III. LEITFADEN BETROFFENENRECHTE

Inhaltsverzeichnis

1. RECHTE DER BETROFFENEN PERSON

1.1. Allgemeine Grundsätze/Prinzipien

Um die Informationen und Mitteilungen im Zusammenhang mit den Betroffenenrechten ordnungsgemäß abzuwickeln und sicherzustellen, sind diese in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Diese Mitteilungen erfolgen grundsätzlich in elektronischer Form, sofern dies für den Betroffenen möglich und sinnvoll ist, ansonsten in einer anderen geeigneten Art und Weise. Dem Betroffenen steht dabei auch das Recht zu, die Informationen mündlich einzufordern. Werden die Betroffenenrechte in elektronischer Form eingefordert, wird dies in der Regel auch in elektronsicher Form bearbeitet.

In jedem Fall muss durch Vorlage eines **Identitätsnachweises** (insb amtlicher Lichtbildausweis) sichergestellt werden, ob die Rechte auch von der dazu berechtigten Person ausgeübt werden, es sei denn die Identität des Betroffenen ist amtsbekannt; an die Identitätsüberprüfung sind dabei strenge Maßstäbe zu setzen. Ist daher eine einwandfreie Identitätsfeststellung nicht möglich, werden dem Betroffenen/Anfragenden keine Daten und Auskünfte herausgegeben/erteilt; der Anfragende ist vielmehr aufzufordern geeignete Identitätsnachweise vorzulegen.

Die Geltendmachung und Abwicklung eines Betroffenenrechts wird **dokumentiert**, insb mit Blick darauf,

- welches Recht wann geltend gemacht wird,
- welche Daten wann herausgegeben werden und
- wie die Identitätsüberprüfung erfolgt ist bzw ob eine Identitätsfeststellung nicht möglich war und warum.

Zudem ist eine allfällige Fristverlängerung zu dokumentieren. Diese Dokumentation wird für die Dauer von 3 Jahren in geeigneter Weise, sicher und vor Zugriff von unberechtigten Dritten geschützt, aufbewahrt.

Den **Betroffenenrechten wird unverzüglich**, längstens jedoch binnen eines Monats, nachgekommen; in besonderen Fällen (insb Komplexität und/oder Anzahl von Betroffenenrechten) kann diese Frist um zwei Monaten verlängert werden. In diesem Fall wird der Betroffene rechtzeitig vor Ablauf der Monatsfrist in geeigneter Weise über die Fristverlängerung informiert.

Wird der Geltendmachung der Betroffenenrechte nicht oder nicht vollständig nachgekommen, wird der Betroffene darüber informiert, dass er dagegen bei der Datenschutzbehörde in Wien eine diesbezügliche Beschwerde einlegen oder gerichtliche Schritte ergreifen kann.

Den berechtigter Weise geltend gemachten **Betroffenenrechten wird unentgeltlich** nachgekommen; dies gilt nicht bei exzessiven oder offenkundig unbegründeten Anträgen. In diesen Fällen kann entweder dem Antrag nachgekommen, dafür aber die tatsächlich entstandenen Kosten vorgeschrieben werden, oder die Erfüllung des Antrags abgelehnt werden.

Grundsätzlich haben die **Informationen** im Rahmen der Betroffenenrechte **schriftlich oder in anderer Form bspw elektronisch zu erfolgen**. Auf ausdrückliches Verlangen der betroffenen Person kann eine Information auch mündlich erfolgen.
Unzulässig ist es die betroffenen Rechte für die Betroffenen zu beschränken, indem bspw nur **bestimmte Kommunikationskanäle für das Auskunftsrecht** vorgegeben werden.
Eine Auskunft Erteilung per Email ist zulässig, wenn die Vertraulichkeit der übermittelten Daten sichergestellt ist, dies gilt insb bei besonderen Kategorien von personenbezogene Daten nach Art 9 DSGVO (zB Bürgerpostfach, e-Brief).

