Unternehmensberatung - Steiermark

Leitfaden zur EU-Datenschutz-Grundverordnung (DSGVO) für ihre Pflichten als Verantwortliche

Unternehmensberaterinnen und Unternehmensberater

1. Allgemein

Mit der EU-Datenschutz-Grundverordnung (DSGVO) und dem österreichischen Datenschutz-Anpassungsgesetz 2018 (DSG) kommen einige betriebliche und organisatorische Änderungen auf österreichische Unternehmen zu. Diese gelten ab dem 25. Mai 2018 für jeglichen betrieblichen Umgang mit personenbezogenen Daten, das sind alle Informationen, welche direkt oder indirekt einen Bezug zu einer Person herstellen können (zB Name, Adresse, Geburtsdatum, genetische Daten, Gesundheitsdaten,...).

Auch Begriffsbestimmungen werden sich ändern, u.a. wird der Begriff des datenschutzrechtlichen Auftraggebers auf „Verantwortlicher" geändert.

Sie sind als externe Unternehmensberaterin und Unternehmensberater Verantwortliche" und „Verantwortlicher" gemäß Art 4 Z 7 der DSGVO, da Sie darüber entscheiden, wie personenbezogene Daten im Unternehmen verwendet werden, für welche Zwecke usw.

Beispiel: Erstellung einer Kundendatei, Aufnahme der Daten zur Erstellung einer Rechnung, Mitarbeiterdatenbank.

Als Unternehmensberaterin und Unternehmensberater können Sie von Ihrer Kundin und Ihrem Kunden auch als externe Datenschutzbeauftragte und externer Datenschutzbeauftragter beauftragt werden.

2. Datensicherheit

Als Verantwortliche und Verantwortlicher müssen Sie für geeignete technische und organisatorische Maßnahmen garantieren, die eine Verarbeitung im Einklang mit den Anforderungen dieser Verordnung sicherstellen und den Schutz der Rechte der betroffenen Person gewährleisten. Sie sind daher als Verantwortliche und Verantwortlicher verpflichtet, Datensicherheitsmaßnahmen zu implementieren, hier sind folgende Maßnahmen in der DSGVO selbst ausgewiesen:

- die **Pseudonymisierung und Verschlüsselung personenbezogener Daten** (z.B. Passwortsicherungen von Dateien): „Pseudonymisierung" ist 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.

- die **Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen** (z.B. Zutritts-/Zugangskontrollen, Zugriffsbeschränkungen). Dazu gehört auch, dass unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung der/des Verantwortlichen verarbeiten („Auftragsprinzip");
- die **Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen** (z.B. Backup-Programme);
- ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmenzur Gewährleistung der Sicherheit der Verarbeitung** (z.B. Selbstevaluierungsprozesse).

2.1. Beurteilung des angemessenen Schutzniveaus

Sie müssen die Risiken berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere bei unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu personenbezogenen Daten („risikobasierter Ansatz").

Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.

2.2. Privacy by design / privacy by default

Zum Schutz der personenbezogenen Daten haben Sie ua auch die Grundsätze des Datenschutzes durch Technik (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) zu berücksichtigen und geeignete interne Strategien festzulegen sowie entsprechende Maßnahmen zu setzen.

- **Datenschutz durch Technik:** Sowohl bei der Planung als auch bei der Datenverarbeitung selbst haben Sie geeignete technische und organisatorische Maßnahmen zu berücksichtigen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen (z.B. Pseudonymisierung).
- **Datenschutzfreundliche Voreinstellungen:** Sie haben geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch entsprechende Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.
- Die Einhaltung eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.

> **Tipp:** Welche Datensicherheitsmaßnahmen konkret im Betrieb sinnvoll / empfehlenswert sind, finden Sie unter www.it-safe.at. Hier sind insbesondere der Onlineratgeber und die Handbücher (KMU und Mitarbeiter) empfehlenswert.

3. Weniger Meldeverpflichtungen – mehr Selbstverantwortung im Betrieb

3.1. Verarbeitungsverzeichnis

Aufgrund der DSGVO muss keine Meldung mehr an das Datenverarbeitungsregister (DVR) erstattet werden und auch die DVR-Nummer gehört der Vergangenheit an. Stattdessen müssen Sie Verzeichnisse über die Verarbeitung von Daten führen. Diese Verzeichnisse sind schriftlich zu führen, wobei dies auch in einem elektronischen Format erfolgen kann. Im Verarbeitungsverzeichnis sind unter anderem die Kategorien von Empfängerinnen und Empfängern (Auftragsverarbeiterinnen und Auftragsverarbeiter, andere Verantwortliche, sonstige Empfängerinnen und Empfänger) anzugeben. Die Steuerberaterin und der Steuerberater wären daher unter diesem Punkt anzugeben.

