Leitfaden Transparenz / Erfüllung der Informationspflichten

wie ist die Transparenz herzustellen?

1. Informationspflichten: Worüber müssen Betroffene informiert werden? (Datenschutzerklärung gem. Art. 13 und 14 DSGVO)

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

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

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

Eine Datenschutzerklärung, die uU auch auf der Website notwendig sein könnte (z.B. bei Webshops, Anmeldungen für Newsletter, etc…), ist auf den aktuellen Stand der Informationsverpflichtungen nach der DSGVO anzupassen. Auch bei anderen Arten der Erhebung von Daten sind die betroffenen Personen ausreichend iSd Art. 13 und 14 DSGVO zu informieren, und die notwendige Texte sind zu erstellen bzw. die bestehenden Texte zu überarbeiten. Die Informationspflicht trifft nach der DSGVO immer den **datenschutzrechtlichen Verantwortlichen.**

2. Erfüllung der Informationspflichten

Die DSGVO schreibt vor, dass der Verantwortliche (dh derjenige, der über den Zweck und die Mittel der Verarbeitung entscheidet) die betroffenen Personen (dh die Personen, deren Daten er verarbeitet) über die Verarbeitungsvorgänge informiert, und zwar einerseits die Personen, von denen er direkt Daten (über die eigene Person) erhält, und andererseits auch Personen, bei denen die Datenerhebung ohne direkten Kontakt mit denselben erfolgt. Einen Auftragsverarbeiter (der im Auftrag eines Verantwortlichen personenbezogene Daten verarbeitet) trifft diese Informationsverpflichtung nicht.

Die Mitteilung ist in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Die Information kann schriftlich oder in anderer Form, z.B. elektronisch, oder wenn die betroffene Person es verlangt, auch mündlich erfolgen.

Die Informationserteilung erfolgt unentgeltlich.

3. Direkte Datenerhebung (Art 13 DSGVO)

Wann sind die Informationen mitzuteilen?

Der Verantwortliche hat (Art 13 DSGVO) der betroffenen Person Informationen bei Erhebung der Daten in direktem Kontakt mit der betroffenen Person zur Verfügung zu stellen.
„Zum Zeitpunkt der Erhebung“: dh grundsätzlich unmittelbar in zeitlichen Zusammenhang mit der tatsächlichen Erhebung der Daten, dh der Aufnahme der Daten (Erfassung) in ein (elektronisches) Dateisystem. Bei einer Anmeldung zu einem Newsletter ist der Zeitpunkt der Erhebung daher der Anmeldzeitpunkt (z.B. im Internet) oder die Abgabe der Einwilligungserklärung (z.B. auf einer Gewinnspielkarte oder einem Formular bei einem Messestand). Bei der Verwendung einer App oder von Software ist dies der Zeitpunkt des Downloads bzw. der Installation auf dem Gerät. Bei einem Vertragsabschluss (mit einem Mitarbeiter, einem Kunden, einem Lieferanten oder Partner) ist dies der Zeitpunkt des Vertragsabschlusses. Bei einem Bewerber ist es der Zeitpunkt, in dem die Bewerberdaten einlangen.

Welche Informationen sind zu erteilen?

Namen und Kontaktdaten (Adresse, Telefonnummer, Email-Adresse) des **Verantwortlichen** und gegebenenfalls seines Vertreters (= ...)

Kontaktdaten des **Datenschutzbeauftragten** (sofern bestellt; es besteht nicht die Notwendigkeit, den Namen offenzulegen, denn es reicht, dass die betroffenen Personen die Möglichkeit zur Kontaktaufnahme haben: dsba@domain.at oder Telefonnummer oder Adresse)

Zweck der Verarbeitung (z.B. zur Abwicklung des geschlossenen Vertragsverhältnisses, Personalverwaltung, Bewerbermanagement, Abwicklung von Geschäftsfällen mit Kunden/ Lieferanten, Kundenbetreuung und Kundengewinnung (Newsletter, andere Marketingmaßahmen), Schutz des Eigentums (Videoüberwachung), Sicherstellung der Verfügbarkeit der IT-Systeme und IT-Sicherheit (Logfiles, Email-Archivierung). Den Zweck der Verarbeitungsvorgang können sie aus dem Verzeichnis gem. Art 30 DSGVO entnehmen.

