DATENSCHUTZGRUND-VERORDNUNG 2018

Übersicht der notwendigen Schritte

Diese Dokumentation gibt einen groben Überblick auf die möglichen Erfordernisse der DSGVO 2018. Keinesfalls ersetzt dieses Dokument aber die Beratung eines zertifizierten Datenschutzbeauftragten, da der Umgang mit den betrieblichen Daten immer eine individuelle Erhebung im jeweiligen Unternehmen, Verein oder Organisation voraussetzen. Mit dieser Dokumentation besteht auch keinerlei Anspruch auf die Vollständigkeit zu diesem Thema.

Inhaltsverzeichnis

1 Grundlagen der EU-DSGVO und des österreichischen Datenschutzrechts

Ab dem 25. Mai 2018 wird die Datenschutzgrundverordnung, ein seit dem Mai 2016 gültiges EU-Recht, schlagend.

Das heißt, ab diesem Zeitpunkt müssen diese Verordnungen, angepasst auf Österreich, durchgeführt werden.

1.1 Einstieg in das Datenschutzrecht

Was erwartet Sie mit dieser Verordnung?

Wir sehen uns nachfolgend das Regelwerk und Grundbegriffe an Hand einiger Fragen und Beispiele an:

- 1.Müssen wir im Unternehmen einen DATENSCHUTZBEAUFTRAGTEN (Datenschutzbeauftragen) bestellen?
- 2.Müssen wir im Unternehmen ein Verarbeitungsverzeichnis erstellen?
- 3.Können wir die DSGVO im Unternehmen ignorieren?

1.1.1 Artikel 8 GRC[1] Schutz von Daten

Schutz pb (personenbezogener) Daten

1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

1.2 Datenschutzgrundverordnung (DSGVO)

- Warum eine EU-Verordnung?
- Harmonisiertes Datenschutzniveau in der EU
- Unmittelbare Anwendbarkeit

[1] Charta der Grundrechte der EU

- ➢ Verdrängt nationales Recht
- ➢ Warum eine „Grundverordnung“?
- Enthält zahlreiche Öffnungsklauseln
- Hybrid aus Verordnung und Richtlinienelemente

1.2.1 Anmerkungen dazu:

1) Die juristische Person wird von der DSGVO nicht mehr erfasst, unterliegt aber zukünftig der ePrivacy-Verordnung. [2]Weiters gelten die §§ 1 bis 3 DSG 2018[3] auch für juristische Personen (arg „jedermann“). Die e-Privacy-Verordnung soll für Anbieter von elektronischen Kommunikationsdiensten sowie für Unternehmen, die Marketing betreiben, gelten und wird eine lex specialis zur DSGVO sein. Mit ihr wurde ein weiteres Sanktionsmodell erschaffen, das in Anlehnung an die DSGVO ebenso empfindliche Geldbußen vorsieht.
2) Die ePrivacy-Verordnung schafft zusammen mit der EU-DSGVO neue Regeln für digitale Medien und elektronische Kommunikationsdienste. Sie stuft alle digitalen Endgeräte im Dialog Marketing- und im Online-Marketing-Kontext grundsätzlich als „personenbezogen“ ein. Dies bedeutet beispielsweise, dass diese Geräte bei der Auslieferung für das Setzen von Cookies oder ähnliche Techniken zunächst einmal deaktiviert sind.
3) Aufgrund der Ähnlichkeit mit den jetzigen Bestimmungen des österreichischen Telekommunikations-Gesetzes ergeben sich keine Änderungen im Verhältnis zur bestehenden nationalen Rechtslage.

1.2.2 DSGVO

a. Harmonisierung des Datenschutzniveaus sowie Sicherstellung des freien Datenverkehrs innerhalb der EU
b. Über 3.000 Änderungsanträge
c. 99 Artikel und 173 Erwägungsgründe
d. In Kraft seit 24.05.2016
e. Unmittelbar anwendbar in allen Mitgliedstaaten ab 25.05.2018
f. Nationales Ausführungs- bzw. Umsetzungsgesetz erforderlich (DSG 2018) BGBl I 120/2017[4]; Reaktionen des Landesgesetzgebers?

---

[2] E-Privacy Verordnung – Website der WKO
[3] Bundesgesetzblatt Datenschutz 2000/Anpassungen 2018
[4] Bundesgesetzblatt Datenschutz 2018

1.3 DATENSCHUTZBEAUFTRAGTE?

Wer braucht im Unternehmen einen Datenschutzbeauftragten?

1.3.1 Artikel 37 Absatz 1:

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen DATENSCHUTZBEAUFTRAGTEN, wenn:

1) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
2) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Artikel, ihres Umfangs und / oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder:
3) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß. Artikel 9 oder von personenbezogene Daten über strafrechtliche Verurteilungen und Strafdaten gemäß. Artikel 10 besteht.

1.4 Beispiele:

1.4.1 Situation:

Ein österreichisches IT-Unternehmen mit 12 MitarbeiterInnen entwickelt Softwareprodukte unter anderem für niedergelassene Ärzte und Rechtsanwälte (PatientInnenverwaltung, Klienten Datei und ähnliche Anwender).

1. Muss das Unternehmen einen Datenschutzbeauftragten bestellen?

Nein, da …

a) es sich um keine Behörde / öffentliche Stelle handelt,
b) die Kerntätigkeit nicht im Bereich der Überwachung von betroffenen Personen, bzw.
c) die Kerntätigkeit nicht im Bereich der Verarbeitung von sensiblen Daten liegt

1.4.2 Situation:

Ein österreichisches IT-Unternehmen mit 12 MitarbeiterInnen entwickelt Softwareprodukte unter anderem für niedergelassene Ärzte und Rechtsanwälte, würde es **Sinn machen, einen DATENSCHUTZBEAUFTRAGTEN zu bestellen?**

Ja, weil…

a) personenbezogene Daten verarbeitet werden (eigene Mitarbeiter bzw. gegebenenfalls Daten von Dritten durch Kundenbetreuung)
b) die DSGVO und ihre Pflichten für den Verantwortlichen zur Anwendung gelangen.
c) die Bestellung eines Datenschutzbeauftragten im „Ernstfall“ eine allfällige Haftung reduzieren kann (Haftung interner/externer DATENSCHUTZBEAUFTRAGTER)

2 Qualifikation des DATENSCHUTZBEAUFTRAGTEN:

2.1 Artikel 37 Absatz 5 DSGVO[5]:

Der Datenschutzbeauftragte wird auf Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 DSGVO - DATENSCHUTZBEAUFTRAGTEN

2.1.1 Anmerkung:

- Bei der Erfüllung seiner Aufgaben ist der DATENSCHUTZBEAUFTRAGTE weisungsfrei und
- unmittelbar der höchsten Managementebene unterstellt.
- Er kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder
- seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

2.1.1.1 Praxistipp:

Achtung Interessenkonflikt bei Geschäftsführer, Personalchef, Prokurist, Administrator, IT-Leiter, Anwalt des Unternehmens, etc.

Unternehmen, die das Netzwerk eingerichtet haben, Softwareanbieter („Selbstkontrolle“) - Diese Personen dürfen nicht als DATENSCHUTZBEAUFTRAGTE eingesetzt werden.