> **Achtung**: Dieses Verzeichnis müssen Sie einmal für sich selbst (= für die eigenen datenschutzrelevanten Vorgänge im Betrieb) und falls Sie auch als Auftragsverarbeiterin und Auftragsverarbeiter für Ihre Kundinnen und Kunden tätig werden, in dieser Rolle jeweils für Ihre Kundinnen und Kunden führen!

Der Umfang der Dokumentationspflicht ist für Sie als Verantwortliche und Verantwortlicher umfassender als für die Auftragsverarbeiterin und den Auftragsverarbeiter, siehe Muster:

- EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher
- Anwendungsbeispiel für Verantwortlichen.

Tipp: Wenn schon Datenanwendungen im DVR registriert sind, können diese als Anhaltspunkt für die Dokumentation dienen. Die bisherigen Meldungen wurden mittlerweile bereits exportierbar zur Verfügung gestellt (vgl: https://www.dsb.gv.at/dvr-online).

Sie sind verpflichtet, bei der Erfüllung Ihrer Aufgaben mit der Aufsichtsbehörde zusammenzuarbeiten. Auf Anfrage sind die Verzeichnisse der Behörde vorzulegen. Anhand dieser Verzeichnisse ist es für die Aufsichtsbehörde möglich, die betreffenden Verarbeitungsvorgänge zu kontrollieren.

Achtung: Das Verarbeitungsverzeichnis ist ein Kernpunkt der DSGVO! Dieses muss unter allen Umständen vorgelegt bzw eingesehen werden können!

3.2. Risikoanalyse & Datenschutzfolgenabschätzung

Sie müssen Risikoanalysen der Datenanwendungen durchführen. Eine genaue Anleitung dieser Analysen.

4. Datenschutzbeauftragte / Datenschutzbeauftragter

Es ist eine Datenschutzbeauftragte und ein Datenschutzbeauftragter verpflichtend zu bestellen, wenn die Kerntätigkeit des Unternehmens eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Beispiel:

- Haupttätigkeit des Unternehmens ist die Bereitstellung von Website-Analysediensten und die Unterstützung bei zielgruppenorientierten Werbe- und Marketingmaßnahmen
- Haupttätigkeit des Unternehmens ist die Verarbeitung von Daten (Inhalte, Datenverkehrsaufkommen, Standort) durch Telefon- oder Internetdienstleister

Unternehmensberaterinnen und Unternehmensberater arbeiten zwar oftmals auch mit sensiblen Daten (Gesundheitsdaten, Daten über religiöse Zugehörigkeit der Mitarbeiter eines Unternehmens), es ist jedoch sehr fraglich, ob sie das in einem umfangreichen Ausmaß (= große Anzahl der betroffenen Personen, umfassendes Datenvolumen,...) tun bzw ob diese konkrete Datenverarbeitung die Kerntätigkeit (= wichtigsten Arbeitsabläufe, Haupttätigkeit) dieses Unternehmens darstellt. Es ist zum jetzigen Stand nicht davon auszugehen, dass Unternehmensberaterinnen und Unternehmensberater standardmäßig Datenschutzbeauftragte benötigen werden. Im Einzelfall könnte aber dennoch die Bestellung eines solchen notwendig werden (zB Spezialisierung im Unternehmen,...).

5. Sub-Auftragsverarbeiterin und Sub-Auftragsverarbeiter

Ihre Auftragsverarbeiterin und Ihr Auftragsverarbeiter darf keine weitere Auftragsverarbeiterin und keinen weiteren Auftragsverarbeiter (Subunternehmerin und Subunternehmer) ohne Ihre vorherige schriftliche Genehmigung beauftragen und muss Sie immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiterinnen und Auftragsverarbeiter informieren. Sie haben die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.

6. Auftragsverarbeitervertrag

Sie müssen mit Ihrer Auftragsverarbeiterin und Ihrem Auftragsverarbeiter schriftlich einen Vertrag abschließen, wobei elektronisch auch als schriftlich gilt. Der Vertrag kann auf Standardvertragsklauseln beruhen, welche entweder die Europäische Kommission oder die Aufsichtsbehörde festlegen kann und hat Folgendes zu beinhalten:

- Bindung an die Verantwortliche und den Verantwortlichen,
- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen und
- die Pflichten und Rechte der/des Verantwortlichen.

Tipp: Verwenden Sie unser Muster auf wko.at!