Rechtsgrundlage der Verarbeitung: Jede Verarbeitungstätigkeit bedarf zumindest einer Grundlage für ihre Rechtmäßigkeit (Datenverarbeitung ist grundsätzlich verboten, außer sie ist (durch einen der Tatbestände der DSGVO) erlaubt). Bei "allgemeinen" Daten finden Sie die „Erlaubnistatbestände" in Art 6 Abs 1 (a) bis (f) DSGVO; bei "besonderen Datenkategorien", dh z.B. Gesundheitsdaten oder biometrischen Daten sind Grenzen der erlaubten Datenverarbeitung in Art 9 festgelegt (und enger als bei "allgemeinen" Daten).

Die Erlaubnistatbestände für die Verarbeitung von "allgemeinen" Daten sind:

- Einwilligung (jederzeit widerrufbar!)
- Ein Vertrag oder die Vertragsanbahnung (ausgehend von der betroffenen Person) - für diejenigen Daten, die für die Vertragserfüllung notwendig sind
- Notwendigkeit der Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt (die sich aus einem Gesetz, einer Verordnung oder einer sonstigen generellen Norm der EU oder eines Mitgliedsstaates ergeben muss)

- Schutz von lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person
- Wahrnehmung einer Aufgabe im öffentlichen Interesse oder Ausübung öffentlicher Gewalt
- Berechtigtes Interesse des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen. Beim berechtigen Interesse besteht eine erhöhte Transparenzpflicht (das Interesse ist im Rahmen der Informationserteilung anzugeben). Es besteht bei der Rechtsgrundlage "berechtigtes Interesse" ein Widerspruchsrecht der betroffenen Personen, dh die betroffenen Personen können der Verarbeitung widersprechen. Die betroffenen Personen sind auf dieses Widerspruchsrecht gesondert hinzuweisen. Behörden in Erfüllung ihrer Aufgaben können sich nicht auf die Rechtsgrundlage des berechtigten Interesses stützen.

Überdies ist auf die **Rechte der betroffenen Person** hinzuweisen.
Es ist auch auf das **Recht auf Beschwerde** hinzuweisen.
Wird das **berechtigte Interesse** als Rechtsgrundlage verwendet (Achtung: Widerspruchsrecht), dann ist auch das berechtigte Interesse konkret zu nennen.
Nutzt die Organisation **automatisierte Entscheidungsfindung inkl. Profiling**[1], dann ist auf das Recht des menschlichen Eingriffs in die Entscheidungsfindung hinzuweisen.

4. Daten von Dritten (Art 14 DSGVO)

Der Verantwortliche hat Personen, deren Daten er von dritter Seite erhält, auch zu informieren. Dies sind z.B. Situationen, in denen ein direkter Kontakt mit einer betroffenen Person besteht, aber (auch) Daten von anderen betroffenen Personen erhoben werden, z.B. im Rahmen einer Hotelbuchung, bei der eine Person die Buchung für eine Gruppe von Personen (z.B. eine Familie) vornimmt, Erstellung einer Marketingdatenbank aus öffentlich verfügbaren Quellen oder Zukauf, Datensammlungen über das Internet oder andere öffentliche Quellen zu bestimmten Zwecken, Verarbeitung von Daten von Bezugspersonen im Bereich der Personalverwaltung (z.B. für Kinderzuschüsse, Pflegefreistellung oder Sonderurlaub bei Heirat).

