Rechtsinfo

DSGVO - Grundsätze, Rechte & Verpflichtungen

Inhaltsverzeichnis

1. Ist wirklich alles neu?

Viele Rechte und Pflichten sind bereits jetzt im nationalen **Datenschutzgesetz** (DSG 2000) vergleichbar geregelt, allerdings mit milderen Strafen versehen. Darüber hinaus spielt der Schutz von Daten in weiteren Gesetzen eine Rolle – z.B. genießen Persönlichkeitsrechte über das **ABGB**, **StGB** oder **Mediengesetz** einen hohen Schutz, neben der generellen Verwertung von Fotos ist der Bildnisschutz von Personen im **Urheberrecht** normiert und die zulässige Nutzung von E-Mail-Adressen wurde in den letzten Jahren im **Telekommunikationsgesetz** mehrmals verschärft (detaillierte Rechtsinfos zu den Themen Urheberrecht, elektronische Werbung, etc. sind über die Website abrufbar).

2. Auf welchen Rechtsgrundlagen basiert Datenschutz?

a. Die **EU-Datenschutz-Grundverordnung** (DSGVO) ist ab 25.05.2018 das umfassende und direkt anwendbare Regelwerk und ist hier abrufbar.

b. Das nationale **Datenschutzgesetz** bleibt in einer novellierten und verschlankten Version bestehen und tritt mit 25.05.2018 in Kraft.

c. Die **ePrivacy-Verordnung** stellt eine Ergänzung zur DSGVO dar und sieht auch in der aktuellen Version (Oktober 2017) einschneidende Regelungen für die elektronische Kommunikation und den Einsatz von Cookies, Tracking-Tools, etc. vor. So soll laut aktuellem Entwurf der Einsatz von Cookies überwiegend von der Zustimmung der User abhängig gemacht werden, Websiten trotz abgelehnter Trackings zugänglich bleiben und Endgeräte nur mehr mit hohen datenschutzrechtlichen Voreinstellungen ausgeliefert werden. Ob diese Punkte nun den weiteren Abstimmungen auf EU-Ebene standhalten oder erneut überarbeitet werden, wird sich ebenso zeigen, wie das ursprünglich geplante Inkrafttreten mit 25.05.2018.

3. Was regelt die DSGVO?

In den 99 Artikeln und 173 Erwägungsgründen geht es kurz zusammengefasst um den **Schutz von personenbezogenen Daten natürlicher Personen**, denen vermehrt Rechte eingeräumt werden, während die Datenverarbeiter unter Androhung hoher Strafen verstärkt

in die Pflicht genommen werden. Folgende Grundsätze / Schwerpunkte leiten sich daraus ab:

a. Verantwortliche müssen umfassend **informieren**;
b. Daten dürfen ausschließlich auf Basis einer **Rechtsgrundlage** verarbeitet werden;
c. Für Datenverarbeitungen sind konkrete **Zwecke** zu definieren;
d. Betroffene können **Auskunfts-, Widerspruchs-, Widerrufs-, Löschungsrechte** geltend machen und Verantwortliche müssen darauf reagieren;
e. Verantwortliche haben für einen ausreichenden **Schutz** der Daten sowie für technische und organisatorische **Sicherheitsmaßnahmen** zu sorgen;
f. Verantwortliche und Auftragsverarbeiter haben ein **Verarbeitungsverzeichnis** zu führen, das auf Anfrage der Datenschutzbehörde vorzulegen ist;
g. Unter bestimmten Voraussetzungen ist ein **Datenschutzbeauftragter** zu ernennen;
h. Datenschutzverletzungen sind binnen 72 h an die **Datenschutzbehörde** zu melden.