Ihre Auftragsverarbeiterin und Ihr Auftragsverarbeiter und eine dieser/diesem unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten nur auf Ihre Weisung verarbeiten, es sei denn, dass Ihre Auftragsverarbeiterin und Ihr Auftragsverarbeiter aufgrund einer gesetzlichen Vorschrift zur Verarbeitung verpflichtet sind. Mitarbeiterinnen und Mitarbeiter sind entsprechend zu belehren (vgl auch: EU-Datenschutz-Grundverordnung (DSGVO): Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen).

7. Informationspflichten

Nach der DSGVO sind den Betroffenen durch die Verantwortliche und den Verantwortlichen gewisse Informationen über die Datenanwendungen zur Verfügung zu stellen.

Die Informationspflichten nach der DSGVO trennen sich in eine Auflistung von Informationen, welche zu erteilen sind, wenn die Daten bei Betroffenen direkt erhoben wurden und für den Fall, dass die Daten nicht bei Betroffenen selbst erhoben wurden.

Die Informationen sind den Betroffenen zum Zeitpunkt der Erhebung der Daten zur Verfügung zu stellen.

Ausnahme: Die Daten müssen nicht zur Verfügung gestellt werden, wenn die betroffene Person bereits über die Informationen verfügt.

Daten werden bei der betroffenen Person selbst erhoben:

- Namen und Kontaktdaten der Verantwortlichen und des Verantwortlichen (und ggf ihrer/seiner Vertreter),
- ggf Kontaktdaten der Datenschutzbeauftragten und des Datenschutzbeauftragten,
- Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung,
- im Falle einer Datenverarbeitung aufgrund berechtigter Interessen der/des Verantwortlichen bzw eines Dritten sind die berechtigten Interessen, die von der/vom Verantwortlichen oder einem Dritten verfolgt werden, auszuweisen,
- ggf Empfänger der Daten,
- falls die Absicht besteht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, muss auch darüber informiert werden, ebenso wie über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission. Weiters ist im Falle von Datenübermittlung vorbehaltlich geeigneter Garantien oder aufgrund von verbindlichen internen Datenschutzvorschriften, bzw generell aufgrund von besonderen Ausnahmebestimmungen eben auf diese geeigneten oder angemessenen Garantien zu verweisen oder zumindest, wo eine Kopie erhältlich wäre,
- Dauer der Datenspeicherung bzw wenn unmöglich die Kriterien für die Festlegung der Dauer,
- Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch
- die Möglichkeit des Widerrufs der Einwilligung,
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- 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,
- ggf über das Bestehen automatisierter Entscheidungsfindung, inkl aussagekräftiger Informationen über die involvierte Logik und die Tragweite der Entscheidung (zB Profiling).

Achtung: Sollen die Daten für einen anderen als den ursprünglichen Zweck weiterverarbeitet werden, müssen vor der Weiterverarbeitung auch Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen erteilt werden.

Daten werden nicht bei der betroffenen Person selbst erhoben:

- den Namen und die Kontaktdaten der/des Verantwortlichen (und ggf Ihrer/seiner Vertreter),
- ggf die Kontaktdaten der/des Datenschutzbeauftragten,
- Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung,
- die Kategorien personenbezogener Daten, die verarbeitet werden,
- ggf Empfänger der Daten,
- falls die Absicht besteht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, muss auch darüber informiert werden, ebenso wie über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission. Weiters ist im Falle von Datenübermittlung vorbehaltlich geeigneter Garantien oder aufgrund von verbindlichen internen Datenschutzvorschriften, bzw generell aufgrund von besonderen Ausnahmebestimmungen eben auf diese geeigneten oder angemessenen Garantien zu verweisen oder zumindest, wo eine Kopie erhältlich wäre,
- Dauer der Datenspeicherung bzw wenn unmöglich die Kriterien für die Festlegung der Dauer,
- im Falle einer Datenverarbeitung aufgrund berechtigter Interessen des Verantwortlichen bzw eines Dritten sind die berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, auszuweisen,
- Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch,
- die Möglichkeit des Widerrufs der Einwilligung,
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- aus welcher Quelle die personenbezogenen Daten stammen (zB öffentlich zugängliche Quelle),
- ggf über das Bestehen automatisierter Entscheidungsfindung, inkl aussagekräftiger Informationen über die involvierte Logik und die Tragweite der Entscheidung (zB Profiling).

Achtung: Sollen die Daten für einen anderen als den ursprünglichen Zweck weiterverarbeitet werden, müssen vor der Weiterverarbeitung auch Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen erteilt werden.