2.2 Aufgaben des DATENSCHUTZBEAUFTRAGTEN

Die Aufgaben sowohl intern als auch externer Natur

2.2.1 Artikel 39 Absatz 1[6]:

1) Dem DATENSCHUTZBEAUFTRAGTEN obliegen zumindest folgende Aufgaben:
2) Unterrichtung und Beratung des Verantwortlichen / Auftragsverarbeiters und der Beschäftigten

[5] Datenschutzgrundverordnung EU –Bestellung eines Datenschutzbeauftragten
[6] Datenschutzgrundverordnung EU-Aufgaben eines Datenschutzbeauftragten

3) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen / Auftragsverarbeiters für den Schutz personenbezogene Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
4) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
5) Zusammenarbeit mit der Aufsichtsbehörde
6) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36 und gegebenenfalls. Beratung zu allen sonstigen Fragen

2.2.1.1 Anmerkung:

- Wichtig ist, dass der DATENSCHUTZBEAUFTRAGTE nicht verantwortlich für die Einhaltung der DSGVO ist.
- Insofern ist es auch nicht möglich, den DATENSCHUTZBEAUFTRAGTEN als Verantwortlichen gemäß § 9 VstG[7] zu nominieren.
- Die Verantwortung für die Einhaltung der DSGVO kommt dem Unternehmen (als Verantwortlicher der Auftragsverarbeiter) zu und nicht dem DATENSCHUTZBEAUFTRAGTEN. Es obliegt daher dem Unternehmen dafür zu sorgen, dass die DSGVO entsprechend erfüllt wird.

2.3 Erfüllende Anforderungen an Ihr Unternehmen:

Welche Anforderungen kommen im Rahmen der DSGVO auf Sie zu?

2.3.1 Rechenschaftspflicht:

Führung eines Verfahrensverzeichnisses; Management der Auftragsverarbeiter; Privacy by Design; Privacy by Default; Compliance von neuen Datenanwendungen; Durchführung von Datenschutz-Folgenabschätzungen

2.3.2 Transparenz:

Etablierung eines Datenschutzmanagementsystems; Informationspflichten an

[7] Verwaltungsstrafgesetz

Betroffene; Regeln für den Datentransfer in Nicht-EU-Länder

2.3.3 Information:

Beratung und Schulung der Mitarbeiter; Fortbildungen und Ausbildung des DATEN-SCHUTZBEAUFTRAGTEN

2.3.4 Kommunikation:

Zusammenarbeit mit der Aufsichtsbehörde; Bearbeitung und Beantwortung von Anfragen von Betroffenen; Bearbeitung und Meldung von Datensicherheitsvorfällen

2.4 Wann ist die DSGVO zu beachten?

a) Helmut (H) spricht mit Meinrad (M) über höchstpersönliche Details des Hans.
b) Birgit (B) scannt die Arbeitsverträge ihrer MitarbeiterInnen ein.
c) Klara (K) speichert die Namen und Telefonnummern ihrer Freunde in ihrem Smartphone ab.

Auf welchen Sachverhalt ist die DSGVO anzuwenden?

2.4.1 Artikel 2 DSGVO (sachlicher Anwendungsbereich)

Der Regelungsbereich der DSGVO erstreckt sich sowohl auf:

- die ganz oder teilweise automatisierte Verarbeitung personenbezogene Daten sowie
- auf die nichtautomatisierte Verarbeitung personenbezogene Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Artikel 2 Absatz 1)

2.4.2 Personenbezogene Daten (Artikel 4 Z 1):

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

2.4.2.1 Anmerkung:

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung

- wie einem Namen,
- zu einer Kennnummer,
- zu Standortdaten,
- zu einer Online-Kennung oder

- zu einem oder mehreren besonderen Merkmalen, die Ausdrücke der physischen, physiologischen, genetischen,
- psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind,

identifiziert werden können

2.5 Anonyme Daten bzw. anonymisierte Daten

… fallen nicht unter die DSGVO, diese können sein:

Absolut anonym	Relativ anonym
Informationen nicht auf den Menschen beziehbar	Informationen können sich auf den Menschen beziehen
Oder der Mensch, auf den sich die Informationen beziehen, ist faktisch nicht identifizierbar	Jedoch unwahrscheinlich

2.6 Pseudonymisierte Daten

2.6.1 Pseudonymisierung bzw. pseudonymisierte Daten (Artikel 4 Z 5)

Diese Daten fallen uneingeschränkt unter die DSGVO!

Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden, kann unter dem **Begriff der Pseudonymisierung zusammengefasst werden.**

2.6.2 Erwägungsgrund 28:

Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen

3 Sensible Daten

3.1 Artikel 9 Absatz 1:

„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt."

- Artikel 4 Z 13: „genetische Daten"
- Artikel 4 Z 14: „biometrische Daten"
- Artikel 4 Z 15: „Gesundheitsdaten

3.2 Weitere neue Begriffsbestimmungen

Welche neuen Begriffsbestimmungen gibt es im Rahmen der DSGVO

3.2.1 Verarbeitung (Artikel 4 Z 2):

1) Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder
2) jede solche Vorgangsreihe im Zusammenhang mit personenbezogener 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

3.3 Was ist ein Dateisystem?

3.3.1 Dateisystem (Artikel 4 Z 6):

„ein Dateisystem“ =

- jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

3.3.1.1 Beispielspiele:

Artikelkartei, Anamneseblätter, nicht aber Akten und Aktenkonvolute

3.4 Ausnahmen vom sachlichen Anwendungsbereich der DSGVO

3.4.1 Die DSGVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten (Artikel 2 Absatz 2 DSGVO)

- außerhalb des Anwendungsbereichs des Unionrechts,
- durch die Mitgliedstaaten im Rahmen von Tätigkeiten der gemeinsamen Außen- und Sicherheitspolitik (Titel V Kapitel 2 EUV[8]),
- durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
- durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (siehe dazu DS-RL-Strafverfolgung 2016/680[9]).

3.5 Keine Anwendung der DSGVO

Die DSGVO findet keine Anwendung auf die Verarbeitung personenbezogene Daten (Artikel 2 Absatz. 2 DSGVO[10]) natürlicher Personen zur Ausübung ausschließlich persönlich oder familiärer Tätigkeiten.

---

[8] EU-Vertrag

[9] EU-Vertrag Richtlinie zum Schutz der natürlichen Personen

[10] EU-Datenschutzgrundverordnung

3.5.1 Erweiterungsgrund 18:

Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Als persönliche oder familiäre Tätigkeiten könnten auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten.

Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogene Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.

3.6 Wann ist die DSGVO also zu beachten?

Nachstehend einige Fallbeispiele dazu

3.6.1 Toni spricht mit Konrad über höchstpersönliche Details des Georg - ist die DSGVO anwendbar?

Nein, da personenbezogene Daten weder automatisiert noch nichtautomatisiert in einem Dateisystem verarbeitet werden.

3.6.2 Silvia scannt die Arbeitsverträge ihrer MitarbeiterInnen ein.

Ja, weil es sich dabei um eine (zumindest teilweise) automatisierte Verarbeitung personenbezogene Daten handelt.

3.6.3 Hanni speichert die Namen und Telefonnummern ihrer Freunde in ihrem Smartphone ab.

Nein, weil es sich dabei um die Ausübung ausschließlich persönlicher Tätigkeiten handelt (siehe Artikel 2 Absatz 2 lit c DSGVO[11])

[11] EU-Datenschutzgrundverordnung

3.7 Räumlicher Anwendungsbereich der DSGVO

„Niederlassungsprinzip“: DSGVO findet auf alle sachlich in ihren Bereich fallenden Datenverarbeitungen im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU Anwendung (Artikel 3 Absatz 1DSGVO[12]).