Begehrt der Betroffene das Recht auf Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung, so informiert der Verantwortliche alle Empfänger, denen die personenbezogenen Daten offengelegt wurden, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn der Betroffene dies verlangt.

Zur Sicherstellung und in Ausnahmefällen können die unten angeführten Betroffenenrechte beschränkt werden, insb wenn es um

- die nationale Sicherheit,
- die Landesverteidigung,
- die öffentliche Sicherheit,
- die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit,
- den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit,
- den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren,
- die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe,
- Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die hier genannten Zwecke verbunden sind,
- den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen oder
- die Durchsetzung zivilrechtlicher Ansprüche sicher zu stellen,

geht.

Ganz generell gilt allerdings, dass auch die betroffene Person bei der Ausübung ihrer Betroffenenrechte in angemessener Weise und im zumutbaren Umfang mitzuwirken hat („Mitwirkungspflicht“).

2. BETROFFENENRECHTE IM EINZELNEN UND KONKRETER PROZESS

2.1. Informationspflicht zu personenbezogenen Daten, Art 13f DSGVO

Im Unterschied zum Auskunftsrecht, dem auf Anfrage des Betroffenen zu entsprechen ist, hat der Verantwortliche von sich aus dem Betroffenen bestimmte Informationen zukommen zu lassen, es sei denn

- der Betroffene verfügt bereits über diese oder
- wenn die Speicherung oder Offenlegung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist oder
- wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist, insb bei der Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

Die Informationen sind den Betroffenen entweder im Einzelfall zugänglich zu machen, oder aber in Form einer allgemeinen „Datenschutzerklärung“ (Art 13 und 14 DSGVO).

Aufgrund der guten Zugänglichkeit und Verfügbarkeit von Internet ist davon auszugehen, dass er Informationsverpflichtung gegenüber den betroffenen Personen auch in Form von Datenschutzerklärungen auf der Website des Verantwortlichen nachgekommen werden kann, sofern diese gut auffindbar sind (vgl dazu auch WP260, 2016/679).

Werden personenbezogene Daten **bei der betroffenen Person erhoben**, so wird diesem zum Zeitpunkt der Erhebung Folgendes mitgeteilt:

a) 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 und die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf dem Vorliegen berechtigter Interessen beruht, die konkreten berechtigten Interessen die verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

Zudem sind zur Sicherung einer fairen und transparenten Verarbeitung folgende Informationen zu geben:

f) die Dauer, für die die personenbezogenen Daten gespeichert werden oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
g) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
h) wenn die Verarbeitung auf einer Einwilligung beruht, den Umstand, dass die Einwilligung jederzeit widerrufen werden kann, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
i) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
j) 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 möglichen Folgen die Nichtbereitstellung hätte und
k) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 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.

Werden personenbezogene Daten **nicht bei der betroffenen Person erhoben**, so ist längstens binnen Monatsfrist oder mit einer allenfalls früheren Kommunikation oder Offenlegung an Dritte über Folgendes zusätzlich zu obigen Infos zu informieren:

a) die Kategorien personenbezogener Daten, die verarbeitet werden;
b) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen.

Die Informationspflicht entfällt allerdings, wenn die Speicherung und Verarbeitung von Daten durch Rechtsvorschriften geregelt ist – diese Ausnahme wird für Gebietskörperschaften in großen Bereichen (insb bei der Ausübung hoheitlicher Gewalt) zutreffen.

[Der Informationspflicht wird ua auch durch die Datenschutzerklärung auf Ihrer Website nachgekommen, Teil „Datenschutzerklärung“ des DKP]

2.2. Auskunftsrecht der betroffenen Person, Art 15 DSGVO

Dem Betroffenen ist zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden, und wenn ja, sind ihm auf Verlangen spezifische Informationen nach Art 15 DSGVO zu geben, wobei dazu die Angaben aus dem Verarbeitungsverzeichnis herangezogen werden können.

