;
g. Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaatsaus aus Gründen eines erheblichen öffentlichen Interesses erforderlich;
h. Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich;

i. Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich;
j. Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich.

Eine Datenverarbeitung von sensiblen Daten in anderen als den abschließend aufgezählten Fällen ist nicht zulässig.

20. Wie muss eine datenschutzrechtlich wirksame Einwilligungserklärung aussehen?

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Eine datenschutzrechtliche Einwilligungserklärung muss gewisse Kriterien erfüllen, damit sie als wirksam abgegeben gilt und der Verantwortliche sich darauf berufen kann.

a. Freiwilligkeit

Die Einwilligung muss freiwillig erteilt werden. Die betroffene Person muss die Einwilligung verweigern oder zurückzuziehen können, ohne daraus Nachteile zu erleiden. Wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht (zB in einem Beschäftigungsverhältnis oder im Verhältnis zu einer Behörde), ist die Freiwilligkeit der Einwilligung stark zu hinterfragen.

Die Einwilligung gilt als nicht freiwillig erteilt, wenn der Abschluss oder die Erfüllung eines Vertrags von der Einwilligung des Betroffenen abhängig gemacht wird, obwohl die Einwilligung dafür nicht erforderlich ist („Kopplungsverbot“).

> *Beispiel:* *Ein Mechanismus, wonach ein Kunde nur dann eine Bestellung aufgeben kann, wenn er auch das Kästchen „Ich erteile meine Zustimmung, dass mein Name und meine E-Mail-Adresse für den Versand eines wöchentlichen Newsletters verarbeitet werden“ ankreuzt, ist unzulässig. Eine solchermaßen erteilte Einwilligung ist nicht wirksam.*

b. Bestimmtheit

Die Einwilligungserklärung muss für den konkreten Fall erteilt werden. Eine pauschale Einwilligung für mehrere Datenverarbeitungen ist nicht wirksam. Vielmehr muss für jede individuelle Datenverarbeitung jeweils eine eigene Einwilligung erteilt werden.

Der Zweck der Datenverarbeitung, für die eine Einwilligung erteilt wird, muss zum Zeitpunkt der Einwilligung klar festgelegt sein. Wenn der Verantwortliche die erhobenen Daten später zu einem anderen Zweck verarbeiten möchte, muss er in Regel zuvor eine separate Einwilligung vom Betroffenen dafür einholen (vgl. aber Frage 23 zur Weiterverarbeitung zu einem anderen Zweck).

> *Beispiel:* *Der Video-Streaming-Anbieter V. holt eine Einwilligung ein, dass er Daten über des Sehverhalten der Nutzer verarbeiten darf, um den Nutzern neue Vorschläge zu unterbreiten. Wenn er die Daten seiner Nutzer später noch zu anderen Zwecken (zB Verkauf der Daten über die Nutzung des Dienstes an Dritte zu Werbezwecken)*

verwenden will, die in der ursprünglichen Einwilligungserklärung nicht angeführt sind, muss er eine weitere Einwilligung der Nutzer einholen.

c. Informiertheit

Die Einwilligungserklärung muss in Kenntnis der Sachlage erteilt werden. Die betroffene Person muss vor Erteilung ihrer Einwilligung darüber informiert werden, wer der Verantwortliche der Datenverarbeitung ist, welche Arten von personenbezogenen Daten verarbeitet werden, zu welchem Zweck die Daten verarbeitet werden sowie ob und gegebenenfalls an wen personenbezogene Daten übermittelt werden und allenfalls welche Risiken mit der Übermittlung in einen Drittland verbunden sind. Ferner sollte die betroffene Person darüber informiert werden, wenn die Daten zu Zwecken einer automatisierten Entscheidung, zB zu Zwecken des „Profiling", verarbeitet werden (vgl. Frage 40).

Beispiel: Eine Einwilligungserklärung, wonach die betroffene Person in die „Verarbeitung ihrer personenbezogenen Daten zu allen erdenklichen Zwecken" einwilligt, ist unwirksam. Vielmehr müssen die einzelnen Datenarten (Name, E-Mail-Adresse etc.) sowie allfällige Empfänger und der genaue Zweck der Datenverarbeitung in der Einwilligungserklärung angeführt werden.

d. Unmissverständlichkeit und Unterscheidbarkeit.

Eine vom Verantwortlichen vorformulierte Einwilligungserklärung muss in verständlicher und leicht zugänglicher Form zur Verfügung gestellt werden. Außerdem muss die Einwilligung selbst in klarer und unmissverständlicher Art erteilt werden. Ein vorangekreuztes Kästchen oder die bloße Nutzung eines Dienstes bzw. der bloße Besuch einer Website kann keine unmissverständliche Einwilligungserklärung darstellen.

Eine Einwilligungserklärung muss aber nicht notwendigerweise schriftlich erteilt werden; vielmehr kann die Einwilligung auch mündlich oder durch eine bestimmte Handlung zum Ausdruck kommen, sofern diese unmissverständlich ist. Für die Verarbeitung „sensibler" Daten ist allerdings jedenfalls eine ausdrückliche (nicht bloß eine schlüssige) Einwilligung erforderlich.

Beispiel: Eine in den AGB „versteckte" datenschutzrechtliche Einwilligungserklärung ist nicht wirksam. Der Verantwortliche kann sich auf eine solche Einwilligung nicht berufen, auch wenn die AGB angekreuzt oder unterschrieben worden sein sollten. Vielmehr sollte der Verantwortliche getrennt von den AGB eine datenschutzrechtliche Einwilligung einholen.

e. Hinweis auf Widerrufsmöglichkeit

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung erfolgen können. Die betroffene Person muss vor Abgabe der Einwilligung über ihr Widerrufsrecht und darüber informiert werden, wie sie ihr Widerrufsrecht ausüben kann. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung nicht berührt.

Beispiel: Wenn die Einwilligung im Rahmen einer Registrierung auf einer Website erteilt wird, muss die Einwilligung auch über diese Website (zB nicht nur telefonisch zu Bürozeiten) widerrufen werden können.

21. Kann mein Kind auch eine Einwilligungserklärung abgeben?

Eine minderjährige betroffene Person kann eine wirksame Einwilligungserklärung abgeben, wenn sie über die dafür notwendige Einsichts- und Urteilsfähigkeit verfügt. Ob und inwieweit eine minderjährige Person über die notwendige Einsichts- und Urteilsfähigkeit verfügt, muss jeweils im Einzelfall beurteilt werden.
Das Gesetz sieht nur für einen bestimmten Fall eine explizite Altersgrenze vor, unter der eine minderjährige betroffene Person keine wirksame Einwilligungserklärung abgeben kann: Wenn eine minderjährige betroffene Person eine Einwilligung im Zusammenhang mit einem ihr angebotenen Dienst der Informationsgesellschaft (Online-Shops, Online-Informationsangebote, soziale Netzwerke etc.) abgeben soll, kann sie erst nach Vollendung des 14. Lebensjahres eine wirksame Einwilligungserklärung abgeben. Vor Vollendung des 14. Lebensjahres muss die Zustimmung des gesetzlichen Vertreters des Kindes eingeholt werden.

> *Beispiel:* *Die 12-jährige S. möchte sich bei dem sozialen Netzwerk F. anmelden. Der Anbieter des sozialen Netzwerks sollte bei der Anmeldung das Alter (in Sinne der Datenminimierung: nicht das Geburtsdatum) von S. abfragen. Wenn S. ihr wahres Alter angibt, sollte der Anbieter des sozialen Netzwerkes F. um Bekanntgabe der E-Mail-Adresse des gesetzlichen Vertreters von S. ersuchen, um auf diese Weise eine Zustimmung des gesetzlichen Vertreters einzuholen. Im Fall einer sehr risikogeneigten Datenverarbeitung (zB eine Verarbeitung sensibler Daten von S.) sollte F. eine andere Maßnahme zur Einholung der Zustimmung des gesetzlichen Vertreters (zB Ersuchen um Überweisung eines geringfügigen Betrages vom Bankkonto des gesetzlichen Vertreters unter Zusage der Rücküberweisung) ergreifen.*

22. Gelten früher abgegebene Einwilligungserklärungen nach In-Geltung-Treten der DSGVO weiter?

Wenn Datenverarbeitungen auf einer Einwilligung gemäß dem außer Kraft getretenen Datenschutzgesetz 2000 (DSG 2000) beruhen, ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen der DSGVO entspricht.
Einwilligungserklärungen, die also zum Zeitpunkt ihrer Erteilung den Anforderungen der DSGVO entsprochen haben, bleiben weiterhin wirksam.
Wenn die damals erteilte Einwilligungserklärung allerdings nicht den Anforderungen der DSGVO entspricht, muss der Verantwortliche eine neue rechtskonforme Einwilligungserklärung einholen.