- Erweiterter Anwendungsbereich (Niederlassungen außerhalb der Union)
- Anbieten von Waren und Dienstleistungen in EU (Marktprinzip)
- Beobachtung des Verhaltens von Betroffenen in der EU (jeweils Benennung eines Vertreters in EU erforderlich)
- Völkerrechtliche Grundlage (z.B. diplomatische bzw. konsularische Vertretungen)

3.7.1 Beispiel 1:

Der Sitz einer Automobilhersteller-AG befindet sich in den USA. Der Konzern hat eine in Österreich gelegene Filiale, die Kundendaten automationsunterstützt für eigene Werbezwecke verarbeitet. Kommt die DSGVO zur Anwendung?

Ja! Bei der Filiale handelt es sich um eine Niederlassung in Österreich, die im Rahmen ihrer Tätigkeiten, Datenverarbeitungen zu Werbezwecken vornimmt. Die DSGVO ist auf diese Verarbeitung personenbezogene Daten anwendbar.

3.7.1.1 Erweiterungsgrund 22:

Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine **feste Einrichtung** voraus. Die **Rechtsform** einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei **nicht ausschlaggebend**

3.7.2 Beispiel 2:

Ein IT-Unternehmen bekommt einen Auftrag für ein Unternehmen mit Sitz in der Türkei personenbezogene Daten von betroffenen Personen zu verarbeiten.

Ist die DSGVO anwendbar?

[12] EU-Datenschutzgrundverordnung

Ja! Die DSGVO ist auch anwendbar, wenn zwar der Verantwortliche seinen Sitz außerhalb der EU hat, aber einen Auftragsverarbeiter mit Niederlassung in der EU (im Rahmen dessen Tätigkeiten) für seine Datenverarbeitung heranzieht, unabhängig davon, ob die Datenverarbeitung selbst in der Union stattfindet.

3.8 Weitere wichtige Begriffsbestimmungen:

3.8.1 Verantwortlicher (Artikel 4 Z 7):

Verantwortlicher =

die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,

- die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogene Daten entscheidet;

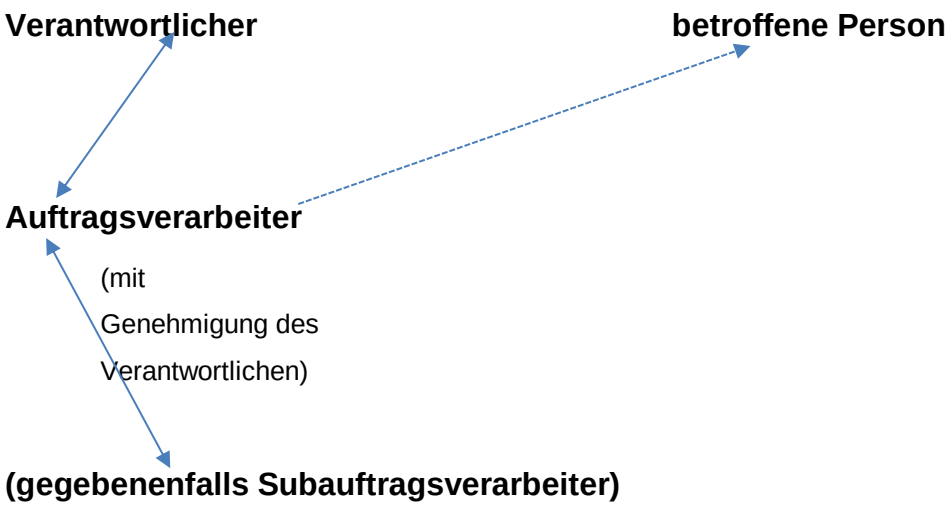
Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche bzw. können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

3.8.2 Auftragsverarbeiter (Artikel 4 Z 8):

Auftragsverarbeiter =

- eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
- Weitere Auftragsverarbeiter (Subauftragsverarbeiter) sind nur mit schriftlicher Genehmigung des Verantwortlichen möglich.
- Jeder Verantwortliche ist bei bevorstehenden Änderungen (Hinzuziehung bzw. Ersetzung) rechtzeitig zu informieren (Artikel 28).

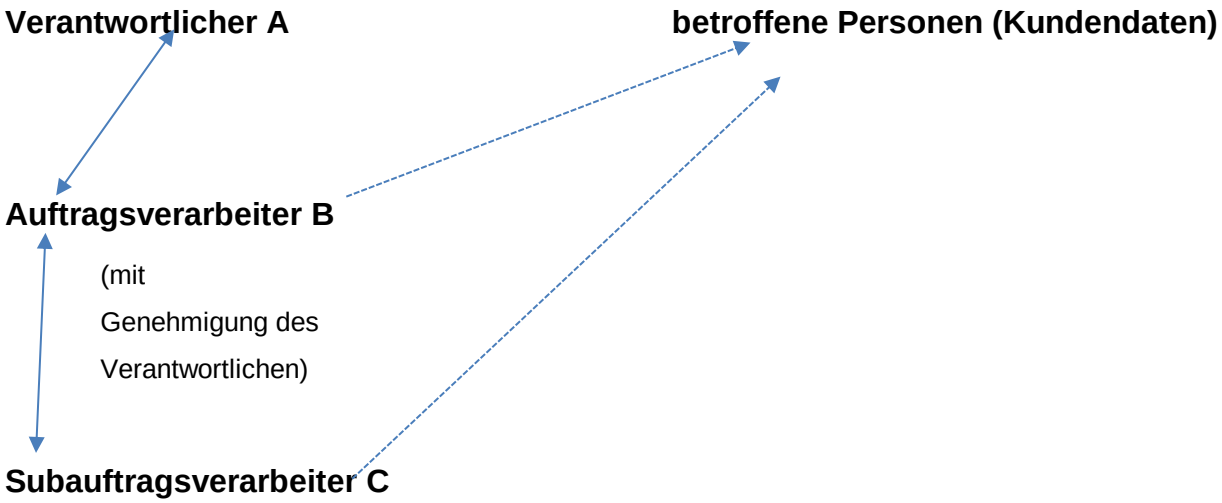
3.9 Welche Beteiligten sind zu beachten:



3.9.1 Beispiel

Das Unternehmen A beauftragt das IT-Unternehmen B mit dem Hosting von Kundendaten. B zieht hierfür zeitweise das IT-Unternehmen C zur Unterstützung heran.

Wie ist die Rollenverteilung zu beurteilen?



Anmerkung:

Bei Auftragsverarbeitungsvereinbarungen ist zu prüfen:

(i) Beschränkung der Verarbeitung auf die vom Verantwortlichen vorgegebenen Zwecke,

(ii) Einhaltung und Wahrung des Datengeheimnisses und der Datensicherheitsmaßnahmen,

(iii) Wahrung der Ansprüche der Betroffenen auf Auskunft, Richtigstellung, Information, Löschung und Portabilität und (iv) Möglichkeit des Verantwortlichen jederzeit auf die Daten zugreifen zu können.