4. Wen betrifft die DSGVO?

Grundsätzlich **jeden**, der Daten **verarbeitet**, also erhebt, speichert, offenlegt, übermittelt, bearbeitet, löscht, etc. und natürlich auch jene, deren Daten verarbeitet werden. Die DSGVO definiert folgende „Hauptakteure“:

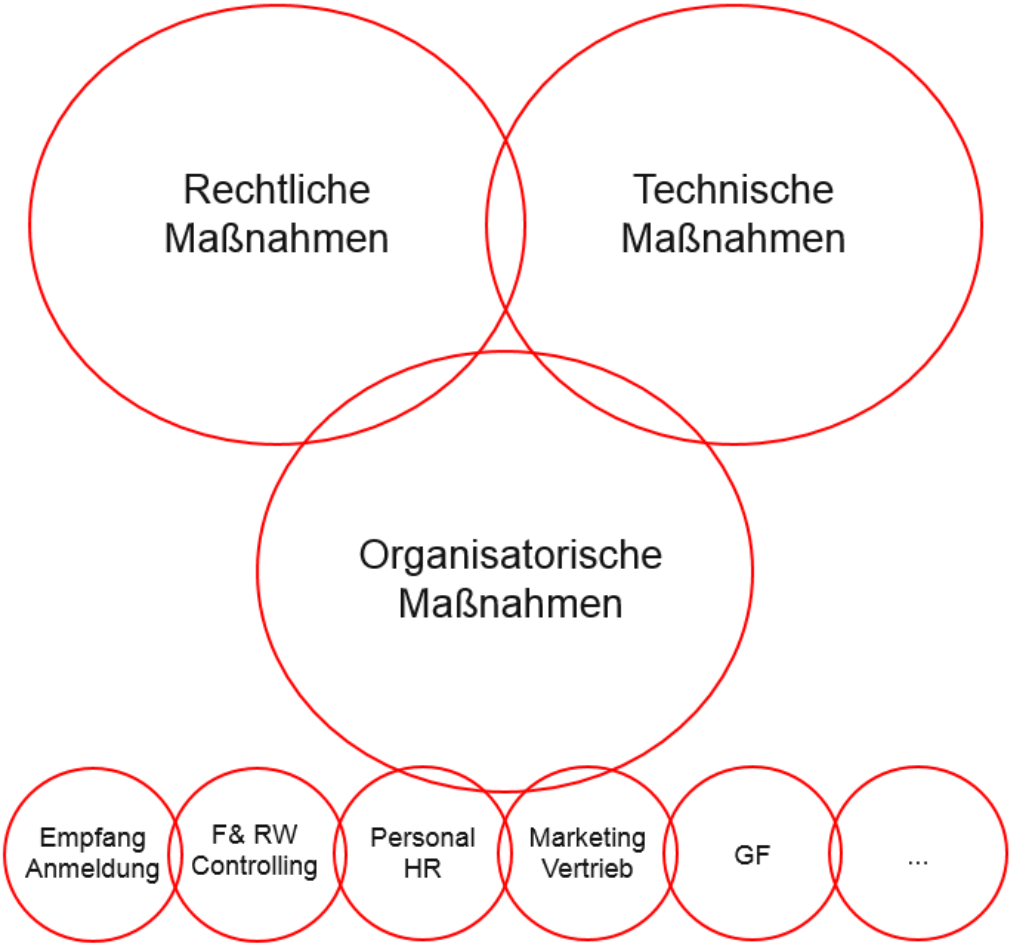
a. **Betroffene**: Natürliche Personen, deren Daten verarbeitet werden – z.B. Kunden, Lieferanten, Geschäftspartner, Gäste, Mitarbeiter, etc.

b. **Verantwortliche** (vormals Auftraggeber): Natürliche oder juristische Personen, Behörden, öffentliche Stellen, die personenbezogene Daten verarbeiten.

c. **Auftragsverarbeiter** (vormals Dienstleister): Natürliche oder juristische Personen, Behörden, öffentliche Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten – z.B. ausgelagerte Lohn- / Gehaltsverrechnung, Mailings, etc.

5. Alles nur Recht?

Neue Gesetze, Richtlinien oder Verordnungen rufen natürlich zuerst den Rechtsbereich auf den Plan. Zur Einhaltung der in der DSGVO definierten Rechte und Pflichten bedarf es allerdings technischer und organisatorischer Maßnahmen, die je nach Unternehmensgegenstand, Organisation oder Abteilung variieren können und sowohl Mitarbeiter als auch Führungskräfte betreffen.



