Unternehmensberatung - Burgenland

Leitfaden zur EU-Datenschutz-Grundverordnung (DSGVO) für Ihre Pflichten als Auftragsverarbeiterinnen und Auftragsverarbeiter

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 Dienstleisters auf „Auftragsverarbeiter" geändert.

Sie sind als externe Unternehmensberaterin und externer Unternehmensberater „Auftragsverarbeiterin" und „Auftragsverarbeiter" gemäß Art 4 Z 8 der DSGVO, da Sie personenbezogene Daten im Auftrag Ihrer Auftraggeberin und Ihres Auftraggebers (Verantwortliche und Verantwortlicher gemäß Art 4 Z 7) bearbeiten.

> **Beispiel:** Sie erhalten und verarbeiten die Bewerbungsunterlagen für die Personalberatung von Ihrer Auftraggeberin und Ihrem Auftraggeber. Im Rahmen Ihrer Strategieberatung haben Sie umfassenden Zugriff auf die Unternehmensdaten wie Bilanzahlen, Mitarbeiterdaten,...

Dieser Leitfaden soll Ihnen einen Überblick über Ihre Pflichten als Auftragsverarbeiterin und Auftragsverarbeiter geben.

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

Die Incite bietet einen Lehrgang zur/zum DSGVO - Geprüfte/r Datenschutzexpertin/-experte an.

2. Datensicherheit

Als Auftragsverarbeiterin und Auftragsverarbeiter 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 Auftragsverarbeiterin und Auftragsverarbeiter 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 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 Maßnahmen zur 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 und Ihre Auftraggeberin und Ihr Auftraggeber 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:** Ihre Auftraggeberin und Ihr Auftraggeber hat 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 http://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 und Ihre Auftraggeberin und Ihr Auftraggeber 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 jeweils für Ihre Kundinnen und Kunden führen!

Der Umfang der Dokumentationspflicht ist für Sie als Auftragsverarbeiterin und Auftragsverarbeiter aber immerhin geringer als für die Verantwortliche und den Verantwortlichen, siehe Muster:

- EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Auftragsverarbeiter
- Anwendungsbeispiel für Auftragsverarbeiter
- 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 und die Verantwortliche und den Verantwortlichen bei Erfüllung ihrer und seiner Pflichten nach der DSGVO unterstützen. 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

Sie dürfen keine weitere Auftragsverarbeiterin und keinen weiteren Auftragsverarbeiter (Subunternehmerin und Subunternehmer) ohne vorherige schriftliche Genehmigung Ihrer Auftraggeberin und Ihres Auftraggebers beauftragen. Liegt nur eine allgemeine schriftliche Genehmigung vor, müssen Sie die Auftraggeberin und den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiterinnen und Auftragsverarbeiter informieren. Ihre Auftraggeberin und Ihr Auftraggeber hat die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben.

Achtung: Grundsätzlich fiele auch die Nutzung von Cloud-Services zur Datenspeicherung unter diesen Passus! Sie müssen einerseits eine DSGVO-konforme Vereinbarung mit Ihren Auftragsverarbeiterinnen und Auftragsverarbeitern abschließen und andererseits sicherstellen, dass diese Speicherung mit Ihrer Auftraggeberin und Ihrem Auftraggeber vereinbart wurde.

6. Auftragsverarbeitervertrag

Sie müssen mit Ihrer Auftraggeberin und ihrem Auftraggeber 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 / 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 Verantwortlichen / des Verantwortlichen.

Dieser Vertrag sieht insbesondere vor, dass die Auftragsverarbeiterin und der Auftragsverarbeiter:

- die personenbezogenen Daten nur auf dokumentierte Weisung der/des Verantwortlichen verarbeitet (auch bei Übermittlung an ein Drittland oder eine internationale Organisation), sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem die Auftragsverarbeiterin und der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt die Auftragsverarbeiterin und der Auftragsverarbeiter der / dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet,
- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
- alle erforderlichen Sicherheitsmaßnahmen ergreift,
- eine vorherige schriftliche Genehmigung der/des Verantwortlichen für die Inanspruchnahme der Dienste einer weiteren Auftragsverarbeiterin (Sub-Auftragsverarbeiterin) und eines weiteren Auftragsverarbeiters (Sub-Auftragsverarbeiter) einhält,
- die Verantwortliche und den Verantwortlichen bei der Beantwortung von Anträgen von Betroffenen unterstützt (unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen),
- die Verantwortliche und den Verantwortlichen bei der Einhaltung der Sicherheitsmaßnahmen und Meldeverpflichtungen unterstützt (unter Berücksichtigung der Art der Verarbeitung und der ihr/ihm zur Verfügung stehenden Informationen),
- nach Vertragserfüllung alle personenbezogenen Daten nach Wahl der Verantwortlichen / des Verantwortlichen entweder löscht oder zurückgibt (sofern keine anderweitige gesetzliche Verpflichtung besteht),
- der Verantwortlichen und dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Pflichtgemäßheit zur Verfügung stellt und Überprüfungen durch die Verantwortliche und den Verantwortlichen ermöglicht und dazu beiträgt. Nimmt die Auftragsverarbeiterin und der Auftragsverarbeiter eine Sub-Auftragsverarbeiterin und einen Sub-Auftragsverarbeiter in Anspruch, werden auch dieser und diesem dieselben Datenschutzpflichten auferlegt.

> **Tipp:** Verwenden Sie unsere Muster: EU-DSGVO-MUSTERVERTRAG-Vereinbarung-Auftragsverarbeitung

Sie und jede Ihnen oder der / dem Verantwortlichen unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten nur auf Weisung Ihrer Auftraggeberin und Ihres Auftraggebers verarbeiten, es sei denn, dass Sie 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).

6.1. Warnpflicht der Unternehmerin und des Unternehmers

Sie unterliegen einer besonderen Warnpflicht, dh Sie haben Ihre Auftraggeberin und Ihren Auftraggeber unverzüglich zu informieren, falls Sie der Auffassung sind, dass eine Weisung gegen Datenschutzrecht verstößt.

7. 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
- Als Auftragsverarbeiter müssen Sie diese Rechte zwar nicht für Ihren Auftraggeber (= den Verantwortlichen) erfüllen, Sie müssen ihn aber bei der Erfüllung seiner Pflichten unterstützen. Wenn Sie zB als Auftragsverarbeiter eine Anfrage eines Kunden Ihres Auftraggebers (= des Verantwortlichen) erhalten, sollten Sie diese Anfrage Ihrem Auftraggeber direkt weiterleiten.

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 Auftragsverarbeiterinnen und Auftragsverarbeiter im Falle einer Rechtsverletzung durch die Auftragsverarbeiterin und den Auftragsverarbeiter (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 Auftragsverarbeiterin / ein Auftragsverarbeiter (oder mehr als eine Verantwortliche /ein Verantwortlicher) 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 Auftragsverarbeiterin / jeder Auftragsverarbeiter (oder jede Verantwortliche / jeder Verantwortliche) 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: 23.01.2018