23. Dürfen meine Daten zu einem anderen Zweck weiterverarbeitet werden, als zu dem sie ursprünglich erhoben wurden?

Grundsätzlich ist die Weiterverarbeitung von Daten zu einem anderen Zweck, als zu dem sie ursprünglich erhoben wurden, nur sehr eingeschränkt zulässig, weil dies im Widerspruch mit dem Grundsatz der Zweckbindung steht.
Der Zweck, zu dem die Daten weiterverarbeitet werden sollen, muss mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar sein. Dabei sind unter anderem (i) jede Verbindung zwischen den Zwecken, (ii) der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, (iii) die Art der personenbezogenen Daten, (iv) die möglichen Folgen der beabsichtigten

Weiterverarbeitung für die betroffenen Personen und (v) das Vorhandensein geeigneter Garantien (zB Verschlüsselung oder Pseudonymisierung) zu berücksichtigen.
Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung.

> *Beispiel:* *Im Rahmen des Verkaufs eines Unternehmens werden bestimmte personenbezogene Daten der Kunden, der Lieferanten, der Mitarbeiter etc. dem potenziellen Käufer offengelegt. Eine solche Weiterverarbeitung von Daten zu anderen Zwecken kann unter bestimmten Umständen zulässig sein.*

24. Unter welchen Bedingungen dürfen meine personenbezogenen Daten an Dritte übermittelt werden?

Die Übermittlung von personenbezogenen Daten stellt eine Datenverarbeitung ebenso wie die bloße Erhebung oder Speicherung von personenbezogenen Daten dar. Die Rechtmäßigkeit der Übermittlung von personenbezogenen Daten misst sich an denselben Kriterien wie die jede andere Datenverarbeitung, wie zB die Erhebung oder Speicherung von Daten. Dies bedeutet, dass die Datenübermittlung im Einklang mit den datenschutzrechtlichen Grundsätzen (siehe Frage 17) und nur aufgrund einer konkreten Rechtsgrundlage (siehe Frage 18) vorgenommen werden darf. Dies bedeutet aber nicht, dass die Datenübermittlung automatisch rechtmäßig ist, wenn nur die Datenerhebung rechtmäßig war. Vielmehr muss jede Datenverarbeitung (Erhebung, Speicherung, Übermittlung, etc.) für sich alleine beurteilt werden.

> *Beispiel:* *Die reiselustige B. bucht im Reisebüro R. einen Pauschalurlaub in Ägypten. Das Reisebüro R. leitet die Daten von B. an die Fluglinie und das Hotel in Ägypten weiter. Die Übermittlung der personenbezogenen Daten von B. an die Fluglinie und das Hotel in Ägypten ist rechtmäßig, weil die Datenübermittlung für die Erfüllung des Vertrages erforderlich ist. Die Übermittlung der personenbezogenen Daten an unbeteiligte Dritte (zB einen Reisestornoversicherer) hingegen wäre ohne entsprechende Einwilligung von B. nicht zulässig.*

25. Dürfen meine personenbezogenen Daten ins Ausland übermittelt werden?

Eine Übermittlung bzw. Offenlegung von personenbezogenen Daten an einen Empfänger mit Sitz in einem anderen EWR-Mitgliedstaat ist unter denselben Voraussetzungen zulässig, wie eine Datenübermittlung (oder einfach: eine Datenverarbeitung) innerhalb Österreichs. Soweit für eine solche Datenübermittlung eine Rechtsgrundlage besteht, darf der Verantwortliche personenbezogene Daten an einen Dritten mit Sitz in einem anderen EWR-Mitgliedstaat übermitteln bzw. offenlegen.
Die Datenübermittlung in einen Drittstaat (d.h. an einen Empfänger mit Sitz außerhalb der EWR) darf hingegen nur in ganz bestimmten Fällen vorgenommen werden:

a. Die Europäische Kommission hat beschlossen, dass das betreffende Drittland ein angemessenes Datenschutzniveau bietet (das betrifft derzeit die Staaten Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay);

b. Der Verantwortliche oder der Auftragsverarbeiter hat geeignete Garantien (zB verbindliche internen Datenschutzvorschriften, die von der zuständigen Aufsichtsbehörde genehmigt worden sind, oder Standarddatenschutzklauseln, die von der Kommission erlassen oder von einer Aufsichtsbehörde angenommen und von der Kommission genehmigt worden sind) vorgesehen, und den betroffenen Personen stehen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung;
c. Bestimmte Ausnahmefälle, zB die betroffene Person hat in die Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die Risiken einer solchen Datenübermittlung unterrichtet wurde; die Datenübermittlung ist für die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich; etc.

Ansonsten darf eine Übermittlung an ein Drittland nur dann erfolgen, wenn (i) die Übermittlung nicht wiederholt erfolgt, (ii) nur eine begrenzte Zahl von betroffenen Personen betrifft, (iii) für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen und (iv) der Verantwortliche geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche muss die Aufsichtsbehörde von solchen Übermittlungen in Kenntnis setzen und die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen informieren.
Was die Datenübermittlung in die USA anbelangt, besteht ein Abkommen zwischen der Europäischen Union und den USA („Privacy Shield“). Demnach können sich US-Unternehmen selbst verpflichten, gewisse datenschutzrechtliche Vorgaben einzuhalten und sich vom US-Handelsministerium zertifizieren lassen. Wurde das US-Unternehmen zertifiziert, ist der Datenfluss an dieses Unternehmen grundsätzlich genehmigungsfrei.

26. Darf ich personenbezogene Daten bei einem Cloud-Dienste-Anbieter mit Sitz außerhalb des EWR speichern?

Sofern der Cloud-Dienste-Anbieter seinen Sitz in einem Drittstaat hat, dem die Europäische Kommission ein angemessenes Schutzniveau attestiert (Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay), darf ich personenbezogene Daten unter denselben Bedingungen speichern, wie ich sie wie bei einem inländischen Cloud-Dienste-Anbieter speichern dürfte. Dasselbe trifft auf US-Unternehmen zu, die nach dem „Privacy Shield“-Regeln zertifiziert sind.
Sofern der Cloud-Dienste-Anbieter seinen Sitz in einem Drittstaat mit nicht angemessenem Datenschutzniveau hat, darf ich personenbezogene Daten nur unter den in Frage 25 dargestellten Voraussetzungen speichern.

> *Beispiel:* *Der Einzelunternehmer F. möchte seine Kundendatenbank beim US-amerikanischen Cloud-Anbieter G. führen, um von allen Orten auf die Kundendatenbank zugreifen zu können. Wenn G. nach dem vom US-Handelsministerium veröffentlichten EU-US Privacy Shield Framework zertifiziert ist, kann F. seine Kundendatenbank bei G. führen, ohne weitere Sicherheitsvorkehrungen hinsichtlich der Datenübermittlung in die USA ergreifen zu müssen. Da der Cloud-Anbieter G. für F. als Auftragsverarbeiter tätig wird, müssen F. und der Cloud-Anbieter G. allerdings zuvor eine schriftliche Vereinbarung über diese Auftragsverarbeitung abschließen (siehe Frage 16).*

27. Dürfen personenbezogene Daten von mir (zB ein Foto von mir) ohne meine Zustimmung auf der Website meines Arbeitgebers veröffentlicht werden?