6. Was sind personenbezogene Daten?

Aufgrund des digitalen Fortschritts und der zunehmenden Möglichkeiten Informationen über Personen zu generieren wurde auch der Begriff „Daten“ neu und umfassender definiert. Somit fallen sämtliche **nicht anonymisierte** Daten, die einen **Personenbezug** herstellen könn(t)en, darunter - beispielsweise:

- Name, Adresse, Geburts-, Bankdaten, Sozialversicherungsnummer
- IP-Adresse, Online-Kennungen, Cookies
- Buchungs-, Einkaufsverhalten, Interessen, Bewegungsdaten
- physische, psychische, genetische, wirtschaftliche, kulturelle oder soziale Merkmale
- sensible Daten wie Gesundheitsdaten, biometrische Daten, rassische / ethnische Herkunft, Religions-, Gewerkschaftszugehörigkeit, politische Meinungen

7. Worauf haben Verarbeiter zu achten?

7.1. Information / Transparenz

Daten in geheimer Mission ermitteln und verwerten? Besser nicht – siehe Punkt 7.8. Vielmehr sind Verantwortliche verpflichtet, sämtliche Informationen über die Verwertung von Daten transparent zu halten und darzulegen, welche Daten zu welchen Zwecken auf welcher Grundlage verarbeitet, wie lange gespeichert, ob sie an Dritte weitergegeben werden etc.

7.2. Rechtmäßige Verarbeitung

Daten ohne Rechtsgrundlage verarbeiten? Besser auch nicht – siehe Punkt 7.8. Somit ist zu prüfen, ob die Daten zumindest eine dieser Bedingungen erfüllen:

a. Rechtliche Verpflichtung / Gesetzesgrundlage?

Z.B. arbeits-, steuerrechtliche Bestimmungen, Meldegesetz, etc.

b. Vertragsgrundlage?

Z.B. Kunden-, Lieferantenverträge, Kooperationsvereinbarungen, Dienstverträge etc.

c. Berechtigtes Interesse?

Diese undefinierte Begrifflichkeit könnte bei ausführlicher Begründung ein Argument für die Datenverarbeitung in den Bereichen Marketing / Werbung sein, falls keine gesetzliche oder vertragliche Grundlage gegeben ist. Mangels praktischer Erfahrungen und gerichtlicher Entscheidungen wirft sie allerdings derzeit (auch seitens der Experten-Experten) große Fragen auf und bringt eine gewisse Unsicherheit mit sich.

Es geht um eine Abwägung der Interessen des Verantwortlichen einerseits und der Geheimhaltungsinteressen seitens der betroffenen Person andererseits. Wichtig ist zu definieren, welche konkreten Daten der Verantwortliche ermitteln möchte, ob diese auch anonym verwertet werden können, welche Ziele verfolgt werden, ob ein Vertrag vorliegt und ev. daraus entsprechende Interessen abgeleitet werden können, etc. Gleichzeitig ist zu prüfen, ob bzw. welche Rechte des Betroffenen eingeschränkt werden und in welchem Verhältnis diese zum Vorhaben des Verantwortlichen stehen.

Jedenfalls ist zu bedenken, dass den Betroffenen ein Widerspruchsrecht einzuräumen ist und im Falle der Geltendmachung die Daten grundsätzlich nicht mehr verarbeitet werden dürfen.

d. Einwilligung?

Falls weder a. noch b. noch c. eine Möglichkeit zur Verarbeitung einräumen und auch kein öffentliches oder lebensnotwendiges Interesse vorliegt, bleibt nur mehr die Möglichkeit die Zustimmung einzuholen. Dies sollte jedenfalls erst als letzte Variante in Frage kommen, da für eine Einwilligung bereits im Vorfeld ausreichende Informationen erforderlich sind und v.a. weil sie jederzeit widerrufen werden kann.

7.3. Zweckgebundene Verarbeitung

Daten dürfen nur für einen bestimmten und konkret definierten Zweck verarbeitet werden. So dürfen beispielsweise Kundendaten nicht „automatisch“ für diverse Werbezwecke werden oder Meldedaten ausschließlich für Meldezwecke erhoben und übermittelt werden.