3.10 Pflichten des Verantwortlichen

- Verantwortung für die Zulässigkeit der Datenverarbeitung (Artikel 5 ff)
- Informationspflichten (Artikel 12 ff)
- Treffen geeigneter Datensicherheitsmaßnahmen (Artikel 24 f, 32)
  - Datenschutz durch Technikgestaltung
  - Datenschutzfreundliche Voreinstellungen
- Schriftl. Vertreterbenennung bei Verantwortlichen / Auftragsverarbeitern außerhalb der EU (Artikel 27)

- Schriftl. Vereinbarung mit Auftragsverarbeiter (Artikel 28)
- Meldung und Benachrichtigung bei Datenmissbrauch (Artikel 33 f)
- Entsprechung wahrgenommener Betroffenenrechte
- Vereinbarung bei gemeinsamen Verantwortlichen (Artikel 26)
- Verzeichnis von Verarbeitungstätigkeiten (Artikel 30)
- Zusammenarbeit mit der Aufsichtsbehörde (Artikel 31)
- Datenschutz-Folgenabschätzung (Artikel 35)
- Bestellung eines DATENSCHUTZBEAUFTRAGTEN (Artikel 37 f)

3.11 Zulässigkeit der Verarbeitung

Verarbeitungsverbot mit Erlaubnisvorbehalt

- Überprüfen des sachlichen / räumlichen Anwendungsbereichs (Artikel 2 f)
- Einhaltung der allgemeinen Grundsätze (Artikel 5)
- Rechtmäßigkeit der Verarbeitung (insbesondere Artikel 6, 9, 10)

3.12 Allgemeine Grundsätze

3.12.1 Artikel 5 Absatz 1

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

b) Zweckbindung

c) Datenminimierung

d) Richtigkeit

e) Speicherbegrenzung

f) Integrität und Vertraulichkeit

Absatz 2: Der Verantwortliche ist für die Einhaltung des Absatz 1 verantwortlich und muss dessen Einhaltung nachweisen können **(Rechenschaftspflicht)!**

3.12.2 Allgemeine Grundsätze in concreto

- **Rechtmäßigkeit, Treu und Glauben, Transparenz:**

  Wurde die betroffene Person rechtzeitig und hinreichend über die Datenverarbeitung informiert?

- **Zweckbindung:**

  Besteht ein festgelegter, eindeutiger und legitimer Zweck?

- **Datenminimierung:**

  Ist die Datenverarbeitung für diesen Zweck angemessen und erheblich und auf das Notwendigste beschränkt?

- **Richtigkeit und Aktualität**

  Sind die Daten sachlich richtig und am neuesten Stand?

- **Speicherbegrenzung**

  Ist die Identifizierung der betroffenen Person für den Zweck der Verarbeitung (noch) erforderlich, bzw. sind die personenbezogene Daten bereits zu löschen?

- **Integrität und Vertraulichkeit**

  Ist für eine angemessene Datensicherheit gesorgt?

- **Rechenschaftspflicht**

  Kann der Verantwortliche die Einhaltung dieser Grundsätze nachweisen?

3.12.3 Rechtmäßigkeit (bei nicht sensiblen Daten)

3.12.3.1 Artikel 6

a) Einwilligung der betroffenen Person für einen / mehrere bestimmte Zwecke

b) Vertragserfüllung oder vom Betroffenen ausgehende (erforderliche) vorvertragliche Maßnahmen

c) Erfüllung rechtlicher Verpflichtung des Verantwortlichen

d) Schutz lebenswichtiger Interessen des Betroffenen oder eines anderen

e) Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder Ausübung öffentlicher Gewalt

f) Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, sofern Interessen des Betroffenen nicht überwiegen

4 Einwilligung „freely given“

4.1 Artikel 4 Z 11:

Einwilligung der betroffenen Person = jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogene Daten einverstanden ist;

4.1.1 Erwägungsgrund 32:

„(…) Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. (…)“

4.2 Einwilligung – Checkliste in 4 Schritten

4.2.1 Rechtsgrundlage

- Einwilligung gemäß Artikel 6 Absatz 1 lit a DSGVO
- Ausdrückliche Einwilligung gemäß Artikel 9 Absatz 2 lit a DSGVO (Verarbeitung besonderer Kategorien von Daten)

4.2.2 Artikel der Einwilligung

4.2.2.1 Freiwilligkeit der Erklärung (Artikel 7 Absatz 4; Erwägungsgründe 32, 42, 43)

- Echte oder freie Wahl; eine Verweigerung oder Zurückziehung der Einwilligung ist ohne Nachteile möglich (Erwägungsgrund 42).
- Die Erfüllung des Vertrags/Erbringung einer Dienstleistung ist nicht von der datenschutzrechtlichen Einwilligung abhängig (Erwägungsgrund 43).
- Zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten kann gesondert eine Einwilligung erteilt werden (Erwägungsgrund 43). Kein klares Ungleichgewicht zwischen betroffener Person und dem Verantwortlichen.

4.2.2.2 Konkret einzelfallbezogene Einwilligungserklärung (Erwägungsgrund 32)

- In Kenntnis der Sachlage und in informierter Weise (Erwägungsgrund 32, 42; Artikel 13).

- Auflistung der betreffenden personenbezogenen Daten (Erwägungsgrund 32).
- Nennung des für die Datenverarbeitung Verantwortlichen (Erwägungsgrund 42).
- Beschreibung der Zwecke der Datenverarbeitung (Erwägungsgrund 42).
- Auflistung aller (potentiellen) Datenempfänger (Artikel 13 lit e).
    - Hinweis auf jederzeitiges Widerrufsrecht und die Rechtmäßigkeit der Verarbeitung vor Widerruf der Einwilligung (Artikel 7 Absatz 3).
    - Unmissverständliche Willensbekundung in Form einer schriftlichen, elektronischen oder mündlichen Erklärung (Erwägungsgrund 32).
    - Eindeutig bestätigende Handlung im Sinne des Einverständnisses mit der Verarbeitung der personenbezogenen Daten (Erwägungsgrund 32).

4.2.3 Bedingungen der Einwilligung (Artikel 7)

- Nachweis der Einwilligung der betroffenen Person (Artikel 7 Absatz 1).
- Abbildung des Ersuchens um Einwilligung in verständlicher und leicht zugänglicher Form (Artikel 7 Absatz 2).
- Das Ersuchen um Einwilligung ist von anderen Sachverhalten klar unterscheidbar (Artikel 7 Absatz 2).
- Das Ersuchen um Einwilligung ist in einer klaren und einfachen Sprache formuliert (Artikel 7 Absatz 2).
- Hinweis auf das jederzeitige Widerrufsrecht der Einwilligung sowie den Umstand, dass der Widerruf die
- Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt (Artikel 7 Absatz 3).
- Der Widerruf der Einwilligung ist so einfach wie die Erteilung (Artikel 7 Absatz 3).

4.2.4 Bedingungen der Einwilligung eines Kindes (Artikel 8)

- Angebot von Diensten der Informationsgesellschaft direkt an das Kind (Artikel 8 Absatz 1).
- Vollendung des 16. Lebensjahres: Einwilligung des Kindes (Artikel 8 Absatz 1). In Österreich: Vollendung des 14. Lebensjahres.
- Ansonsten: Einwilligung des Trägers der elterlichen Verantwortung (Artikel 8 Absatz 1).
- Nachweis der Einwilligung des Trägers der elterlichen Verantwortung (Artikel 8 Absatz 2).
    - Anstrengungen zur Vergewisserung (Artikel 8 Absatz 2).
    - Angemessenheit der Maßnahmen (Artikel 8 Absatz 2).