Grundsätzlich ist eine Veröffentlichung von Mitarbeiterdaten auf der Website eine Datenverarbeitung, die nur aufgrund eines bestimmten Erlaubnistatbestands zulässig ist. Die Veröffentlichung von Mitarbeiterdaten (zB Name oder Telefonnummer) wird dann aufgrund eines berechtigten Interesses des Arbeitgebers zulässig sein, wenn die Zweckbestimmung des Arbeitsverhältnisses eine solche Veröffentlichung erfordert (zB Tätigkeit als Kundenberater oder Außendienstmitarbeiter). Die Veröffentlichung eines Fotos des Mitarbeiters wird allerdings in der Regel die Einwilligung des betreffenden Mitarbeiters erfordern.

28. Was bedeutet mein Recht auf Auskunft?

Jede betroffene Person kann vom Verantwortlichen Auskunft darüber verlangen, ob betreffende personenbezogene Daten verarbeitet werden. Wenn der Verantwortliche keine personenbezogenen Daten des Betroffenen verarbeitet, muss eine „Negativauskunft" erteilt werden, d.h. eine Bestätigung, dass keine personenbezogenen Daten verarbeitet werden. Wenn der Verantwortliche allerdings personenbezogene Daten des Betroffenen verarbeitet, muss er Auskunft über diese personenbezogenen Daten sowie die folgenden Punkte erteilen:

a. die Verarbeitungszwecke;
b. die Kategorien personenbezogener Daten, die verarbeitet werden;
c. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
d. falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
e. das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
f. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
g. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (d.h. jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen) und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Im Gegensatz zu den Informationen, die dem Betroffenen bei der Erhebung seiner Daten zur Verfügung gestellt werden, erhält der Betroffene im Rahmen seines Auskunftsersuchens materielle Einblick in die verarbeiteten Daten beim Verantwortlichen (und seinem Auftragsverarbeiter).

> *Beispiel:* *Der Student S. beantragt bei der Bank B. einen Kredit, um ein Auto kaufen zu können. Die Bank B. gewährt dem S. allerdings keinen Kredit, weil eine automatisierte Bonitätsprüfung ein negatives Ergebnis über S. ergeben hat. Nach einem entsprechenden Auskunftsersuchen muss die Bank B. unter anderem*

Auskunft darüber geben, wie die (automatisierte) Entscheidung über S. fehlende Bonität zustande gekommen ist. Außerdem muss die Bank B. darüber informieren, dass S. eine Beschwerde an die Datenschutzbehörde erheben kann.

29. Wie mache ich mein Auskunftsrecht geltend?

Das Auskunftsbegehren kann grundsätzlich formlos gestellt und muss nicht begründet werden. Der Verantwortliche kann allerdings einen Identitätsnachweis der betroffenen Person verlangen. Nach Einlangen des Auskunftsersuchens darf der Verantwortliche die personenbezogenen Daten der um Auskunft ersuchenden betroffenen Person nicht mehr löschen.
Der Verantwortliche muss der betroffenen Person eine Kopie der personenbezogenen Daten und die sonstigen Informationen in Papierform oder in einem gängigen elektronischen Format zur Verfügung stellen. Nach Möglichkeit sollte der Verantwortliche der betroffenen Person auch ein Fernzugang (zB einen Zugang zu einer elektronischen Datenbank, in dem die personenbezogenen Daten gespeichert werden) gewähren.
Der Verantwortliche muss dem Auskunftsbegehren einer betroffenen Person grundsätzlich innerhalb eines Monats nachkommen. In begründeten Fällen kann die Frist um weitere zwei Monate verlängert werden.
Wenn der Verantwortliche nicht binnen der Frist von einem bzw. drei Monaten Auskunft erteilt, kann die betroffenen Person eine Beschwerde bei der Datenschutzbehörde erheben (siehe Frage 49).
Für die Auskunftserteilung darf kein Entgelt verlangt werden; nur bei offenkundig unbegründeten oder exzessiven Anträgen (zB mehrfache Auskunftsersuchen binnen kurzer Zeitabstände) darf der Verantwortliche ein angemessenes Entgelt verlangen oder sich weigern, aufgrund des Antrags tätig zu werden.

Beispiel: *Der Pensionist P. erhält seit einiger Zeit Zusendungen von einem Unternehmen, das ihm nicht bekannt ist. F. kann das Unternehmen formlos (zB telefonisch) um Auskunft unter anderem darüber ersuchen, über welche personenbezogenen Daten von F. das Unternehmen verfügt und woher es diese Daten erhalten hat. F. kann von dem Unternehmen verlangen, ihm diese Informationen in Papierform zur Verfügung zu stellen. Wenn P. binnen eines Monats keine Auskunft und keine Antwort vom Unternehmen erhält, kann er eine Beschwerde an das Bundesverwaltungsgericht erheben.*

30. Was bedeutet mein Recht auf Berichtigung?

Eine betroffene Person hat das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten (z.B. eine alte Adresse) zu verlangen. Grundsätzlich besteht aber ohnehin eine eigenständige Verpflichtung des Verantwortlichen zur Berichtigung unrichtiger personenbezogener Daten.
Gegenstand des Rechts auf Berichtigung sind nur personenbezogene Informationen, die unrichtige Tatsachen betreffen. Unzutreffende Werturteile (d.h. subjektive Meinungen) können hingegen nicht berichtigt werden.
Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, dass unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung des Betroffenen — vervollständigt werden.
Wenn der Verantwortliche nicht binnen der Frist von einem bzw. (in begründeten Fällen) drei Monaten dem Verlangen nach Berichtigung nachkommt, kann die betroffenen Person eine Beschwerde bei der Datenschutzbehörde erheben (siehe Frage 49).

31. Was bedeutet mein Recht auf Löschung?

Jede betroffene Person kann vom Verantwortlichen verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der folgenden Gründe zutrifft:

a. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
b. Die betroffene Person widerruft ihre Einwilligung, auf die Datenverarbeitung gestützt war, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
c. Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
d. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
e. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

> *Beispiel:* *Das Unternehmen U. erhält im Rahmen einer Job-Ausschreibung Dutzende Bewerbungen von Arbeitssuchenden. Sobald das Bewerbungsverfahren abgeschlossen und U. die ausgeschriebene Stelle besetzt hat, muss U. die Bewerbungen der nicht zum Zug gekommenen Bewerber löschen (siehe aber Beispiel unten). Das Unternehmen U. dürfte Bewerbungen nur dann weiter speichern, wenn der/die Bewerber/in zuvor eingewilligt hat, dass seine/ihre Bewerbung für den Zweck der Berücksichtigung im Rahmen zukünftiger Job-Ausschreibungen vom Unternehmen gespeichert werden darf.*

Die Löschung ist nicht vorzunehmen, soweit die Verarbeitung der personenbezogenen Daten für die folgenden Fälle erforderlich ist:

a. zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
b. zur Erfüllung einer rechtlichen Verpflichtung, der die Verarbeitung unterliegt, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
c. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
d. für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, soweit das Recht auf Löschung voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
e. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

> *Beispiel:* *Das Unternehmen U. erhält im Rahmen einer Job-Ausschreibung Dutzende Bewerbungen von Arbeitssuchenden. Nachdem sich das Unternehmen im Rahmen eines Auswahlverfahrens für eine Bewerberin entschieden hat, beschwert sich der abgewiesene Bewerber X., dass er aufgrund seines Alters nicht ausgewählt worden sei und kündigt an, Schadenersatzansprüche geltend zu machen. Da das Unternehmen die Bewerbung des X. zur Verteidigung gegen die geltend gemachten Ansprüche des X. benötigt, darf es die Bewerbung des X. bis zum Abschluss des Gerichtsverfahrens über die Schadenersatzansprüche des X. weiterhin speichern.*