Eine vergleichbare Regelung gilt bereits seit Jahren für die Zusendung von Newsletter. Aus diesem Grund dürfen E-Mail-Adressen aus unverbindlichen Anfragen auch nur für die Anfragebeantwortung verwendet und nicht in einen Newsletter-Verteiler aufgenommen werden. (Diese Thematik beschäftigte auch den VwGH – Details dazu in einer gesonderten Rechtsinfo zur elektronischen Werbung).

7.4. Sicherheit / Schutz / Speicherung des Datenbestandes

Verantwortliche / Auftragsverarbeiter haben neben den korrekten Verarbeitungsvorgängen auch für die entsprechende Datensicherheit zu sorgen. Sie müssen gewährleisten, dass der

Datenbestand ordnungsgemäß geschützt ist, entsprechende Berechtigungen für Zutritt und Zugriff vorliegen, Verlust, Zerstörung von Daten oder Einflüsse von außen abgewehrt werden können und auch Sicherheitsstandards, Kosten für die Implementierung etc. berücksichtigt werden.

7.5. Bearbeitung von Anträgen

Verantwortliche müssen Betroffene über ihre Rechte informieren und an sie gerichtete Anträge innerhalb 1 Monats bearbeiten. Im Falle eines Auskunftsbegehrens ist konkret darzulegen, welche Daten, für welche Zwecke, auf welcher Grundlage etc. verwendet werden. Bei Anträgen auf Widerspruch / Widerruf und insbesondere bei Löschungsanträgen ist zu prüfen, ob gesetzliche Aufbewahrungsfristen (UGB, BAO, arbeitsrechtliche Vorschriften, etc.), laufende Verfahren, bestehende Vertragsgrundlagen etc. vorliegen, die zum Zeitpunkt des Antrages einer Löschung entgegenstehen.

7.6. Dokumentation der Verarbeitung / Verarbeitungsverzeichnis

Laut DSGVO sind Verantwortliche / Auftragsverarbeiter ab 250 Mitarbeiter zur Führung eines Datenverarbeitungsverzeichnisses verpflichtet. Jene mit weniger als 250 Mitarbeiter „nur“ dann, wenn die Verarbeitung „nicht nur gelegentlich“ erfolgt oder sensible Daten beinhaltet. Da schon die Personalverwaltung sensible Daten verarbeitet oder Gehälter idR regelmäßig angewiesen werden, wird es in der Praxis kaum Ausnahmen geben.

Ob das Verzeichnis mit Hilfe von Softwarelösungen, Excel- oder Worddokumenten geführt wird, ist Sache des jeweiligen Datenverarbeiters und wird von der Art und Größe des Unternehmens sowie der verarbeiteten Daten abhängen. Wichtig ist, dass ein Verzeichnis geführt wird (anderenfalls siehe Punkt 7.8.), da die Verarbeitungsvorgänge speziell gegenüber der Datenschutzbehörde nachgewiesen werden müssen.

⇨ OÖTG befindet sich derzeit in Abstimmung mit verschiedenen Anbietern und prüft auch mögliche Varianten und Ausgestaltungen für touristische Organisationen.

⇨ Die WKO hat auf ihrer Website ein unverbindliches Muster in Form einer Word-Datei veröffentlicht.

7.7. Meldung von Datenschutzverletzungen

Jegliche Form von Datenschutzverletzungen (Verlust, Fremdzugriffe, etc.) sind binnen 72 h der Datenschutzbehörde sowie der / den betroffenen Person/en anzuzeigen.

7.8. Exorbitante Strafen

Einer der wesentlichen Unterschiede zum noch aktuellen Datenschutzgesetz ist die drastische Erhöhung der Strafbestimmungen, die je nach Verstoß bis EUR 20 Mio. oder 4 % des Vorjahresumsatzes bzw. bis EUR 10 Mio. oder 2 % des Vorjahresumsatzes betragen.

8. Welche Rechte stehen Betroffenen zu?

Wie bereits angesprochen, stehen ihnen neben dem Recht sämtliche **Informationen** über die verarbeiteten Daten zu erhalten, u.a. folgende Rechte zu:

8.1. Auskunft über verarbeitete Daten

Jeder Betroffene ist berechtigt bei Unternehmen, Behörden und öffentlichen Stellen zu hinterfragen, welche Daten auf welcher Basis, für welche Zwecke etc. verarbeitet werden. Der Verantwortliche darf sich im Zweifel die Identität des Betroffenen nachweisen lassen und hat binnen 1 Monats die entsprechende Auskunft zu erteilen.