4.2.5 ? Praxistipp:

1) Werden personenbezogene Daten bei einem Dritten (z.B. Cloud-Services) gespeichert oder bearbeitet, ist - die Einwilligung der Betroffenen vorausgesetzt - der Verantwortliche (das ist der Auftraggeber) verpflichtet, dafür Sorge zu tragen, dass der Auftragsverarbeiter die Einhaltung der datenschutzrechtlichen Vorgaben erfüllt und die Rechte der Betroffenen schützt.
2) Subauftragnehmer sind ohne explizite Zustimmung unzulässig!
3) Einbindung der Einwilligung in AGB grundsätzlich erlaubt, aber nur wenn die Zustimmung die Verarbeitung von Daten betrifft, die auch für die Vertragserfüllung benötigt werden.
4) Die Verarbeitung anderer Daten wird wohl nur auf Basis einer separaten, freiwilligen Zustimmungserklärung möglich sein.
5) Vom Verantwortlichen sind auch die Transparenz- und Informationspflichten der Artikel 12 ff (insbesondere Artikel 13 und 14) DSGVO zu beachten!
6) Datenschutzrechtliche Einwilligungen müssen demnach für ihre Wirksamkeit neben der Erfüllung der Grundprinzipien der Einwilligung nur die Voraussetzungen erfüllen, die eine Wirksamkeitsbedingung nach der DSGVO für die Einwilligung darstellen.
7) Nach dem Datenschutzgesetz 2000 erteilte Zustimmungen bleiben aufrecht, sofern sie den Vorgaben der DSGVO entsprechen, vergleiche explizit **§ 69 Absatz 9 DSG 2018**

4.3 Beispiele:

4.3.1 Fallsituation 1

Ein österreichisches Friseur-Unternehmen will automationsunterstützt personenbezogene Kundendaten verarbeiten. Beurteilen Sie die Zulässigkeit einer solchen Datenverarbeitung!

1) Sachlicher und räumlicher Anwendungsbereich der DSGVO
2) Allgemeine Grundsätze
   - Zweck (festgelegte, eindeutige, legitime), Datenkategorien (sensible, oder nicht?),
   - Datenminimierung (Rechtmäßigkeit)
   - Transparenz (Informations- und Offenlegungspflichten)
   - Integrität und Vertraulichkeit (Datensicherheit)
   - Sachliche Richtigkeit
   - Speicherbegrenzung
   - Rechenschaftspflicht

3) Rechtmäßigkeit
   - Einwilligung (jederzeitiger Widerruf möglich)
   - ausdrückliche Einwilligung bei sensiblen Daten (z.B. Speicherung von Allergien)

Weiterverarbeitung der Daten für statistische Zwecke grundsätzlich ohne weitere Rechtsgrundlage möglich (vergleiche Artikel 5 Absatz 1 lit b iVm Artikel 89)

4.3.2 Fallsituation 2:

Ein österreichisches Friseur-Unternehmen will automationsunterstützt personenbezogene Kundendaten verarbeiten. Welche Pflichten kommen gegebenenfalls auf das Unternehmen zu?

1) Beurteilung der Zulässigkeit der Verarbeitung (immer)
2) Führen eines Verzeichnisses?
3) Datenschutz-Folgenabschätzung?
4) Treffen hinreichender und geeigneter Datensicherheitsmaßnahmen (immer)
5) Benennung eines DATENSCHUTZBEAUFTRAGTEN?
6) Informations- und Meldepflichten (immer)
7) Wahrung der Betroffenenrechte (immer)

4.4 Das Führen von Verzeichnissen:

Beachte:

1) Entfall einer generellen Meldepflicht der Datenverarbeitungen (DVR).
2) Jeder Verantwortliche / Auftragsverarbeiter ist verpflichtet,
   - mit der Aufsichtsbehörde zusammenzuarbeiten und
   - dieser auf Anfrage ein gegebenenfalls Verzeichnis der Verarbeitungstätigkeiten vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können

4.5 Die Ausnahme von der Grundregel

Ein Verzeichnis ist jedenfalls ab 250 Mitarbeitern zu führen.

Darunter nur, wenn

- ein (konkretes) Risiko für die Rechte und Freiheiten der betroffenen Person

  ODER

- die Verarbeitung nicht nur gelegentlich erfolgt ODER

- sensible bzw. strafrechtsbezogene Daten verarbeitet werden.

Beachte:

Fall 2 der Ausnahmen praktisch höchstrelevant!

5 Datenschutz-Folgenabschätzung Artikel 33

1) Vor Aufnahme einer Datenanwendung, insbesondere bei Verwendung neuer Technologien, die aufgrund der Artikel, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten hat, vorab eine Abschätzung der Folgen für den Schutz personenbezogene Daten durchführen.
2) Weiters ist gemäß Absatz 2 eine Datenschutz-Folgenabschätzung auch dann erforderlich, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen durchgeführt wird ("Profiling"), biometrische Daten verwendet werden oder Videoüberwachung eingesetzt wird. Die Definition dieser Begriffe erfolgt in Artikel 4 DSGVO.
3) Ergebnisse der Abschätzung hilft geeignete Maßnahmen zu ergreifen, um eine Verarbeitung im Sinne des DSGVO zu gewährleisten.
4) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den **Rat des DATENSCHUTZBEAUFTRAGTEN** ein. (Artikel 35 Absatz 2 DSGVO)

Praxistipp:

Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) auch noch nach dem Inkrafttreten beachten! (StF: BGBl. II Nr. 312/2004)

5.1 Datenschutz-Folgenabschätzungen in einem Schrittesystem

5.1.1 Systematische Beschreibung der Verarbeitung und Zwecke, sowie der Interessen:

- Zweck der Datenanwendung, Betroffenenkreise, Datenarten mit Angaben über ihre Sensibilität, Übermittlungsempfänger nach EWR- und Drittstaaten, Dauer der Speicherung, Löschfristen.
- Ziel dieser Beschreibung ist es, ein möglichst umfassendes und vollständiges Bild der Datenanwendung zu erhalten.

Bewertung der Notwendigkeit und Verhältnismäßigkeit

5.1.2 ? Bewertung der Risiken durch Risikoanalyse:

- Diese beginnt mit der Ermittlung jener potenziellen Risiken der Datenanwendung, welche der Einhaltung der in der DSGVO enthaltenen Ziele entgegenstehen;

- z.B. Gewährleistung der Datenqualität, Rechtmäßigkeit der Verarbeitung, Einhaltung der Informationsverpflichtungen sowie des Auskunfts-, Richtigstellungs- und Löschungsrechts, Einhaltung des Widerspruchsrechts, Beachtung der Sicherheit der Verarbeitung, Einhaltung der Meldeanforderungen, etc.

5.1.3 Geplante Kontroll- und Abwehrmaßnahmen (inkl. Garantien, Sicherheitsvorkehrungen und Verfahren):

- In dieser Phase sind Überlegungen anzustellen, wie die festgestellten Datenschutzrisiken durch Kontrollmaßnahmen minimiert werden können. Diese können technischer oder nichttechnischer Natur sein, wie –
- z.B. Maßnahmen zur Datenminimierung, Vorgaben für die Speicherung und Löschung der personenbezogenen Daten, Einsatz von Verschlüsselungsverfahren.