Das Auskunftsrecht ist also zweistufig:

a) Zunächst ist eine Auskunft zu geben, ob Daten gespeichert sind oder nicht („Negativauskunft“);
b) im Falle einer „Positivauskunft“ sind die oben angegebenen Informationen zu erteilen.

Der Verantwortliche stellt dazu auch kostenlos einmalig eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Wenn die betroffene Person den Antrag elektronisch stellt, so wird die Kopie der Informationen in einem gängigen elektronischen Format zur Verfügung gestellt, es sei denn der Betroffene verlangt eine besondere, aber angemessene Form der Auskunftserteilung.

Bei der Auskunftserteilung ist zwischen Auskunft über die personenbezogenen Daten einerseits und den Zugang zu Dokumenten, die personenbezogene Daten enthalten, andererseits zu differenzieren; hinsichtlich der zuletzt genannten Informationen besteht kein Zugangs-/Auskunftsrecht nach der DSGVO. In diesem Zusammenhang sei allerdings der Vollständigkeit halber auf das im öffentlichen Bereich existierende Recht auf Akteneinsicht nach § 17 AVG verwiesen, das vom Auskunftsrecht nach der DSGVO unabhängig existiert.

Auskunft ist auch darüber zu geben, ob besondere Kategorien personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, verarbeitet werden, sowie ob eine Verarbeitung von genetischen und biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person erfolgt (Art 9 DSGVO).

Zudem ist Auskunft über Informationen zu geben, die direkt oder indirekt mittels Zuordnung zu einer Kennung eine Identifizierung von natürlichen Personen ermöglicht.
Um dem Betroffenen es zu ermöglichen, dass er die von ihm verarbeiteten Daten auch auf Richtigkeit überprüfen kann, ist der Verantwortliche auch verpflichtet den konkreten Inhalt der personenbezogenen Daten zu beauskunften, also zB welcher Vorname oder Nachname im Konkreten tatsächlich verarbeitet wird.
Insgesamt hat der Verantwortliche nach Art 15 Abs 3 DSGVO eine Kopie der personenbezogenen Daten des Betroffenen herauszugeben, also nicht nur die Datenkategorie, sondern die konkreten personenbezogenen Daten.
Wird allerdings eine große Menge an Daten über die betroffene Person verarbeitet, trifft diese eine Präzisierungsobliegenheit – der Betroffene hat eine Mitwirkungspflicht!

2.2.1. Auskunftsprozess

Den betroffenen Personen ist **binnen eines Monats** (Verlängerungsmöglichkeit um 2 Monate) über die sie betreffenden automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell geführten Dateien Auskunft zu geben; der Auskunftsprozess ist wie folgt durchzuführen, wobei **jeder der nachfolgenden Schritte hinsichtlich Zeitpunkt und Tätigkeit entsprechend dauerhaft zu protokollieren und dieses Protokoll drei Jahre lang aufzubewahren**:

(1) Datum des Einlangens des Auskunftsbegehrens und Bestätigung des Einlangens
(2) Prüfung der Identität des Antragstellers – einfordern einer Kopie eines amtlichen Lichtbildausweises, es sei denn der Anspruchsteller ist amtsbekannt
(3) Einfordern einer elektronischen Zustelladresse für die Auskunft oder sonstiges vom Betroffenen gewünschtes Zustellmedium
(4) **Negativauskunft**, weil keine Daten verarbeitet werden, oder Übermittlung folgender Informationen (**Positivauskunft**) an die bekanntgegebene elektronische Adresse in einem gängigen elektronischen Format oder sonst speziell gewünschten Medium:
    a. Verarbeitungszweck
    b. die personenbezogenen Daten die verarbeitet werden bzw besondere Kategorien von Daten

c. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
d. allenfalls Empfänger in Drittländern oder bei internationalen Organisationen
e. falls möglich die geplante Dauer der Verarbeitung oder Kriterien für die Festlegung der Dauer
f. Informationen über die Herkunft der personenbezogenen Daten, wenn die Daten nicht bei der betroffenen Person erhoben wurden;
g. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und wenn ja, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen

(5) folgende allgemeine Mitteilung:

„Sie haben grundsätzlich das Recht im Zusammenhang mit den Sie betreffenden personenbezogenen Daten die Berichtigung oder Löschung oder Einschränkung der Verarbeitung zu verlangen sowie Widerspruch gegen eine bestimmte Verarbeitung einzulegen.