32. Wie mache ich mein Recht auf Löschung geltend?

Das Löschungsbegehren kann formlos gestellt werden. Bei elektronischen Datenverarbeitungen sollte die Möglichkeit bestehen, den Löschungsantrag elektronisch zu stellen. Das Löschungsersuchen sollte Angaben zum Antragsteller und zum Grund für die Löschung enthalten.
Das Löschungsersuchen muss grundsätzlich innerhalb eines Monats beantwortet werden. Die Frist kann im Einzelfall – aufgrund der Komplexität des Antrags oder der hohen Anzahl der Anträge – um weitere zwei Monate verlängert werden. Sollte der Verantwortliche nach Prüfung des Antrags zum Ergebnis kommen, dass keine Löschpflicht besteht, muss er die betroffene Person innerhalb eines Monats über die Gründe der Ablehnung zu informieren. Gleichzeitig ist der Betroffene darüber zu unterrichten, dass er eine Beschwerde bei einer Aufsichtsbehörde erheben kann (siehe Frage 49).
Die Löschung bedeutet die Vernichtung bzw. jede Art der Unkenntlichmachung der personenbezogenen Daten und ist grundsätzlich unverzüglich vorzunehmen. Kann die Löschung nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist zumindest die Verarbeitung der betreffenden personenbezogenen Daten bis zu diesem Zeitpunkt einzuschränken. Die Löschung ist auch dann vorzunehmen, wenn hiermit ein unverhältnismäßig hoher Aufwand verbunden ist.

33. Was bedeutet mein Recht auf „Vergessenwerden“?

Das Recht auf „Vergessenwerden“ ist mit dem Recht auf Löschung nicht ganz identisch. Das Recht auf „Vergessenwerden“ beruht im Grundsatz auf einem Urteil des Europäischen Gerichtshofs aus dem Jahr 2014 (EuGH C-131/12 Google Spain). Demnach kann eine betroffene Person von einem Suchmaschinenbetreiber unter bestimmten Umständen verlangen, dass bei Eingabe ihres Namens bestimmte Suchergebnisse/Links nicht mehr angezeigt werden. Wenn die betroffene Person die Löschung bestimmter Suchergebnisse verlangt, muss der Suchmaschinenbetreiber dieses Recht auf „Vergessenwerden“ mit dem Informationsinteresse der Allgemeinheit und seinen eigenen wirtschaftlichen Interessen abwägen und in Einklang bringen. Ob dem Betroffenen das Recht auf „Vergessenwerden“ tatsächlich zu kommt, muss immer im Einzelfall abgewogen werden.

> *Beispiel:* *Bei Eingabe des Namens des Arztes A. werden Suchergebnisse zu einem jahrzehntealten Online-Bericht über eine längst vergangene Jugendsünde von A. angezeigt. In diesem Fall wird das Interesse von A. an der Geheimhaltung gegenüber dem Informationsinteresse der Allgemeinheit überwiegen. A. kann vom Suchmaschinenbetreiber verlangen, dass die betreffenden Suchergebnisse nicht mehr angezeigt werden. Anderes könnte dann gelten, wenn es sich bei A. um eine Person des öffentlichen Interesses handelt, die sich rühmt, nie eine Jugendsünde begangen zu haben.*

Um dem Recht auf „Vergessenwerden“ mehr Geltung zu verschaffen, sieht die DS-GVO weiterführende Informationspflichten für den Verantwortlichen vor. So hat ein Verantwortlicher, der personenbezogenen Daten öffentlich gemacht und zu deren Löschung verpflichtet ist (zB der Betreiber einer Suchmaschine), unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen zu treffen, um Dritte, die die gegenständlichen personenbezogenen Daten verarbeiten (zB den Betreiber der Website, auf der die personenbezogenen Daten veröffentlicht wurden), darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien

oder Replikationen dieser personenbezogenen Daten verlangt hat.

> *Beispiel:* *im Zuge der Löschung der A. betreffenden Suchergebnisse hat der Suchmaschinenbetreiber nach Möglichkeit den Herausgeber des Online-Berichts bzw. den betreffenden Website-Betreiber darüber zu informieren, dass A. die Löschung der personenbezogenen Daten (und somit des Online-Berichts) verlangt hat.*

34. Kann ich von einem Suchmaschinenbetreiber die Löschung bestimmter Suchergebnisse zu meinem Namen verlangen?

Dies kommt immer auf den Einzelfall an und hängt von der Art der verarbeiteten und veröffentlichten Daten sowie dem Informationsinteresse der Allgemeinheit ab. Wenn die Suchergebnisse zu personenbezogenen Daten verlinken, die unwahr oder veraltet sind, wird der Betroffene in der Regel einen Anspruch auf Löschung der Suchergebnisse haben. Wenn die im Rahmen der Suchergebnisse angezeigten personenbezogenen Daten im Zusammenhang mit dem Berufsleben des Betroffenen stehen, kann das Informationsinteresse der Allgemeinheit das Interesse des Betroffenen an der Geheimhaltung dieser personenbezogenen Daten überwiegen. Es kommt letztlich immer auf eine Abwägung der Interessen im Einzelfall an.
Es ist zweckmäßig, primär den Betreiber der Webseiten zu kontaktieren, auf der personenbezogene Daten veröffentlicht werden, weil die personenbezogenen Daten nur auf diesem Wege aus dem Internet verschwinden können. Der Suchmaschinenbetreiber kann nämlich nur die Anzeige bestimmter Suchergebnisse blockieren, während die betreffenden Webseiten auch bei Entfernung der Suchergebnisse weiterhin für jedermann abrufbar bleiben. Es ist aber nicht notwendig, den Betreiber der Website zu kontaktieren, bevor man mich sich an den Suchmaschinenbetreiber wendet.

35. Was bedeutet mein Recht auf Einschränkung der Verarbeitung?

Unter gewissen Voraussetzungen kann die betroffene Person vom Verantwortlichen verlangen, dass dieser personenbezogene Daten der betroffenen Person nur mehr eingeschränkt verarbeitet. Die Daten dürfen dann – von ihrer Speicherung abgesehen – nur mehr mit Einwilligung der betroffenen Person oder zur Geltendmachung von Rechtsansprüchen, zum Schutz der Rechte einer anderen Person oder aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden.
Die betroffene Person kann eine Einschränkung der Verarbeitung der personenbezogenen Daten zum Beispiel dann verlangen, wenn sie die Richtigkeit der personenbezogenen Daten bestreitet oder einen Widerspruch gegen die Datenverarbeitung erhoben hat. Die Datenverarbeitung ist dann so lange einzuschränken, bis der Verantwortlich die die Richtigkeit der personenbezogenen Daten bzw. die Zulässigkeit der Datenverarbeitung überprüfen konnte.

> *Beispiel:* *Die betroffene Person P. bestreitet die Richtigkeit von auf der Website des Verantwortlichen veröffentlichten personenbezogenen Daten. In diesem Fall muss der Verantwortliche die personenbezogenen Daten von P. vorübergehend von Website entfernen, bis die Richtigkeit der Daten geklärt ist.*

36. Was bedeutet mein Recht auf Datenübertragbarkeit?

Das Recht auf Datenübertragbarkeit soll es dem Betroffenen ermöglichen, ihn betreffende personenbezogenen Daten von einem Verantwortlichen zu einem anderen Verantwortlichen zu übertragen bzw. von einer IT-Umgebung zu einer anderen zu transferieren. Davon sind aber nur personenbezogene Daten betroffen, nicht etwa die bei Cloud- oder Streaming-Diensten lagernden, nicht vom Betroffenen zur Verfügung gestellten Dateien. Ziel der Regelung ist es, dem Betroffenen die Kontrolle über „seine" personenbezogenen Daten zurückzugeben. Es soll dem „Lock-in-Effekt", wonach Unternehmer Kunden mit schwierigen Wechselmodalitäten an sich zu binden versuchen, entgegenwirken.
Die betroffene Person hat ein Recht darauf, dass der Verantwortliche dem Betroffenen jene personenbezogenen Daten, die vom Betroffenen bereitgestellt wurden und vom Verantwortlichen aufgrund einer Einwilligung oder eines Vertragsverhältnisses verarbeitet werden, zur Verfügung stellt. Der Verantwortliche muss die Daten in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zur Verfügung stellen, damit die Daten von einem anderen Verantwortlichen problemlos (weiter-)verarbeitet werden können. Darüber hinaus kann die betroffene Person sogar verlangen, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist. Hierzu sollen Anbieter gemeinsam interoperable Formate entwickeln, die die Datenübertragbarkeit ermöglichen.
Für das Recht auf Datenübertragbarkeit gilt auch eine Frist von einem Monat, die in begründeten Fällen auf drei Monate verlängert werden kann.