5.2 Praxistipp für die Ausarbeitung einer Folgenabschätzung

- Als Beispiel für die Umsetzung dieser Forderungen könnte die derzeit im DSG 2000 in der Standard- und Musterverordnung 2004 (StMV 2004) angeführten Standard-und Musteranwendungen herangezogen werden.
- Konkrete Beispiele, in welchen Fällen in Zukunft eine Datenschutz-Folgenabschätzung vorzunehmen sein wird, sind Projekte, bei welchen die RFID-Technik eingesetzt wird oder die als Big Data-Projekte eingestuft werden können, bzw. wenn es sich um solche Datenanwendungen handelt, die in Kapitel IX DSGVO angeführt sind, wie die Verarbeitung personenbezogene Daten für Gesundheitszwecke (Artikel 81) oder die Verarbeitung genetischer Daten (Artikel 81a); vergleiche dazu www.bfdi.bund.de/SharedDocs/Publikationen/RFID_PIA.de.html
- ? Gemäß Artikel 33 Absatz 1a berät der DATENSCHUTZBEAUFTRAGTEN - falls ein solcher ernannt sein sollte – den Auftraggeber bei der Durchführung einer Datenschutz-Folgenabschätzung. Die nationale Aufsichtsbehörde erstellt eine Liste mit jenen Datenanwendungen, für die eine Datenschutz-Folgenabschätzung vorzunehmen ist (Positivliste, Artikel 33 Absatz 2a); gemäß Absatz 2 b kann sie auch eine Liste über jene Datenanwendungen erstellen, für die keine Datenschutz-Folgenabschätzung angestellt werden muss (Negativliste).
- In Bezug auf den Einsatz von Smart Metering hat die EU-Kommission am 10.10.2014 eine Empfehlung „über das Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme“ (2014/724/EU) veröffentlicht. Dieser Empfehlung sind zwei Stellungnahmen der Artikelikel-29-Datenschutzgruppe (22.04. 2013, WP 205; 4. 12. 2013, WP 209) vorangegangen. Auch dieses Muster kann für die Vornahme einer Datenschutz-Folgenabschätzung herangezogen werden; vergleiche

dazu https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smArtikel_grids_forces.pdf

5.3 Datenschutz-Folgenabschätzung - Zusammenfassung

Erforderlich, wenn…

1) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
2) umfangreiche Verarbeitung sensibler oder strafrechtsbezogener Daten
3) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

5.4 Datensicherheit

Durch technische und organisatorische Maßnahmen ist ein angemessenes Schutzniveau zu gewährleisten.

5.4.1 Betrifft Verantwortliche:

- Artikel 24 Absatz 1: Treffen geeigneter technischer und organisatorischer Maßnahmen
- Artikel 25: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung

Achtung: Die Maßnahmen müssen bereits zum Zeitpunkt der Festlegung der Mittel sowie zum Zeitpunkt der Verarbeitung feststehen!

5.4.2 Betrifft Verantwortliche und Auftragsverarbeiter:

Artikel 32: Sicherheit und Verarbeitung

Dabei sind zu berücksichtigen:

- Stand der Technik
- Implementierungskosten
- Artikel, Umfang, Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere eines Risikos

5.5 Data Breach Notification

Bei einer Verletzung der Sicherheit, die zur Vernichtung, Verlust, Veränderung, unbefugten Offenlegung oder unbefugten Zugang zu personenbezogene Daten führt, ist unverzüglich (spätestens binnen 72 Stunden) eine Meldung mit folgendem Inhalt an die Datenschutzbehörde - und bei hohem Risiko auch direkt an die Betroffenen - zu erstatten:

- Beschreibung der Artikel der Verletzung
- Angabe von Kategorien und Zahl der Betroffenen und Daten
- Name und Kontaktdaten des DATENSCHUTZBEAUFTRAGTEN
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen oder vorgeschlagenen Gegenmaßnahmen

5.6 Informationspflichten

Beachte:

- DVR gibt es nur mehr bis 31.12.2019; Meldungen sind bis 25.05.2018 noch möglich!
- Verzeichnis von Verarbeitungstätigkeiten und
- gegebenenfalls Datenschutz-Folgenabschätzung
- „Eigenverantwortung“ des Unternehmens

5.6.1 Allgemeines zur Informationspflicht (Artikel 12)

vollständig, präzise, transparent, verständlich, leicht zugänglich, in klarer und einfacher Sprache, schriftlich oder in anderer Form (auch elektronisch möglich)

5.6.2 Informationspflicht bei Erhebung beim Betroffenen (Artikel 13)

Werden künftig Daten bei der betroffenen Person selbst erhoben, hat der Verantwortliche ihr nach Artikel 13 DSGVO (zum Zeitpunkt der Erhebung dieser Daten) insbesondere folgendes mitzuteilen, wenn und soweit sie darüber nicht schon verfügt:

- Name und Kontaktdaten des Verantwortlichen (z.B. RA, WT, Heimträger) und gegebenenfalls des DATENSCHUTZBEAUFTRAGTEN,
- die Verwendungszwecke und die Rechtsgrundlage für die Verarbeitung,

- wenn Rechtsgrundlage eine Interessenabwägung ist, die entsprechenden berechtigten Interessen,
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

5.6.2.1 Beispiel:

Ein potentieller neuer Heimbewohner erscheint zu einem Erstgespräch und füllt mit Vertretern der Heim- und Pflegeleitung einen Fragebogen zur Abklärung seiner Pflegebedürftigkeit aus. Bei dieser Gelegenheit sind ihm die obigen Informationen mitzuteilen.

5.6.3 Informationspflicht bei Erhebung nicht beim Betroffenen (Artikel 14):

- Namen und Kontaktdaten des Verantwortlichen und des DATENSCHUTZBEAUFTRAGTEN,
- die Verwendungszwecke und die Rechtsgrundlage für die Verarbeitung,
- die **Kategorien** personenbezogene Daten, die verarbeitet werden,
- gegebenenfalls die Empfänger oder Kategorien von Empfängern,
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln.

Eine **Ausnahme** von dieser Informationspflicht nach Artikel 14 DSGVO besteht dann, wenn die Erlangung oder Offenlegung in Rechtsvorschriften ausdrücklich geregelt ist oder die Daten einer berufsrechtlichen Verschwiegenheitspflicht unterliegen (Berufsgeheimnis), was bei RA oder z.B. im Heim- und Pflegerecht regelmäßig der Fall sein wird.

5.6.3.1 Beispiel:

Die Heimleitung bekommt von der Gemeinde die Bewilligung eines Zuschusses zu den Heimkosten für einen potentiellen neuen Bewohner zur Kenntnis übermittelt. Nach den betreffenden landesgesetzlichen Heimvorschriften sind alle Mitarbeiter des Heimträgers zur Geheimhaltung verpflichtet. Eine gesonderte Informierung des Heimbewohners über den Erhalt der Zuschussbewilligung ist somit nicht erforderlich.

5.7 Sonstige Informationsrechte

- **Mitteilungspflicht bei Berichtigung oder Löschung** (Artikel 19)
- **Meldung eines Datenmissbrauchs** an die Aufsichtsbehörde (Artikel 33)
- Benachrichtigung des Betroffenen von einem Datenmissbrauch (Artikel 34)
- **Information der Aufsichtsbehörde und des Betroffenen bei Datenübermittlungen in Drittländer** nach Artikel 49

5.7.1 Beispiel:

Im Rahmen einer Bestellung in einem Online-Shop (S) muss sich der Käufer (K) einen Account unter Angabe personenbezogene Daten anlegen, um die Bestellung auch durchführen zu können. Welche Informationen muss S diesbezüglich aus datenschutzrechtlicher Sicht anführen?