Die/Der Verantwortliche erteilt die Informationen innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, spätestens innerhalb eines Monats. Falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an die Person, oder falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

Ausnahmen:

Wenn

- die betroffene Person bereits über die Informationen verfügt,
- die Erteilung dieser Informationen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert (zB bei Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke) oder falls die Verwirklichung der Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt werden würde,
- die Erlangung oder Offenlegung durch Rechtsvorschriften der Europäischen Union oder der Mitgliedstaaten ausdrücklich geregelt ist,
- die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis oder einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Tipp: Verwenden Sie zur Erstellung Ihrer Datenschutz-Erklärung unseren Onlineratgeber.

Die/Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen und alle Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Die Übermittlung der Informationen erfolgt schriftlich, elektronisch oder in einer anderen Form. Die Informationen können nach den Erwägungsgründen beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist, bereitgestellt werden.

8. Sonstige Betroffenenrechte

Als Verantwortliche und Verantwortlicher müssen Sie den von einer Datenanwendung betroffenen Personen (Betroffene) Rechte gewährleisten:

- Informationspflicht (siehe Punkt 7.)
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung ("Recht auf Vergessenwerden")
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

- Widerspruchsrecht

Abgesehen von den Informationspflichten ist innerhalb von 4 Wochen auf Betroffenenanfragen zu reagieren. Diese Frist kann um weitere zwei Monate verlängert werden (die Frist kann daher insgesamt drei Monate betragen), wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche muss die betroffene Person aber innerhalb eines Monats nach Eingang der Anfrage über eine Fristverlängerung unterrichten, das zusammen mit den Gründen für die Verzögerung.

Tipp: Versuchen Sie standardisierte, rasche Abläufe (zB eine Person „kümmert" sich um die Anfrage, im Verarbeitungsverzeichnis werden Wegweiser mit abgespeichert, um eine schnelle Auffindbarkeit von Daten zu ermöglichen,...) für die Gewährleistung dieser Rechte im Betrieb zu implementieren, um zeit- und ressourcensparend vorgehen zu können!

8. Aufbewahrungsfristen

Eine häufige Anfrage von Kundinnen und Kunden stellen die Speicherfristen dar. Wenn die Aufbewahrung der Daten tatsächlich aus steuerrechtlichen / bilanzrechtlichen Gründen notwendig ist, können diese Daten natürlich auch aufbewahrt werden. Gleiches gilt für Daten, welche aufgrund von vertragsrechtlichen Überlegungen (Gewährleistung, Schadenersatz,...) potentiell benötigt werden. Pauschal alle personenbezogene Daten aber für sieben Jahre zu speichern würde u.a. gegen den Grundsatz der Speicherbegrenzung verstoßen.

9. Haftung

Betroffene Personen haben neben verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfen auch das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche im Falle einer Rechtsverletzung durch die Verantwortliche und den Verantwortlichen (zB Ansprüche auf Schadenersatz).

Betroffene Personen können auf materiellen oder immateriellen Schadenersatz klagen. Jeder an einer Verarbeitung Beteiligte haftet für den Schaden, der durch eine unrechtmäßige Verarbeitung verursacht wurde. Die Haftung entfällt, wenn die fehlende Verantwortung für den Umstand, durch den der Schaden eingetreten ist, nachgewiesen werden kann.

Ist mehr als eine Verantwortliche /ein Verantwortlicher (oder mehr als eine Auftragsverarbeiterin / ein Auftragsverarbeiter) oder sowohl eine Verantwortliche / ein Verantwortlicher als auch eine Auftragsverarbeiterin / ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie für einen Schaden verantwortlich, haftet jede Verantwortliche / jeder Verantwortliche (oder jede Auftragsverarbeiterin / jeder Auftragsverarbeiter) für den gesamten Schaden. Es ist jedoch möglich, von den übrigen an derselben Verarbeitung Beteiligten den Teil des Schadenersatzes zurückzufordern, der ihrem Anteil an der Verantwortung für den Schaden entspricht, also Regress zu nehmen.

10. Geldstrafen

Es drohen Verwaltungsstrafen bis zu einer Maximalhöhe von EUR 20 Mio bzw 4% des weltweiten Konzernumsatzes des vorangegangenen Geschäftsjahres, je nach dem, was höher ist.

Achtung: Obwohl diese Verwaltungsstrafen Maximalstrafen sind, werden datenschutzrechtliche Verletzungen in Zukunft sicher einschneidender und teurer werden. Datenschutz darf nicht mehr auf die leichte Schulter genommen werden.

Stand: 19.01.2018