> *Beispiel:* *Der Nutzer N. möchte seine Liste von Kontakten vom E-Mail-Anbieter G. zum E-Mail-Anbieter O. übertragen oder die beim Musik-Streaming-Dienst T. gespeicherten Profildaten (Vorlieben, Playlists etc.) exportieren und beim Musik-Streaming-Dienst S. importieren.*

37. Was bedeutet mein Recht auf Widerspruch?

Das Widerspruchsrecht räumt dem Betroffenen bei Vorliegen bestimmter Voraussetzungen das Recht ein, eine rechtmäßige und auf gesetzlicher Grundlage erfolgende Verarbeitung ihn betreffender personenbezogener Daten zu unterbinden. Sofern eine Datenverarbeitung überhaupt unrechtmäßig erfolgt, dürfte die Datenverarbeitung gar nicht stattfinden und hat der Betroffene ohnehin einen Anspruch auf Löschung der personenbezogenen Daten. Der Widerspruch ist nicht zu verwechseln mit dem Widerruf einer vom Betroffenen erteilten Einwilligung.
Die betroffene Person hat ein allgemeines Widerspruchsrecht, wenn eine Datenverarbeitung auf der Rechtsgrundlage eines öffentlichen Interesses oder eines berechtigten Interesse des Verantwortlichen oder eines Dritten erfolgt und damit grundsätzlich rechtmäßig wäre, doch die besondere Situation des Betroffenen die konkrete Datenverarbeitung ausnahmsweise unzulässig macht. Ob eine besondere Situation vorliegt, ist im Einzelfall zu prüfen und kann in einer veränderten Situation des Betroffenen oder einer sich nachträglich verändernden Eingriffsqualität des Eingriffs in die Rechte der betroffenen Person begründet liegen. Die von einem berechtigten Widerspruch erfassten Daten sind sodann zu löschen.

> *Beispiel:* *Die Online-Zeitung Z. veröffentlicht einen Artikel, in dem über die Insolvenz des Unternehmer U. berichtet wird. Die Verarbeitung der personenbezogenen Daten durch die Online-Zeitung Z. ist rechtmäßig, weil ein erhebliches Informationsinteresse der Allgemeinheit besteht und das Geheimhaltungsinteresse von U. nicht überwiegt. Der Unternehmer U. hat kein*

Recht dieser Datenverarbeitung zu widersprechen. Viele Jahre später erhebt der Unternehmer U. Widerspruch gegen die Datenverarbeitung. Die Online-Zeitung Z. wird die weitere Datenverarbeitung (d.h. die Abrufbarkeit des Artikels) unterlassen müssen, weil sich die Situation von U. mittlerweile geändert hat und die Datenverarbeitung das berufliche Fortkommen des Unternehmers U. mittlerweile unverhältnismäßig erschwert.

Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen. In diesem Fall findet keine Interessenabwägung statt. Der Betroffene muss spätestens zum Zeitpunkt der ersten Kommunikation auf das Widerspruchsrecht hingewiesen werden.

Beispiel: *Das Sportwarengeschäft S. erhält im Rahmen eines Verkaufs eines Sportartikels die Kontaktdaten des Kunden K. und schickt K. in weiterer Folge einen Brief, in dem der baldige Sommerschlussverkauf bei S. beworben wird. Die Datenverarbeitung durch das Sportwarengeschäft S. ist grundsätzlich rechtmäßig, weil das Sportwarengeschäft S. ein berechtigtes Interesse an der Direktwerbung hat. Der Kunde kann der Datenverarbeitung aber sofort widersprechen, worauf S. die zu Werbezwecken durchgeführte Datenverarbeitung sofort zu beenden und die personenbezogenen Daten von K zu löschen hat, soweit die Speicherung nicht aufgrund eines anderen Erlaubnistatbestands (zB zur Abwehr von Gewährleistungsansprüchen von K.) zulässig ist.*

38. Worüber muss ich vor einer Datenverarbeitung informiert werden?

Wenn personenbezogene Daten bei der betroffenen Person erhoben werden bzw. wenn eine Person personenbezogene Daten zur Verfügung stellt, muss der Verantwortliche die betroffene Person über Folgendes informieren:

a. den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b. gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d. gegebenenfalls die berechtigten Interessen des Verantwortlichen oder eines Dritten an der Datenverarbeitung;
e. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f. gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie gegebenenfalls einen Hinweis auf das nicht angemessene Datenschutzniveau in diesem Drittland.
g. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
h. das Bestehen eines Rechts auf Auskunft sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
i. wenn die Verarbeitung auf einer Einwilligungserklärung beruht, das Bestehen eines Widerrufsrechts;
j. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

k. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
l. das Bestehen einer automatisierten Entscheidungsfindung einschließlich „Profiling“ und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
m. wenn der Verantwortliche die Weiterverarbeitung die personenbezogenen Daten für einen anderen Zweck beabsichtigt, vor der Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen.

Die Informationen müssen erteilt werden, bevor die Daten tatsächlich erhoben werden. In welcher Form diese Informationen erteilt werden müssen, ist nicht speziell geregelt. Eine wohl zulässige Variante wäre, die essentiellen Informationen unmittelbar anzugeben und bezüglich der übrigen Informationen auf einen Link zu einer ausführlicheren Information zu verweisen. Die Informationen sollten jedenfalls vollständig, verständlich und leicht zugänglich sein und in einer klaren und einfachen Sprache gehalten sein.
Wenn personenbezogene Daten nicht beim Betroffenen selbst, sondern bei einem Dritten erhoben worden sind, teilt der Verantwortliche dem Betroffenen zusätzlich mit, welche Kategorien von Daten verarbeitet werden und aus welcher Quelle die personenbezogenen Daten stammen; dies spätestens innerhalb eines Monats nach Erlangung der personenbezogenen Daten bzw. spätestens mit der ersten Mitteilung an den Betroffenen bzw. der ersten Offenlegung der Daten an einen anderen Empfänger.

> *Beispiel:* *Der Student S. beantragt bei der Bank B. einen Kredit, um ein Auto kaufen zu können. Die Bank B. muss den Studenten S. darüber informieren, wenn die Entscheidung über die Kreditgewährung auf einer automatisierten Entscheidung aufgrund einer automatisierten Datenverarbeitung erfolgt („Scoring“) und aussagekräftige Informationen über die involvierte Logik geben.*

39. Was ist eine Datenschutzerklärung?

Eine Datenschutzerklärung stellt üblicherweise eine Information des Verantwortlichen gegenüber den Betroffenen (Kunden, Website-Besucher etc.) über die vorgenommenen Datenverarbeitungen dar. Eine Datenschutzerklärung ist nicht mit einer datenschutzrechtlichen Einwilligungserklärung zu verwechseln. Mit einer Datenschutzerklärung kommt ein Verantwortlicher gegenüber Betroffenen seinen datenschutzrechtlichen Informationspflichten nach. Dagegen wird eine datenschutzrechtliche Einwilligungserklärung von einem Betroffenen erteilt wird und stellt eine Rechtsgrundlage für eine Datenverarbeitung dar.
Manchmal wird eine datenschutzrechtliche Einwilligungserklärung vom Verantwortlichen in die allgemeine Datenschutzerklärung verpackt, die dem Betroffenen in der Gesamtheit dann zur Zustimmung vorgelegt wird. Dies ist grundsätzlich nicht der richtige Weg. Die datenschutzrechtliche Einwilligungserklärung sollte klar, verständlich und von sonstigen Informationen zu unterscheiden sein, weil sonst Zweifel an deren Wirksamkeit bestehen können.