Sie haben zudem das Recht, sich bei der Datenschutzbehörde über Ihrer Meinung nach im Zusammenhang mit dem Recht auf Schutz Ihrer personenbezogenen Daten unberechtigte Behandlung zu beschweren; das gilt insbesondere, wenn Sie sich im Zusammenhang mit der Geltendmachung des Auskunftsrechts benachteiligt fühlen.

Sie haben das Recht, einmal im Jahr, eine kostenlose Kopie über den Gegenstand der Sie betreffenden Verarbeitung der personenbezogenen Daten, zu erhalten. Für darüberhinausgehende Kopien sind wir berechtigt ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten zu verlangen.

(6) Im Falle einer Nichterteilung der Auskunft ist der betroffenen Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür zu unterrichten, zB ungeeigneter Identitätsnachweis, missbräuchliches Ausüben des Auskunftsrechts.

[Ein Muster eines Auskunftsschreibens finden Sie in Teil „Musterformulare“ des DKP.]

2.3. Berichtigung, Art 16 DSGVO

Der Betroffene hat das Recht unverzüglich (also ohne unnötige Verzögerung) die

- Berichtigung oder
- Vervollständigung

der ihn betreffenden unrichtigen oder unvollständigen personenbezogenen Daten zu verlangen. Die Norm regelt also nicht nur die Richtigstellung, sondern auch die Vervollständigung von unvollständigen Daten.

Die Datenberichtigung ist allerdings auch im Sinne des Grundsatzes der „Datenrichtigkeit“ nach Art 5 Abs 1 lit d DSGVO stets zu beachten - Daten sind vom Verantwortlichen demnach stets sachlich richtig und erforderlichenfalls auf dem neuesten Stand zu halten.

2.3.1. Berichtigungsprozess

Die Abwicklung des Berichtigungsbegehrens ist **ohne unnötige Verzögerung** vorzunehmen; es ist **jeder der nachfolgenden Schritte hinsichtlich Zeitpunkt und Tätigkeit entsprechend dauerhaft zu protokollieren** und dieses Protokoll drei Jahre lang aufzubewahren:

(1) Datum des Einlangens des Auskunftsbegehrens
(2) Prüfung der Identität des Antragstellers – einfordern einer Kopie eines amtlichen Lichtbildausweises, es sei denn der Anspruchsteller ist amtsbekannt
(3) Einfordern eines amtlichen Dokuments, aus dem sich die Unrichtigkeit des zu berichtigenden Datensatzes ergibt
(4) Einfordern einer elektronischen oder sonstigen Adresse an die die Information über die Durchführung/Ablehnung der Berichtigung gesendet wird
(5) Mitteilung über die durchgeführte Berichtigung oder nicht durchgeführte Berichtigung samt Ablehnungsbegründung

2.4. Löschung, Art 17 DSGVO

Der Betroffene hat das Recht, vom Verantwortlichen zu verlangen, dass die ihn betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern keine Rechtsgrundlage mehr für die zulässige Verarbeitung vorliegt (insb Vertrag, berechtigtes Interesse, rechtliche/gesetzliche Verpflichtung).

Im Falle der Veröffentlichung der Daten durch den Verantwortlichen hat dieser unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art zu ergreifen, um andere Verarbeiter darüber zu informieren, dass der Betroffene die Löschung aller Links zu den personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Ausgenommen vom Löschungsrecht sind Verarbeitungen die erforderlich sind um die Meinungsäußerung sicher zu stellen oder für die eine rechtliche Verpflichtung besteht oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Löschung heißt nicht zwingend nur physisch löschen, sondern kann auch eine logische Löschung umfassen. Nach der stRsp verlangt der OGH eine physische Löschung jedenfalls dann, wenn die Datenerhebung/-verarbeitung rechtswidrig war/ist.