Informationspflicht bei Erhebung der Daten beim Betroffenen (Artikel 13) in der Regel:

- Name des Verantwortlichen,
- Kontaktdaten des DATENSCHUTZBEAUFTRAGTEN,
- Zweck und Rechtsgrundlage (bei Einwilligung auch Hinweis auf jederzeitige Widerrufsmöglichkeit),
- Übermittlungsempfänger,
- Transfer ins Ausland,
- Speicherdauer,
- Hinweis über Betroffenenrechte und Beschwerdemöglichkeit an die Aufsichtsbehörde

5.8 Weitere Betroffenenrechte

5.8.1 Informationsrechte (Artikel 12-14)

5.8.1.1 Recht auf Auskunft (Artikel 15) betrifft:

die Verarbeitungszwecke,

die Kategorien personenbezogene Daten, die verarbeitet werden,

die Empfänger, denen die Daten offengelegt werden,

die geplante Speicherdauer oder zumindest die Kriterien dafür,

das Bestehen eines Rechts auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts,

das Bestehen eines Beschwerderechts bei der Datenschutzbehörde.

5.8.1.2 Recht auf Berichtigung gemäß Artikel 16 (Darlegungs- und Beweislast liegt größtenteils beim Betroffenen)

5.8.1.3 Recht auf Löschung/Vergessen (Artikel 17) bei folgender Annahme:

Beispiele

- Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

- Die Daten wurden unrechtmäßig verarbeitet.
- Die Löschung ist aufgrund einer gesetzlichen Vorschrift erforderlich.
- Die Verarbeitung zur Erfüllung einer gesetzlichen Verpflichtung oder öffentlichen Aufgabe ist notwendig (so wie bei der Pflege- und Betreuungsdokumentation, die nach der Beendigung des Heimaufenthalts des betreffenden Heimbewohners in der Regel zehn Jahre aufzubewahren ist) oder
- die Datenverarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen z.B. der sozialen Einrichtung ist notwendig.

5.8.1.4 Recht auf Einschränkung der Verarbeitung (Artikel 18):

- Die Richtigkeit der Daten wird bestritten.
- Die Verarbeitung ist unrechtmäßig, die betroffene Person hat aber die Löschung der Daten abgelehnt und stattdessen die Einschränkung ihrer Nutzung verlangt.
- Die Daten werden vom Verantwortlichen nicht mehr für die Zwecke der Verarbeitung benötigt, die betroffene Person braucht sie aber noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die betroffene Person hat Widerspruch gegen die Datenverarbeitung eingelegt.

Beachte:

Als Konsequenz der eingeschränkten Verarbeitung dürfen die Daten nur mehr gespeichert bleiben (im System ist dies entsprechend zu kennzeichnen). Anderes gilt nur dann, wenn z.B. die betroffene Person in die weitere Verarbeitung einwilligt.

5.8.1.5 Recht auf Datenübertragbarkeit (Artikel 20):

Unklar ist derzeit, wie genau eine allfällige Übertragung ausgestaltet sein muss, die DSGVO selbst spricht von einem strukturierten, gängigen und maschinenlesbaren Format!

Beispiel:

Damit soll die betroffene Person die Daten ohne zusätzlichen Aufwand weiterverwenden können, z.B. dann, wenn sie einen Cloud-Dienst in Anspruch nimmt und in der Folge den Cloud-Dienstleister wechselt. In diesem Fall wäre der „alte“ Cloud-Dienstleister, der die Daten in der Cloud lagert, verpflichtet, die Daten an den „neuen“ Cloud-Dienstleister zu übertragen.

Allerdings steht dieses Recht auf Datenübertragbarkeit nur unter bestimmten Voraussetzungen zu, unter anderem muss die Übertragung technisch möglich sein und die betroffene Person muss in die Datenverarbeitung eingewilligt haben.

5.8.1.6 Widerspruchsrecht (Artikel 21)

Nach Artikel 21 DSGVO hat eine betroffene Person das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzulegen, und zwar dann, wenn die Daten

- entweder zur Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen, verarbeitet werden (Artikel 6 Absatz 1 lit e DSGVO) oder
- aufgrund von berechtigten Interessen des Verantwortlichen oder eines Dritten verarbeitet werden (Artikel 6 Absatz 1 lit f DSGVO).
- Kann der Verantwortliche keine zwingenden schutzwürdigen Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder
- dient die Verarbeitung nicht der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, darf der Verantwortliche die betreffenden personenbezogenen Daten nicht mehr verarbeiten.

Beachte:

Die Rechte auf Auskunft, Berichtigung, Löschung und Widerspruch stehen bereits nach dem DSG 2000 zu. Die Erfahrung hat gezeigt, dass bis dato nur das Recht auf Auskunft von praktischer Bedeutung war.

5.9 Modalitäten bei Rechtsausübung

1) Übermittlung von Daten in präziser, transparenter, verständlicher und leicht vergänglicher Form in einer klaren und einfachen Sprache;
2) Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. (Mündlich auf Verlangen des Betroffenen möglich, sofern die Identität der betroffenen Person nachgewiesen wurde);
3) Informationen (z.B. bei Auskunftsbegehren) sind unverzüglich, längstens aber binnen 1Monats nach Eingang des Antrags zur Verfügung zu stellen;
4) Informationen, Mitteilungen und Maßnahmen (insbesondere Artikel 13-22) sind unentgeltlich zu erteilen (Ausnahme: exzessive Anträge);
5) Musterinformationsschreiben

5.9.1 Beispiel:

Sie bekommen unaufgefordert postalische Werbung zugesandt und möchten nun unter anderem wissen, wie der Absender an Ihre Daten gelangt ist und auf welcher Rechtsgrundlage

die Daten verarbeitet werden, um die Zusendungen zu stoppen und ggf. weitere rechtliche Schritte einleiten zu können.

WAS werden Sie WIE tun?

- Auskunftsbegehren (Art 15)
- Widerruf etwaiger Einwilligung oder Löschungsbegehren bzw. Widerspruchsbegehren
- Beschwerde bei DATENSCHUTZBEAUFTRAGTEN bzw. Klage bei Landesgericht

  Beachte:

  Dabei können sie sich künftig durch Non-Profit Organisationen vertreten lassen. Siehe dazu - aktuell: www.noyb.eu

Beachte:

1) Darüber hinaus hat jede Person, der wegen eines Verstoßes gegen die DSGVO oder gegen das DSG ein materieller oder immaterieller Schaden entstanden ist, - so wie bereits bisher - Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
2) Strafrechtliche Verantwortung?