> *Beispiel:* *Der Nutzer N. besucht die Website W. Er fragt sich, ob der Betreiber der Website W. personenbezogene Daten von N. verarbeitet. Wenn dies der Fall ist, sollte sich auf der Homepage der Website zumindest ein Link („Datenschutzerklärung“,*

„Datenschutzbestimmungen“, „Privacy Policy“ oÄ) finden, unter dem man zu den Informationen des Verantwortlichen über die Verarbeitung personenbezogener Daten der Website-Besucher gelangt.

40. Was versteht man unter „Profiling“?

„Profiling“ ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte zu bewerten (zB um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen).
„Profiling“ stellt mit anderen Worten zum Beispiel die automatisierte Erstellung eines bestimmten Käuferprofils aufgrund des bisherigen Kaufverhaltens einer Person oder die automatisierte Erstellung eines bestimmten Nutzerprofils aufgrund des bisherigen Internet-Surfverhaltens eines Nutzers dar. Aber auch die automatisierte Datenverarbeitung zur Erhebung und Darstellung der Kreditwürdigkeit einer Person stellt eine Art des „Profiling“ dar.

Beispiel: Die Hausfrau H. bestellt wöchentlich neue Kleidung bei einem Online-Shop. Der Online-Händler wertet das Verhalten von H. automatisch aus (zB Welche Farben bevorzugt H.? Wie schnell bezahlt H. die Rechnungen?) und erstellt ein Profil von H., um ihr vergleichbare Waren anbieten zu können und mehr über die Kreditwürdigkeit von H. herauszufinden.

41. Welche Rechte habe ich bei automatisierten Entscheidungen aufgrund von „Profiling“?

Eine Person darf nur unter bestimmten Umständen einer ausschließlich automatisierten Entscheidung, die auf einer automatisierten Datenverarbeitung (zB „Profiling“) basiert und rechtliche Wirkungen gegenüber dem Betroffenen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, unterworfen werden. Die betroffene Person hat das Recht, nicht einer solchen Entscheidung unterworfen zu werden, es sei denn die Entscheidung ist

a. für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich,
b. aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten zulässig oder
c. erfolgt mit ausdrücklicher Einwilligung der betroffenen Person.

In den Fällen a. und c. muss der Betroffene aber zumindest das Recht darauf haben, dass eine Person seitens des Verantwortlichen die automatisierte Verarbeitung überprüft. Auch muss der Betroffene in diesen Fällen seinen eigenen Standpunkt darlegen können und die Entscheidung des Verantwortlichen anfechten können.

Beispiel: Der Student S. bewirbt sich über eine Online-Maske bei dem Unternehmen U.. Unmittelbar nach Abschicken seiner Bewerbung über die Online-Maske erhält S. bereits ein Absageschreiben des Unternehmens U. per E-Mail. Die Absage des Unternehmens U. beruht offensichtlich auf einer automatisierten Datenverarbeitung (nämlich einer automatisierten Verarbeitung der Bewerbungsdaten von S.) und stellt eine automatisierte Entscheidung dar, die S.

erheblich beeinträchtigt. Eine solche automatisierte Entscheidung des Unternehmens U. wäre nur dann zulässig gewesen, wenn S. ausdrücklich darin eingewilligt hätte und S. die Möglichkeit gehabt hätte, die Entscheidung durch den Verantwortlichen überprüfen zu lassen und allenfalls anzufechten.

42. Was bedeutet Datenschutz durch Technikgestaltung („*Privacy by design*“)?

„Datenschutz durch Technikgestaltung“ („*Privacy by Design*“) bedeutet, dass ein Verantwortlicher bereits vor der eigentlichen Datenverarbeitung geeignete technische und organisatorische Maßnahmen treffen soll, um Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen. Verantwortliche sollen das Thema Datenschutz also beispielsweise bereits bei der Entwicklung neuer Technologien berücksichtigen und datenschutzkonforme Lösungen anbieten. Die Entwicklung neuer Software-Programme oder neue Geräte sollen also in eine datenschutzfreundliche Richtung gehen; neue Software-Programme und Geräte sollen nicht darauf ausgelegt sein, möglich viele Daten von möglichst vielen Personen zu erheben. Der Datenschutz soll also bereits auf der Technik-Ebene Einzug halten.

Beispiel: *Viele Online-Dienste erfassen und speichern IP-Adressen ihrer Nutzer, obwohl dies vielfach gar nicht zwingend notwendig ist. Ein „Privacy-by-design“-Ansatz wäre hier, auf die Speicherung und Weitergabe der IP-Adressen der Nutzer zu verzichten und anstelle dessen die IP-Adressen der Nutzer nur in verkürzter Form zu erheben und zu verarbeiten.*

43. Was bedeutet Datenschutz durch datenschutzfreundliche Voreinstellungen („*Privacy by default*“)?

Datenschutz durch datenschutzfreundliche Voreinstellungen („*Privacy by default*“) bedeutet, dass bereits durch Voreinstellungen grundsätzlich sichergestellt wird, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Ein Verantwortlicher hat also dafür zu sorgen, dass zum Bespiel seine Programme, seine App o.Ä nicht so voreingestellt ist, dass möglichst viele Daten im größtmöglichen Umfang verarbeitet werden. Die Maßnahmen des Verantwortlichen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Beispiel: *Der Anbieter eines sozialen Netzwerks oder eines Browsers hätte nach dem Grundsatz „Privacy by default“ sicherzustellen, dass die Voreinstellungen der App oder des Browsers datenschutzfreundlich eingestellt sind. Der Nutzer sollte die Einstellungen also nicht erst von „öffentlich“ auf „privat“ ändern müssen, sondern die App bzw. der Browser sollten so eingestellt sein, dass personenbezogene Daten von Haus aus nicht veröffentlicht werden. Wenn der Nutzer die Daten veröffentlichen will, müsste er dies in den Einstellungen erst ändern.*

44. Wer muss ein Verzeichnis von Datenverarbeitungen führen?

Praktisch jede Person, die personenbezogene Daten nicht nur bei der Ausübung rein persönlicher und familiärer Tätigkeiten und nicht nur gelegentlich verarbeitet, hat ein Verzeichnis von Datenverarbeitungen zu erstellen und auf dem Laufenden zu halten. Die Verpflichtung zur Führung eines Verarbeitungsverzeichnisses ersetzt die frühere Verpflichtung zur Meldung von Datenanwendungen an die Datenschutzbehörde zum Zweck der Registrierung im Datenverarbeitungsregister (DVR). Mit In-Geltung-Treten der DSGVO wurde das Datenverarbeitungsregister abgeschafft.
Das Verzeichnis von Datenverarbeitungen hat folgende Angaben zu jeder Datenverarbeitung zu enthalten:

a. den Namen und die Kontaktdaten des/der Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
b. die Zwecke der Verarbeitung;
c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
d. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
e. gegebenenfalls Angaben zur Übermittlung von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation;
f. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
g. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, die zur Gewährleistung eines angemessenen Datenschutzniveaus ergriffen werden.

Es besteht keine Verpflichtung, das Verarbeitungsverzeichnis zu veröffentlichen. Es ist allerdings der Datenschutzbehörde auf Anfrage zur Verfügung zu stellen. Ein Verstoß gegen diese Verpflichtung kann mit Strafen geahndet werden. Auch der Auftragsverarbeiter hat ein vereinfachtes Verarbeitungsverzeichnis zu erstellen und zu führen.
Die Erstellung eines Verarbeitungsverzeichnisses kann mit einer Inventur der durchgeführten Datenverarbeitungen verglichen werden. Es hat den Zweck, sich selbst und anderen einen Überblick über die durchgeführten Datenverarbeitungen zu verschaffen. Das Verarbeitungsverzeichnis kann auch als eine gute Grundlage dienen, um etwa Auskunfts- oder Löschungsersuchen fristgerecht beantworten zu können.