In den meisten Fällen ist ein „Löschbegehren“ der betroffenen Person aber als Zweckänderung zu verstehen/interpretieren, weil bestimmte andere Rechtfertigungsgründe zur Datenverarbeitung (insb öffentliches Interesse, berechtigte Interessen des Verantwortlichen/Dritten oder rechtliche Verpflichtungen) weiter bestehen bleiben. In diesen Fällen wird eine physische Löschung der Daten nicht möglich sein, vielmehr wird durch Änderung der Datenzugriffsberechtigung der Zweckänderung entsprochen („logisches Löschen“).

2.4.1. Löschungsprozess

Die Abwicklung des Löschungsbegehrens ist grundsätzlich **ohne unnötige Verzögerung vorzunehmen**, wobei **jeder der nachfolgenden Schritte hinsichtlich Zeitpunkt und Tätigkeit entsprechend dauerhaft zu protokollieren** und dieses Protokoll drei Jahre lang aufzubewahren ist:

(1) Datum des Einlangens des Löschungsbegehrens

(2) Prüfung der Identität des Antragstellers – einfordern einer Kopie eines amtlichen Lichtbildausweises, es sei denn der Anspruchsteller ist amtsbekannt

(3) Einfordern einer elektronischen oder sonstigen Adresse an die die Information über die Durchführung/Ablehnung der Löschung gesendet wird

(4) Prüfung des Löschungsbegehrens in der Sache:

a. **Änderung des Verarbeitungszweckes:**

   Kündigung eines Mitarbeiters => Beseitigung des aktiven Datenvorhalts, dh Daten sind technisch als „gelöscht“ zu kennzeichnen, für andere Zwecke, die rechtliche vorgesehen sind, aber im notwendigen Umfang auch weiterhin zu speichern (zB Ausstellung eines Dienstzeugnisses, Gewährleistungs- und Garantiefristen); Änderung des Berechigungskonzepts.

b. **Rechtswidrig erhobene und verarbeitete Daten**:

   i. Daten sind „physisch zu löschen“.

   ii. Diese physische Löschung ist auch in den Sicherungskopien umzusetzen: Löschungsansprüche sind aber in den Sicherungskopien nicht unverzüglich umzusetzen, sondern nur zum, aus wirtschaftlicher und technischer Sicht, nächstmöglichen Zeitpunkt; bis zu diesem Zeitpunkt ist eine logische Löschung in den Sicherungskopien (Zugriffsbeschränkung) möglich (§ 4 Abs 2 DSG idF Nov. 2018). Es ist allerdings sicherzustellen, dass im Fall des Einspielens des Back-ups an sich physisch zu löschende Daten nicht wieder in das laufende System aufgenommen (aktiviert) werden.

(5) Dem **Löschungsanspruch ist daher insb dann nicht nachzukommen**, wenn die Daten notwendig sind

a. zur Erfüllung einer rechtlichen Verpflichtung oder

b. zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder

c. um der Ausübung öffentlicher Gewalt nachzukommen oder

d. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

(6) Mitteilung an den Betroffenen, ob dem Löschungsbegehren nachgekommen wurde oder nicht; wird dem Begehren nicht nachgekommen, ist dies zu begründen.

2.5. Recht auf Einschränkung der Verarbeitung, Art 18 DSGVO

Die Einschränkung der Verarbeitung kann verlangt werden, wenn

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird,
b) die Verarbeitung unrechtmäßig ist und der Betroffene die Einschränkung der Nutzung verlangt
c) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
d) die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Wenn die Verarbeitung eingeschränkt wird, so dürfen diese personenbezogenen Daten nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen verarbeitet werden; die bloße Speicherung bleibt aber zulässig. Wird die Einschränkung der Verarbeitung aufgehoben, wird die betroffene Person davon verständigt. Die Einschränkung der Verarbeitung wird anderen Empfängern der Daten mitgeteilt.