5.10 Ausblick DSG 2018

- Das Grundrecht des § 1 DSG verbleibt (Schutz für juristische Personen?)
- Kompetenzprobleme bleiben bestehen
- Verarbeitung strafrechtlich relevanter Daten durch Private (§ 4 Absatz 3 DSG)
- Selbstständige Einwilligung von Kindern bei Diensten der Informationsgesellschaft ab dem 14. Lebensjahr (§ 4 Absatz 4)
- DATENSCHUTZBEAUFTRAGTEN – Aussageverweigerungsrecht (§ 5 Absatz 2)
- Datengeheimnis (§ 6)
- Archivzwecke, wissenschaftliche Forschung, Statistik (§ 7)
- Zurverfügungstellung von Adressen (§ 8)
- Medien (§ 9)
- Katastrophenfall (§ 10)
- Beschädigungskontext – ArbVG iVm Art 88 DSGVO (§ 11
- Bildverarbeitung (§§ 12, 13)
- Datenschutzrat (§§ 14-17)
- Datenschutzbehörde (§§ 18-23)
- Rechtsbehelfe, Haftung, Sanktionen (§§ 24-30)
- Beschwerde an DATENSCHUTZBEAUFTRAGTE / Klage an Landesgericht nur bei Schadenersatz

- Keine Geldbußen für Behörden / öffentliche Stellen
- Aufsichtsbehörde nach RL (EU) 2016/680 (§§ 31-35)
- Verarbeitung strafrechtlich relevanter Daten durch Behörden (RL (EU) 2016/680) (§§ 36-61)
- Strafbestimmungen (§§ 62, 63)
- Schlussbestimmungen (§§ 64-70)

5.11 Die neuen Herausforderungen – Ausblick/Time is running out

- Die Verpflichtung, technische Maßnahmen zu setzen, die Datenschutz fördern, erfordert im Zweifel, die Verarbeitung, das heißt insbesondere auch die Speicherung, nach Grundlage und Maßgabe der unterschiedlichen Verwendungszwecke zu strukturieren. Dies ist nicht nur aus Gründen der Datensparsamkeit, sondern auch im Hinblick auf die Reduktion von immanenten Problemen bei der Handhabung unstrukturierter Daten und der Vermeidung von Doppelgleisigkeiten in der Datenverarbeitung empfehlenswert.
- Unternehmensintern und im Klienten-/Kundenverkehr sind Prozesse zu etablieren, die eine entsprechende Umsetzung tatsächlich ermöglichen, wobei hiervon auch die (standardisierte) Beantwortung von Anforderungen von Betroffenen (Rechtauf Löschung, Berichtigung, Datenübertragung,...) umfasst ist. Das kann IT-Systeme, Mitarbeiterschulungen, standardisierte Prozesse im Kundenverkehr oder Ähnliches inkludieren
- Regelmäßige, gezielte Überprüfungen des Datenbestandes und des Vorhandenseins der Berechtigung, Daten tatsächlich zu verarbeiten, sind (eventuell automatisiert) notwendig. Sind Daten zu löschen oder zu berichtigen, sind Strukturen und Systeme vorzusehen, die dies datenschutzrechtskonform (beachte: Backups stellen eine Datenverarbeitung dar) ermöglichen.
- Idealerweise werden personenbezogene Daten derart verarbeitet, dass einzelne Aufbewahrungspflichten und -möglichkeiten strukturiert erfüllt werden können, während eine spezifische Datenlöschung oder -berichtigung unter Wahrung der Datenintegrität des Gesamtdatenbestandes möglich ist.
- ? Ihr Unternehmen als Dienstleister ist mit den internen Prozessen - und damit auch Problemfeldern - ihrer Kunden möglicherweise eng vertraut. Die Kunden – im zulässigen Rahmen - auf mögliche Problemfelder, insbesondere in den Bereichen Personal, Buchhaltung & Lohnverrechnung, IT, AGB und Musterverträge hinzuweisen, ebenso auf allfällige Aspekte der Übertragung z.B. von Finanzdaten an Dritte (z.B. Cloud- Anbieter) und sie ggf. bei der Umsetzung zu unterstützen, sollte selbstverständlich sein.

- Datenschutz ist ein Qualitätsmerkmal mit Zukunft.
- Nach dem noch geltenden, alten Regime sind neue Prozesse vor Inbetriebnahme bei der Datenschutzbehörde zu melden. Darüber hinaus bestehen für risikogeneigte Datenanwendungen - also besonders bei der Verwendung von sensiblen oder strafrechtlich relevanten Daten - zusätzliche behördliche Vorabprüfungen und bei Datentransfers ins EU-Ausland das Erfordernis einer Genehmigung. De facto haben jedoch nur die wenigsten Unternehmen - mit Ausnahme solcher aus dem regulierten Umfeld (Bankwesen, Versicherungen und Pharmaunternehmen) - ein vollständiges Datenverarbeitungsregister (DVR).
- ? Mit Anwendbarkeit der DSGVO müssen jedoch die Prozesse statt der Schleife über die Behörde künftig umfassend intern auf ihre datenschutzrechtliche Zulässigkeit geprüft, gegebenenfalls eigenverantwortlich umgesetzt und dokumentiert werden. Es geht damit weg von der Freizeichnung durch die Behörde hin zu einer eigenverantwortlichen Entscheidung, die ex post im Anlassfall nachgeprüft wird.
- Der Dreh- und Angelpunkt der DSGVO ist dabei das nach Art 30 zu führende Verzeichnis der Verarbeitungstätigkeiten aus dem sich ein lückenloser Überblick über sämtliche Datenverarbeitungen und -ströme ergibt. Neben den vorhandenen DVR Meldungen und Überleitung der bisher von der Meldepflicht ausgenommenen Standard- und Musteranwendungen der StMV ist daher in der Praxis eine umfassende Datenerhebung erforderlich.

6 Verarbeitungsverzeichnis

6.1 empfohlener Mindestinhalt:

- Name und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Beschreibung der Kategorien der Betroffenen und der Daten
- Kategorien der Empfänger
- Beschreibung der geeigneten Garantien bei Übermittlungen in Drittländer
- Fristen für Löschung von Daten
- Beschreibung der technischen und organisatorischen
- Sicherheitsmaßnahmen

6.2 Prioritäten richtig setzten:

1) Erstellung des Verfahrensverzeichnisses
2) Erweiterung bestehender Dienstleistervereinbarungen zu Auftragsverarbeitungsvereinbarungen
3) Überarbeitung etwaiger Einwilligungserklärungen
4) Erstellung der verpflichtenden Informationsunterlagen für Betroffene
5) Überarbeitung bestehender Datenschutz-Bedingungen/-Erklärungen, etc.
6) Erstellung der Datenschutz-Folgenabschätzungen
7) Vorbereitung auf die Data Breach Notification
8) Umsetzung der erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen
9) Vorbereitung auf die Erfüllung der erweiterten Betroffenenrechte

7 Literaturverzeichnis

Berauer/Jahnel. (2017). *das neue Datenschutzrecht.* Jan Sramek Verlag.

dejure.org. (kein Datum). *https://dejure.org/gesetze/GRCh/8.html.*

Feiler. (2017). *Gesetzbuch Datenschutzrecht.* Verlag Österreich.

Heißl. (2017). *Persönlichkeitseingriffe im Internet.* Verlag Österreich.

https://www.datenschutz-grundverordnung.eu/grundverordnung/art-37-ds-gvo/. (2018). *EU-Datenschutzgrundverordnung.* Von Art.37 – EU-DSGVO – Benennung eines Datenschutzbeauftragten. abgerufen

https://www.datenschutz-grundverordnung.eu/grundverordnung/art-39-ds-gvo/. (2018). *Eu-Datenschutz.* Von Art.39 – EU-DSGVO – Aufgaben des Datenschutzbeauftragten. abgerufen

https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40095483. (2018). *Bundeskanzleramt.* Von Besondere Fälle der Verantwortlichkeit. abgerufen

https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig. (2018). *Bundesgesetzblatt.* Von Datenschutz Anpassungsgesetz. abgerufen

Knyrim. (2015). *Datenschutzrecht 3.* Manz Verlag.

Pachinger/Peham. (2017). *Datenschutz-Audit² .* LexisNexis.

Verlag, M. (2018). *Datenschutz konkret.* Manz Verlag.

Verlag, W. (kein Datum). *Datenschutz Praxis.* Weka Verlag.

WKO. (2018). *WKO - ePrivacy-Verordnung.*