> *Beispiel:* *Der Schuster S. verarbeitet im Rahmen seines Geschäftsbetriebs personenbezogene Daten nur zum Zweck der Verrechnung seiner Leistungen an den Kunden (es gibt keine Newsletter-Versand oÄ). Wenn er die personenbezogenen Daten nicht nur gelegentlich verarbeitet, muss er ein Verarbeitungsverzeichnis erstellen. Dieses hat neben Angaben über sich selbst („Ernst Schuster, e.U., Postgasse 1, 1234 Stadt, Telefonnummer: 01234 56789, E-Mail-Adresse: ernst@schuster.at“) insbesondere Angaben zum Zweck der Datenverarbeitung (zB „Rechnungswesen“), zu den Kategorien betroffener Personen (zB „Kunden“), den Kategorien personenbezogener Daten (zB „Name, Adresse, Rechnungsnummer, Zahlungsmittel, Vermerk über Zahlungseingang“), den Kategorien von Empfängern („Buchhaltung, Finanzbehörden“) und den Fristen für die Löschung der verschiedenen Datenkategorien („nach Ende der gesetzlichen Aufbewahrungsfrist von 7 Jahren gemäß § 132 Abs 1 BAO bzw. §§ 190, 212 UGB bzw. § 18 Abs 2 3. UAbs UStG“). Darüber hinaus sollte das Verarbeitungsverzeichnis eine Beschreibung der technischen und organisatorischen Maßnahmen, die zur Gewährleistung eines angemessenen Datenschutzniveaus ergriffen werden, enthalten („Kundenkartei wird in einem*

verschließbarem Schrank aufbewahrt; nur Ernst Schuster verfügt über einen Schlüssel etc.“).

45. Was ist eine Datenschutz-Folgenabschätzung?

Eine Datenschutz-Folgeabschätzung ist eine Maßnahme, die ein Verantwortlicher vor der Durchführung risikogeneigter Datenverarbeitungen durchführen muss. Wenn eine Datenverarbeitung ein hohes Risiko für betroffene Personen darstellt (zB bei der Verwendung neuer Technologien, bei einer umfangreichen Verarbeitung sensibler Daten etc.), muss der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Datenschutz durchführen, die Risiken bewerten und zur Bewältigung der Risiken geplanten Abhilfemaßnahmen (Garantien, Sicherheitsvorkehrungen etc.) ergreifen und dokumentieren.
Die Datenschutzbehörde veröffentlicht eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist („Black-List“), sowie Liste der Arten von Verarbeitungsvorgängen, für die keine Datenschutz-Folgenabschätzung erforderlich ist („White-List“).

46. Wer muss einen Datenschutzbeauftragten bestellen?

Es besteht keine generelle Verpflichtung zur Bestellung eines Datenschutzbeauftragten. Ein Datenschutzbeauftragter muss nur in den folgenden Fällen vom Verantwortlichen/Auftragsverarbeiter bestellt werden:
a) die Verarbeitung wird von einer öffentlichen Stelle (außer: Gerichten) durchgeführt wird;
b) die Kerntätigkeit besteht in der Durchführung von Verarbeitungsvorgängen, welche eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen;
c) die Kerntätigkeit besteht in der umfangreichen Verarbeitung sensibler Daten.
Der Datenschutzbeauftragte hat primär eine beratende Funktion. Er berät den Verantwortlichen und alle Beschäftigte hinsichtlich der datenschutzrechtlichen Pflichten und achtet auf die Einhaltung der datenschutzrechtlichen Vorschriften. Er ist er vom Verantwortlichen frühzeitig in alle mit dem Datenschutz zusammenhängenden Fragen einzubinden und dient auch als Verbindungsstelle zur Datenschutzbehörde. Die Kontaktdaten des Datenschutzbeauftragten müssen öffentlich gemacht werden.
Betroffene Personen können den Datenschutzbeauftragten zu allen Datenschutzfragen zu Rate ziehen. Er unterliegt bei der Erfüllung seiner Aufgaben als Datenschutzbeauftragter keinen Weisungen und darf deswegen auch nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte kann allerdings auch mit anderen Aufgaben und Pflichten betraut werden. Er berichtet unmittelbar der höchsten Managementebene und ist zur Geheimhaltung und Vertraulichkeit verpflichtet.

47. Welche Maßnahmen hat der Verantwortliche bei Datenschutzverletzungen zu ergreifen?

Im Falle einer Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche die Verletzung grundsätzlich binnen 72 Stunden der Datenschutzbehörde melden, es sei denn, dass die Datenschutzverletzung voraussichtlich kein hohes Risiko für die Betroffenen darstellt. Die Meldung muss auch eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung ihrer möglichen nachteiligen Auswirkungen beinhalten.
Wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Betroffenen darstellt, muss der Verantwortliche die betroffene Person unverzüglich von der Verletzung benachrichtigen. Die Benachrichtigung kann nur in bestimmten Fällen unterbleiben, zB wenn das Risiko nicht mehr besteht. Wenn die Benachrichtigung der Betroffenen mit einem unverhältnismäßigen Aufwand verbunden wäre, hat stattdessen

eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zur Information des Betroffenen zu erfolgen.

Beispiel: *Im Rahmen eines Hacker-Angriffs auf das Unternehmens V. erhalten Hacker Zugriff auf die personenbezogenen Daten (inkl. Kreditkartendaten) von Zehntausenden Kunden des Unternehmens V.. Das Unternehmen V. muss die betroffenen Kunden unverzüglich verständigen und die Datenschutzverletzung binnen 72 Stunden der Datenschutzbehörde melden sowie die Maßnahmen beschreiben, die das Unternehmen V. ergreift, um die Folgen dieser Datenschutzverletzung gering zu halten.*

48. An wen kann ich mich bei Verletzung meiner Rechte wenden?

Im Fall einer Verletzung ihrer Rechte kann sich eine betroffene Person direkt an die österreichische Datenschutzbehörde wenden und dort eine Beschwerde einreichen. Die Datenschutzbehörde muss den Gegenstand der Beschwerde untersuchen und den Beschwerdeführer innerhalb von drei Monaten ab Einbringung der Beschwerde über den Stand und das Ergebnis der Ermittlungen informieren (siehe Frage 50). Das Beschwerdeverfahren vor der Datenschutzbehörde ist kostenlos.
Jede betroffene Person hat unbeschadet des Rechts auf Beschwerde bei der Datenschutzbehörde das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass ihre Rechte infolge einer unrechtmäßigen Datenverarbeitung verletzt wurden. Der Kläger hat die Wahl, ob er die Klage bei dem Landesgericht einbringt, wo er seinen gewöhnlichen Aufenthalt oder Sitz hat oder beim gewöhnlichen Aufenthalt oder Sitz/Niederlassung des Beklagten. Eine Klage ist allerdings mit Kosten verbunden und muss durch einen Rechtsanwalt eingebracht werden.
Die betroffene Person kann sich gegebenenfalls auch bestimmte qualifizierte Einrichtungen ohne Gewinnerzielungsabsicht wenden und diese beauftragen, ihre Rechte für die betroffene Person wahrzunehmen. Die qualifizierte Einrichtung hat das Recht, im Namen der betroffenen Person eine Beschwerde bei der Datenschutzbehörde einzureichen oder eventuell auch das Recht auf Schadenersatz im Namen der betroffenen Person geltend zu machen.