2.6. Recht auf Datenübertragbarkeit, Art 20 DSGVO

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder zu verlangen, dass diese Daten einem anderen Verantwortlichen zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht und
b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Das Recht auf Datenübertragbarkeit kann daher nicht gegen Verantwortliche ausgeübt werden, die personenbezogenen Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es gilt auch nicht, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist.

2.7. Widerspruchsrecht / autom. Entscheidungsfindung im Einzelfall, Art 21f DSGVO

Der Betroffene hat das Recht, aus besonderen Gründen, jederzeit gegen die Verarbeitung der ihn personenbezogener Daten, die aufgrund eines berechtigten Interesses oder in Ausübung öffentlicher Gewalt verarbeitet werden, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.
Die Verarbeitung ist einzustellen, es sei denn, der Verantwortliche kann zwingende Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen, insb zur Ausübung oder Verteidigung von Rechtsansprüchen.
Gegen Datenverarbeitungen die der Direktwerbung dienen kann jederzeit Widerspruch eingelegt werden. Dies gilt auch für das Profiling, soweit es mit Direktwerbung in Verbindung steht.
Über das Widerspruchsrecht muss der Betroffene spätestens zum Zeitpunkt der ersten Kommunikation hingewiesen werden. Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

Der Betroffene hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, es sei denn die Entscheidung ist

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich oder
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung in Hinblick auf diese automatisierte Verarbeitung durch die betroffene Person erfolgt.

2.8. Mitteilungspflicht gegenüber Empfängern, Art 19 DSGVO

Es ist sicherzustellen, dass Einschränkungen oder Löschungen der Verarbeitung sowie Berichtigung der Daten auch an die Datenempfänger kommuniziert werden. Eine Ausnahme davon besteht nur bei Unmöglichkeit oder unverhältnismäßigem Aufwand. Es ist zu dokumentieren in welchem Umfang die Mitteilung erfolgt bzw warum eine Mitteilung an Empfänger im Konkreten unmöglich oder unverhältnismäßig ist.

Sollte die betroffene Person die konkreten Datenempfänger verlangen, so ist dieser die Liste der Datenempfänger offenzulegen (siehe Verarbeitungsverzeichnis – Anhang), im Falle der Unmöglichkeit der Offenlegung ist dies entsprechend zu dokumentieren.

2.9. Meldung von Datenschutzverletzungen, Art 33f DSGVO

Der Datenschutzbehörde ist Meldung im Falle einer Datenschutzverletzung mit Risken für die Rechte und Freiheiten der davon betroffenen Personen zu machen („**Data Breach Notification**“). Für die Melde- bzw Benachrichtigungsverpflichtung nach Art 33 und 34 DSGVO gilt grundsätzlich Folgendes (vgl dazu auch WP250, 2016/679):

Nach Art 33 DSGVO ist eine **Meldung** von Verletzungen des Schutzes personenbezogener Daten an die **Datenschutzbehörde** notwendig (die Datenschutzbehörde wird dazu aller Voraussicht nach ein Web-Formular zur Verfügung stellen), und zwar unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, **es sei denn**, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen** führt. Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.
Folgende Infos sind im Falle der Meldung an die Datenschutzbehörde zu geben:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Nach Art 34 DSGVO ist auch eine **Benachrichtigung der betroffenen Person** von einer Verletzung des Schutzes personenbezogener Daten erforderlich, wenn diese voraussichtlich e**in hohes Risiko für die persönlichen Rechte und Freiheiten**

natürlicher Personen zur Folge hat. Die Benachrichtigung hat unverzüglich zu erfolgen und beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten.