Wann ist die Information zu erteilen:

Die Information ist zu folgenden Zeitpunkten zu erteilen, wobei derjenige Zeitpunkt zu wählen ist, der früher eintritt:

- in angemessener Frist nach Erhebung (max. 1 Monat)
- bei der ersten Kommunikation mit der betroffenen Person
- zum Zeitpunkt der ersten Offenlegung an einen anderen Empfänger

Wann ist die Information nicht zu erteilen:

- die betroffene Person verfügt bereits über die Informationen
- die Informationserteilung erweist sich als unmöglich oder erfordert einen unverhältnismäßigen Aufwand
- wenn die Informationserteilung die Ziele der Verwirklichung der Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt (z.b. Überwachung durch einen Detektiv) die personenbezogenen Daten (nach dem Recht der EU oder eines Mitgliedsstaates) einem Berufsgeheimnis (Rechtsanwälte, Ärzte, Wirtschaftstreuhänder ...) einschließlich einer

[1] Unter Profiling wird eine automatisierte Bewertung oder Vorhersage persönlicher Aspekte von Betroffenen, wie z.B. wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Aufenthaltsorte etc. verstanden.

satzungsgemäßen Geheimhaltungspflicht unterliegen und daher vertraulich behandelt werden müssen

Zusätzlich zu den Informationen gem. Art 13 DSGVO (siehe oben) sind folgende Informationen zur Verfügung zu stellen:

Datenkategorien: Es sind auch die Datenkategorien zur Kenntnis zu bringen, da kein Kontakt mit der betroffenen Person direkt besteht, und die betroffene Person daher keine Möglichkeit hat, direkt zu erkennen, welche Daten erhoben werden.

Herkunft der Daten: da die Daten nicht direkt bei der betroffenen Person erhoben werden, ist auch bekannt zu geben, woher die Daten stammen (z.B. aus öffentlichen Quellen, Zukauf von Marketingdaten, von einer betroffenen Person)

5. Hinweise:

Beschäftigte

Es handelt sich um eine direkte Datenerhebung, da ein direkter Kontakt mit der betroffenen Person besteht. Die Informationserteilung kann z.B. bei Unterfertigung des Dienstzettels oder Dienst- oder Arbeitsvertrages erfolgen, oder auch im Intranet. Jedenfalls ist sicherzustellen, dass beim Einritt der Beschäftigten die Informationen erteilt werden und auch dann, wenn neue Verarbeitungsvorgänge hinzukommen, die Informationspflicht erfüllt wird.

Bewerber

Bewerber wenden sich mit „Initiativbewerbungen" oder auf Inserate (Print, Online) oder bewerben sich über Online-Portale.

Initiativbewerbung:

Wenn eine nicht angefragte Bewerbung einlangt, dann ist der/die Bewerber/in über die Datenverarbeitung (direkte Erhebung, daher gem. Art 13 DSGVO) zu informieren. Werden die Daten "erhoben", dann kann dies in einem Standardschreiben (z.B. per Email) erfolgen, mit dem auf die Bewerbung reagiert wird (Bestätigung des Einlangens der Bewerbung, Einladung zu einem Bewerbungsgespräch). Erfolgt eine Absage, dann ist davon auszugehen, dass der Zweck der Verarbeitung mit dem Eingang der Bewerbung weggefallen ist, und die Bewerbung ist daher zu löschen.

Bewerbung auf eine ausgeschriebene Stelle:

In diesem Fall ist maßgebend, auf welche Art und Weise die Ausschreibung der Stelle (Inserat, Portal etc.) erfolgt, und wie die Bewerbung selbst erfolgt. Bei einem Inserat oder einer Schaltung in einem Online-Portal sollte der Hinweis auf die Verarbeitung von personenbezogenen Daten bereits in der Stellenausschreibung erfolgen und bei diesem Hinweis kann auf die Datenschutzerklärung auf der Website verwiesen werden (zB wir weisen darauf hin, dass wir die von Bewerbern mitgeteilten Daten automationsunterstützt speichern. Wir löschen die Daten - sofern wir keine Zustimmung für eine Evidenzhaltung erhalten - 6 Monate und 2 Wochen nach Beendigung des Bewerbungsprozesses. Weitere Informationen erhalten Sie unter: www.domain.at/dsinfo

Erfolgt die Bewerbung über ein Portal oder die Website, dann sollte die Datenschutzinformation auch direkt im Rahmen des Bewerbungsprozesses abrufbar sein, und zwar entweder durch einen Mouseclick auf eine Unterseite oder durch die Möglichkeit die Information (z.B. als PDF) downzuloaden.