Beispiel: *Im Rahmen eines Hacker-Angriffs auf das Unternehmen V. erhalten Hacker Zugriff auf die personenbezogenen Daten (inkl. Kreditkartendaten) des Kunden P. Der Kunde P. begehrt darauf Auskunft von V. darüber, welche seiner Daten von V. verarbeitet wurden, um das Ausmaß des eingetretenen Schadens abschätzen zu können. Das Unternehmen V. erteilt dem Kunden P. keine Auskunft. P. kann dagegen Beschwerde bei der Datenschutzbehörde erheben. Parallel dazu kann P. auch eine Klage auf Schadenersatz bei Gericht einbringen, wenn ihm aus dem Hacker-Angriff ein Schaden erwachsen sein sollte.*

49. Wie muss eine Beschwerde an die Datenschutzbehörde aussehen?

Eine Beschwerde an die Datenschutzbehörde hat die folgenden Angaben zu enthalten:

a. die Bezeichnung des als verletzt erachteten Rechts,
b. soweit dies zumutbar ist, die Bezeichnung des Beschwerdegegners,
c. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,

d. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
e. das Begehren, die behauptete Rechtsverletzung festzustellen und
f. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

Gegebenenfalls sind auch der zu Grunde liegende Antrag der betroffenen Person (Antrag auf Auskunft, Antrag auf Löschung etc.) und eine allfällige Antwort des Beschwerdegegners der Beschwerde beizulegen. Die Beschwerde muss spätestens innerhalb eines Jahres, nachdem die betroffene Person Kenntnis von der Datenschutzverletzung erlangt hat, und spätestens innerhalb von drei Jahren ab der Datenschutzverletzung eingebracht werden.

50. Was tut die Datenschutzbehörde nach dem Einlangen meiner Beschwerde?

Die Datenschutzbehörde hat nach dem Einlangen einer Beschwerde die behauptete Datenschutzverletzung zu untersuchen. Die Datenschutzbehörde kann vom Verantwortlichen oder vom Auftragsverarbeiter alle notwendigen Aufklärungen verlangen und Einsicht in Datenverarbeitungen und diesbezügliche Unterlagen nehmen. Sie darf nach entsprechender Verständigung sogar die (Geschäfts-) Räumlichkeiten des Verantwortlichen oder Auftragsverarbeiters betreten, Datenverarbeitungsanlagen (Computer etc.) in Betrieb nehmen, Kopien von Datenträgern herstellen usw.
Wenn sich die Beschwerde der betroffenen Person als berechtigt erweist, kann die Datenschutzbehörde Abhilfemaßnahmen ergreifen, um die Datenschutzverletzung zu unterbinden, zB den Verantwortlichen anweisen, die Verarbeitungsvorgänge innerhalb eines bestimmten Zeitraums in Einklang mit dem Datenschutzrecht zu bringen, ein Verbot der Datenverarbeitung zu verhängen etc. Die Datenschutzbehörde kann auch zusätzlich zu diesen Maßnahmen, je nach den Umständen des Einzelfalls, auch eine Geldbuße verhängen.

51. Wie hoch können die von der Datenschutzbehörde Geldbußen sein?

Die Datenschutzbehörde kann zusätzlich zu den sonstigen Abhilfemaßnahmen auch Geldbußen verhängen. Die Geldbußen sollten in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Das bedeutet, dass die Geldbuße für die rechtswidrig handelnde Person jedenfalls spürbar sein, aber auch in einem angemessenen Verhältnis zur begangenen Datenschutzrechtsverletzung stehen sollte. Dabei sind Elemente wie zB die Art, Schwere und Dauer des Verstoßes, das Ausmaß des Verschuldens und allenfalls getroffene Maßnahmen zur Minderung des entstandenen Schadens zu berücksichtigen.
Im Fall bestimmter Rechtsverstöße (zB bei Verstößen gegen die Bedingungen für die Einwilligung oder bei der Verletzung des Rechts auf Auskunft oder des Rechts auf Löschung) kann die Datenschutzbehörde Geldbußen von bis zu EUR 20.000.000 oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes verhängen.

52. Kann ich bei der österreichischen Datenschutzbehörde auch eine Beschwerde gegen einen Verantwortlichen oder Auftragsverarbeiter mit Sitz im Ausland erheben?

Ja, eine betroffene Person kann bei der österreichischen Datenschutzbehörde auch eine Beschwerde gegen einen Verantwortlichen oder Auftragsverarbeiter mit Sitz im Ausland erheben.
Wenn der Verantwortliche oder Auftragsverarbeiter seine Hauptniederlassung oder seine einzige Niederlassung (eine Niederlassung ist jede feste Einrichtung, die der Geschäftstätigkeit zu dienen bestimmt ist)

in einem anderen EU-Mitgliedstaat hat, muss die österreichische Datenschutzbehörde die Aufsichtsbehörde in dem betreffenden EU-Mitgliedstaat mit dem Fall befassen. Diese Aufsichtsbehörde fungiert dann als federführende Aufsichtsbehörde bei den Untersuchungen der Datenschutzverletzung. Die Aufsichtsbehörden tauschen untereinander alle zweckdienlichen Informationen aus. Die federführende Aufsichtsbehörde bindet andere betroffene Aufsichtsbehörden (zB die Aufsichtsbehörde, bei der die Beschwerde erhoben wurde oder die Aufsichtsbehörde einer anderen Niederlassung) in den Entscheidungsprozess mit ein und erlässt gegebenenfalls letztendlich die erforderlichen Anordnungen gegenüber dem Verantwortlichen.
Wenn der Verantwortliche keine einzige Niederlassung innerhalb der EU unterhält, sind die Aufsichtsbehörden aller EU-Mitgliedstaaten parallel zuständig. Die Datenschutzbehörden sind in diesem Fall aber jedenfalls auf die Kooperation mit den Behörden des Heimatstaates des Verantwortlichen angewiesen.

Beispiel: *Der österreichische Schüler E. erhebt vor der österreichischen Datenschutzbehörde eine Beschwerde gegen den Betreiber eines sozialen Netzwerks F. mit Hauptniederlassung in Irland. Die österreichische Datenschutzbehörde befasst die irische Aufsichtsbehörde, die den Gegenstand der Beschwerde in weiterer Folge untersucht. Wenn sich die Beschwerde des E. als berechtigt erweist, trägt die irische Aufsichtsbehörde nach Rücksprache mit der österreichischen Datenschutzbehörde dem Betreiber des sozialen Netzwerks F. Maßnahmen auf oder erlässt Sanktionen gegen ihn. Wenn sich die Beschwerde als nicht berechtigt erweisen sollte, erlässt die österreichische Datenschutzbehörde einen Bescheid, mit dem die Beschwerde des E. abgewiesen wird.*

53. Was kann ich tun, wenn die Datenschutzbehörde meine Beschwerde nicht behandelt oder die meine Beschwerde abgewiesen wird?

Die Datenschutzbehörde hat den betroffenen Beschwerdeführer innerhalb von drei Monaten ab Einbringung der Beschwerde über den Stand und das Ergebnis der Ermittlungen zu unterrichten. Wenn die Datenschutzbehörde die Beschwerde gar nicht behandelt und den Beschwerdeführer nicht binnen drei Monaten über den Stand und das Ergebnis der Ermittlungen informiert, kann der betroffene Beschwerdeführer eine Beschwerde an das Bundesverwaltungsgericht erheben.
Ebenso kann eine betroffene Person, deren Beschwerde von der Datenschutzbehörde abgelehnt oder abgewiesen wurde, Beschwerde an das Bundesverwaltungsgericht erheben. Eine solche Beschwerde ist in der Regel binnen 4 Wochen ab Zustellung des Bescheids der Datenschutzbehörde zu erheben.

54. Kann ich im Fall einer Datenschutzverletzung auch Schadenersatz geltend machen?

Jede Person, der wegen einer Datenschutzverletzung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
Ein solcher materiellen oder immateriellen Schaden kann im Verlust der Kontrolle über seine eigenen personenbezogenen Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanziellen Verlusten, unbefugter Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen für die betroffene natürliche Person bestehen. In welchen Fällen ein solcher Schadenersatz von den Gerichten tatsächlich zugesprochen wird und wie hoch dieser Schadenersatz sein kann, wird die zukünftige Rechtsprechung zeigen.

Der Kläger hat die Wahl, ob er die Klage bei dem Landesgericht einbringt, wo er seinen gewöhnlichen Aufenthalt oder Sitz hat oder beim gewöhnlichen Aufenthalt oder Sitz/Niederlassung des Beklagten. Eine Klage ist allerdings mit Kosten verbunden und muss durch einen Rechtsanwalt eingebracht werden.