8.2. Widerruf der Einwilligung

Erteilte Einwilligungserklärungen können von Betroffenen jederzeit widerrufen werden. Auf diese Widerrufsmöglichkeit ist bereits im Zusammenhang mit der Einwilligungserklärung hinzuweisen (wie bereits seit Jahren bei der Versendung von Newsletter verpflichtend).

8.3. Löschung der verarbeiteten Daten

Wie bereits angeführt, ist dem Antrag nachzukommen, sofern keine rechtlichen Gründe oder Fristen zur Aufbewahrung o.ä. entgegenstehen.

8.4. Beschwerde bei der Datenschutzbehörde

Betroffene Personen, die von einer nicht rechtmäßigen Verarbeitung ihrer Daten ausgehen, haben das Recht bei der zuständigen Behörde Beschwerde einzulegen und mögliche Verletzungen prüfen zu lassen.

9. Was ist ein Datenschutzbeauftragter und wer hat einen zu bestellen?

a. Sowohl die DSGVO als auch das DS-Anpassungsgesetz enthalten Regelungen zum Datenschutzbeauftragten, lassen allerdings auch einige Fragen offen. Feststeht, dass dieser eine beratende / prüfende Tätigkeit einnimmt, weisungsfrei agiert und über entsprechende fachliche Kenntnisse (rechtlicher und technischer Natur) verfügen muss. Wie die Ausbildung konkret aussehen soll, ist trotz zahlreicher Möglichkeiten derzeit noch nicht hinreichend definiert.

Die Position kann sowohl **extern** als auch **intern** besetzt werden – wichtig ist interne Interessenskonflikte zu vermeiden, was im Falle einer Ernennung durch Mitglieder der GF oder durch Verantwortliche der Bereiche IT, Recht, HR oder Compliance der Fall wäre.

b. **Unternehmen** mit einer **Kerntätigkeit in Verarbeitungsvorgängen** zum Zwecke der systematischen Überwachung bzw. Verarbeitung sensibler Daten sowie **Behörden** und **öffentliche Stellen** müssen einen Datenschutzbeauftragten ernennen. „Öffentliche Stellen“ werden auf Gesetzes- und Verordnungsebene unterschiedlich definiert - folgende Einrichtungen fallen unter diese Begrifflichkeit:

- Staat und Gebietskörperschaften
- Einrichtungen des öffentlichen Rechts
  - im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art
  - Rechtspersönlichkeit
  - von Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts finanziert oder unter deren Aufsicht

- Verantwortliche des öffentlichen Bereichs
  - in Formen des öffentlichen Rechts eingerichtet
  - in Formen des Privatrechts eingerichtet, in Vollziehung der Gesetze tätig

⇨ OÖTG befindet sich derzeit in Abstimmung mit der Aufsichtsbehörde, um Lösungsmöglichkeiten für touristische Organisationen zu eruieren.

10. Umsetzung der DSGVO?

Wie in der Erstinfo dargelegt, ist die Evaluierung der Ist-Situation empfehlenswert, um ersichtlich zu machen, wer als Verantwortlicher / Auftragsverarbeiter welche Daten in seinem Unternehmen bzw. Unternehmensbereichen verarbeitet und ob hierfür eine rechtliche Grundlage gegeben ist. Sind die Kategorien von Daten und deren Verarbeitungsvorgänge bekannt, sind in einem weiteren Schritt unternehmensbezogene Anpassungsmaßnahmen zu definieren, die es bis Mai 2018 umzusetzen gilt.