Kunden / Lieferanten

Beim Kunden und Lieferanten handelt es sich um einen Vertragspartner des Verantwortlichen, mit dem er in direktem Kontakt steht. Beim ersten Kontakt sollte daher dem Kunden/Lieferanten in angemessener Art und Weise die Datenschutzinformation zur Verfügung gestellt werden bzw. der Kunde sollte auf die wesentlichste Information hingewiesen werden, und ihm die Zugangsmöglichkeit zur generellen Datenschutzinformation gegeben werden.

Direkter persönlicher Kontakt im Rahmen des Vertragsabschlusses:

Wenn der Verantwortliche direkt mit dem Kunden/Lieferanten direkt persönlich in Kontakt tritt, kann er diesem im Rahmen der Übergabe von Dokumenten (z.B. Angebot, Annahme, Felder, sonstige Unterlagen, Schriftstücke, Visitenkarte etc) die wesentlichsten Informationen mitteilen, und auf die Zugangsmöglichkeit zur generellen Datenschutzinformation hinweisen. In diesem Fall empfiehlt es sich, dass beim Vertragsabschluss grundsätzlich der Vertreter des Verantwortlichen auch einen Ausdruck der Datenschutzinformation dabei hat, um im Fall einer Anfrage des Kunden diese Information direkt herausgeben zu können.

Direkter telefonischer Kontakt im Rahmen des Vertragsabschlusses:

Hier ist es nicht möglich, dass ein Dokument übergeben wird, sodass ein Hinweis (bitte beachten Sie unsere Datenschutzinformationen auf der Homepage: www.domain.at unter "Datenschutzinformation") im Rahmen des Telefonats sinnvoll ist. Wird dem Kunden/Lieferanten unmittelbar nach dem Telefonat etwas zugesendet, z.B. bereits das Angebot/Annahmeerklärung per Email oder auch nur eine Bestätigung, dass ein Telefonat stattgefunden hat, und ein Angebot erstellt und übermittelt werden wird, kann in dieser Mitteilung auf die Verarbeitung der personenbezogenen Daten hingewiesen werden, und auf die Homepage mit der generellen Datenschutzinformation verwiesen werden.

CHECKLISTE

Informationspflicht bei direkter Erhebung
von personenbezogenen Daten

(Art 13 DSGVO)

1. **Namen** und **Kontaktdaten des Verantwortlichen** sowie gegebenenfalls seines Vertreters;
2. **Kontaktdaten des Datenschutzbeauftragten**;
3. die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen,
4. **Rechtsgrundlage** für die Verarbeitung (allgemeine Datenkategorien) - Art 6 (1) DSGVO:

    a) Einwilligung

    b) Vertrag oder Vertragsanbahnung

    c) rechtliche Verpflichtung des Verantwortlichen

    d) öffentliches Interesse / öffentliche Aufgabe

    e) lebenswichtige Interessen der betroffenen Person oder eines Dritten

    f) berechtigte Interessen des Verantwortlichen oder eines Dritten;

5. bei Verarbeitung aufgrund berechtigtem Interesse: die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
6. Empfänger oder **Kategorien von Empfängern**
7. Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
8. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

9. das Bestehen eines Rechts

    1. auf **Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie

    2. auf **Berichtigung** oder

    3. **Löschung** oder

    4. auf **Einschränkung** der Verarbeitung oder

    5. eines **Widerspruchsrechts** gegen die Verarbeitung sowie

    6. des Rechts auf **Datenübertragbarkeit**;

10. bei **Einwilligung** als Grundlage: das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

11. das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde;

12. 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

13. 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.