Die **Benachrichtigung kann unterbleiben**, wenn

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch **Verschlüsselung**; oder

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Abs 1 aller Wahrscheinlichkeit nach nicht mehr besteht; oder

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Die Infos nach b, c und d gemäß Pkt 2.9. sind dem Betroffenen im Falle der Benachrichtigungspflicht mitzuteilen.

2.9.1. Prozess zur data breach notification

Nach Art 33 bzw 34 DSGVO sind im Falle einer Verletzung des Schutzes personenbezogener Daten unter bestimmten Voraussetzungen eine Meldung an die Datenschutzbehörde **bis längstens 72 Stunden ab Bekanntwerden bzw unverzüglich** ab Bekanntwerden eine Benachrichtigung an die davon betroffenen Personen, vorzunehmen, und zwar nach folgenden Vorgaben:

1. Liegt eine Verletzung des Schutzes personenbezogener Daten vor (weil zB ein USB-Stick oder anderes Speichermedium verloren oder ein Laptop gestohlen wurde), führt dieses aber **nicht zu einem Risiko** für die Rechte/Freiheiten der Betroffenen, ist **keine Meldung erforderlich**, und zwar weder an die Behörde noch an die betroffene Person. Dies ist bspw der Fall, wenn zwar Speichermedien mit personenbezogene Daten abhandenkommen, das Speichermedium aber vor unberechtigtem Zugriff angemessen geschützt ist (zB Datenverschlüsselung oder Zugriffsschutz durch ausreichendes Passwort).

2. Liegt eine Verletzung des Schutzes personenbezogener Daten vor (weil zB ein USB-Stick oder anderes Speichermedium verloren oder ein Laptop gestohlen wurde) und führt dies **zu <u>einem Risiko</u>** für die Rechte/Freiheiten der Betroffenen, ist **zwar diese Verletzung an <u>die Datenschutzbehörde zu melden</u>**, **nicht aber an die davon betroffenen Personen (Art 33 DSGVO)**. Dies ist bspw der Fall, wenn kein angemessener Schutz vor unberechtigten Zugriff auf die personenbezogenen Daten gegeben ist, es sich aber nicht um besondere Kategorien von Daten (Art 9 DSGVO = Gesundheitsdaten odgl) handelt oder um Daten die über bloße Stammdaten hinausgehen oder durch Zusammenführung mit anderen zugänglichen Daten für eine betroffene Person besondere Bedeutung haben.
3. Liegt eine Verletzung des Schutzes personenbezogener Daten vor (weil zB ein USB-Stick oder anderes Speichermedium verloren oder ein Laptop gestohlen wurde) und führt dies **zu <u>einem hohen Risiko</u>** für die Rechte/Freiheiten der Betroffenen, ist **diese Verletzung sowohl an die Datenschutzbehörde (Art 33 DSGVO)**, **als auch unverzüglich an die davon b<u>etroffenen Personen zu melden</u> (Art 34 DSGVO)**. Dies ist bspw der Fall, wenn kein angemessener Schutz vor unberechtigten Zugriff auf besondere Kategorien von Daten gegeben ist (Art 9 DSGVO = Gesundheitsdaten odgl) oder auf Daten die über bloße Stammdaten hinausgehen oder auf Daten die durch Zusammenführung mit anderen zugänglichen Daten für eine betroffene Person besondere Bedeutung haben (zB weil bspw besondere Verhaltensweisen oder Profile des Betroffenen erstellt werden könnten).

Folgende <u>Infos sind an die Datenschutzbehörde</u> im Falle <u>eines Risikos für die Betroffenen</u> binnen längstens 72 Stunden ab Bekanntwerden der Verletzung zu melden:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Folgende <u>Infos sind dem Betroffenen</u> im Falle eines <u>hohen Risikos für die Betroffenen</u> unverzüglich zu geben:

a) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
c) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die Überlegungen die zu einer oder keiner Meldung an die Datenschutzbehörde und/oder die betroffenen Personen führen, sind entsprechend dauerhaft zu protokollieren und zumindest drei Jahre lang aufzubewahren.