10.1. Evaluierung

Die Erhebung der verarbeiteten Daten und Prozesse liegt im Ermessen des jeweiligen Verantwortlichen / Auftragsverarbeiters – hierfür können **beispielsweise** folgende Punkte herangezogen werden:

a. Welche **Personen / Personenkategorien** sind betroffen?
Mitarbeiter, Kunden, Lieferanten, Geschäftspartner, Funktionäre, unverbindliche Anfrager, Website-User, …

b. Welche **personenbezogenen Daten / Datenkategorien** werden verarbeitet?
Name, Adresse, Geburts-, Bankdaten, E-Mail-, IP-Adresse, Cookies, Userverhalten, sensible Daten, …

c. Auf welcher **Grundlage** werden Daten verarbeitet?
Gesetz, Vertrag, berechtigtes Interesse (+ Begründung), Einwilligung, öffentliches Interesse

d. Für welche **Zwecke** werden sie verarbeitet?
Gesetzlicher Auftrag, Personalverwaltung, Vertragserfüllung, Zusendung Newsletter, Beantwortung Anfragen, Marketingaktivitäten (konkretisieren!), …

e. Werden die Daten weitergegeben bzw. an welche **Empfänger**?
Finanzamt, GKK, Gebietskörperschaft, Bank, Steuerberater, Versicherung, Vertragspartner, Auftragsverarbeiter, Unternehmen (welche?) im Rahmen eines Vertragsverhältnisses, „Dritte“ (welche?) aufgrund einer ausdrücklichen Zustimmung, …

f. **Wo** sind die Daten gespeichert / wo physisch abgelegt?
CRM, spezielle Software, Clouds, Excel, Word, Outlook, Ordner, Karteien, …

g. Wie sehen **Maßnahmen zur Datensicherheit** aus?
Datenspeicherung, Schutz vor unberechtigten Zugriffen, Verlust, Zerstörung, …

h. **Wie lange** werden Daten **gespeichert** / wann **gelöscht**?
Wichtig für das Verfahrensverzeichnis! Es gilt die gesetzlichen Aufbewahrungsfristen zu beachten – z.B. grs. 7 Jahre im Unternehmens- und Steuerrecht, 3 bzw. 30 Jahre bei Schadenersatzansprüchen, arbeitsrechtliche Ansprüche variieren zw. 6 Monaten und 30 Jahren, …

10.2. Definition Anpassungsmaßnahmen / interne Prozesse

Auf Basis des evaluierten Ist-Zustandes sind Maßnahmen / Prozesse zu definieren, die bis zum Ablauf der Umsetzungsfrist anzupassen sind. Diese variieren je nach Unternehmensgegenstand, interner Organisation sowie rechtlichem und technischem Ist-Zustand - **beispielsweise**:

a. Vorab: Allgemeine **Bewusstseinsbildung** im Unternehmen sowie Sensibilisierung der Mitarbeiter

b. **Prüfung** sämtlicher Unternehmensbereiche und deren Inhalte wie z.B.:
- Organisationsstrukturen, interne Organisationsabläufe, -richtlinien, …
- Ansprechpersonen / verantwortliche Personen
- Interne Überlegungen hinsichtlich einer für Datenschutz zuständigen Ansprechperson
- Prüfung Datenherkunft
- Rechtsgrundlagen für die einzelnen Datenverarbeitungen
- Inhaltliche Prüfung Verträge, AGB, …

- Inhaltliche Prüfung Betriebsvereinbarungen, Datenschutzerklärungen, …
- Inhaltliche Prüfung Zustimmungserklärungen, Buchungsvorgänge, Online-Formulare, Teilnahmebedingungen, Anmeldemodalitäten Newsletter, Katalogbestellungen, …
- Prüfung Hinweispflichten für Widerrufs-, Auskunfts-, Löschungsrechte
- Check Umgang mit Anfrage-, Buchungs-, Meldedaten, …
- Check rechtskonforme Verarbeitung von Fotos (u.a. von Mitarbeitern), …
- Check Weitergabe von Daten an Dritte
- Check räumliche Zutrittsmöglichkeiten – intern, extern, öffentliche Bereiche, Bereiche mit Verarbeitung sensibler Daten, …
- Check Zugriffsermächtigungen Mitarbeiter, IT-Verantwortliche für Software, Server, Räumlichkeiten, …
- Check Sicherheits-, Sicherungs- und Speichermodalitäten, …
- Auseinandersetzung mit dem Inhalt von Verfahrensverzeichnissen
- …
- …
- …

10.3. Umsetzung der definierten Maßnahmen bis Mai 2018!

Oktober 2017
Mag. Alexandra Fally, LL.B.