Buchhaltung

Leitfaden zur EU-Datenschutz-Grundverordnung (DSGVO) für Ihre Pflichten als Verantwortlicher

Bilanzbuchhalter, Buchhalter und Personalverrechner

1. Allgemein

Mit der EU-Datenschutz-Grundverordnung (DSGVO) und dem österreichischen Datenschutz-Anpassungsgesetz 2018 (DSG) kamen einige betriebliche und organisatorische Änderungen auf österreichische Unternehmen zu. Diese gelten seit 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 haben sich geändert, u.a. wird der Begriff des datenschutzrechtlichen Auftraggebers auf „Verantwortlicher".

Sie sind als Bilanzbuchhalter, Buchhalter oder Personalverrechner „Verantwortlicher" gemäß Art 4 Z 7 DSGVO für Ihr eigenes Unternehmen und die Daten, die Sie im Rahmen Ihrer Tätigkeit als Bilanzbuchhalter, Buchhalter und Personalverrechner für andere Unternehmen verarbeiten (also auch als externer Dienstleister!).

> **Beispiel für Datenverarbeitung als Verantwortlicher:** Erstellung Ihrer eigenen Kundendatei, Aufnahme von Daten zur Erstellung einer Rechnung, Führung Ihrer eigenen Mitarbeiterdatenbank. Aber auch: Durchfürhung einer Lohnverrechnung für einen Auftraggeber, Erstellung einer Bilanz für einen Auftraggeber.

2. Rechtsgrundlage

Grundsätzlich dürfen personenbezogene Daten nur verarbeitet werden, wenn dies auf eine gültige Rechtsgrundlage gestützt wird (z.B. auf eine Einwilligung des Betroffenen). Besonders „sensible" Daten benötigen dafür eine Rechtsgrundlage gemäß Artikel 9 DSGVO (z.B. Gesundheitsdaten, Religionsdaten, etc.). Die Verarbeitung sonstiger allgemeiner Daten muss demgegenüber auf eine Rechtsgrundlage gemäß Artikel 6 DSGVO gestützt werden. Hinsichtlich der Frage, welche konkrete Rechtsgrundlage herangezogen werden kann, sind folgende Fälle zu unterscheiden:

- Bei Vertragsverhältnissen mit einem Auftraggeber, der dabei jeweils selbst die datenschutzrechtlich betroffene Person ist (z.B. Vertrag mit einem Arbeitnehmer selbst über dessen eigene Arbeitnehmerveranlagung): Hinsichtlich „sensibler" Daten benötigen Sie hier in der Regel eine Einwilligung der betroffenen Person. Sonstige Daten dürfen auch ohne Einwilligung des Betroffenen verarbeitet werden, z.B. wenn dies zur Erfüllung eines Vertrags notwendig ist (z.B. zur Durchführung der Arbeitnehmerveranlagung). Hier finden Sie nähere Informationen und eine entsprechende Muster-Datenschutzinformation und -Einwilligungserklärung.
- Bei Vertragsverhältnissen mit einem Auftraggeber, bei denen die datenschutzrechtlich betroffenen Personen selbst nicht Vertragsparteien sind

(z.B. die Durchführung einer Personalverrechnung für ein Unternehmen: die ArbeitnehmerInnen sind zwar von der Datenverarbeitung betroffen, aber selbst nicht Vertragspartei): Hinsichtlich „sensibler" Daten benötigen Sie in der Regel keine Einwilligung, sondern können die Datenverarbeitung auf ein „erhebliches öffentliches Interesse" stützen (Artikel 9 Abs. 2 lit g DSGVO). Hinsichtlich sonstiger Daten benötigen Sie in der Regel ebenfalls keine Einwilligung, sondern können die Datenverarbeitung auf „berechtigte Interessen" stützen (Artikel 6 Abs. 1 lit f DSGVO). Nähere Informationen hierzu, insbesondere auch zu den vorzunehmenden Interessenabwägungen finden Sie in unseren FAQ zum Datenschutz für Bilanzbuchhaltungsberufe.

Hinweis: Es handelt sich hierbei um unverbindliche rechtliche Empfehlungen. Diese entbinden Sie nicht von Ihrer Pflicht gemäß DSGVO, die jeweilige Rechtsgrundlage im Einzelfall, erforderlichenfalls anhand einer konkreten Interessenabwägung, zu bestimmen.

Hinweis: Bilanzbuchhalter, Buchhalter und Personalverrechner verarbeiten z.B. folgende sensible Daten: Daten zur Gesundheit bei der Erfassung von Krankheitstagen, Daten zur Entgeltfortzahlung oder Daten zu religiösen oder weltanschaulichen Überzeugungen bei der Erfassung von Feiertagen oder Kantinenrücksichtnahmen. Weitere Informationen zu sensiblen Daten finden Sie auf der Website der WKO.

3. Datensicherheit

Als Verantwortliche 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 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 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).

3.1. 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.

3.2. 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 http://www.it-safe.at/. Hier sind insbesondere der Onlineratgeber und die Handbücher (KMU und Mitarbeiter) empfehlenswert.

4. Weniger Meldeverpflichtungen – mehr Selbstverantwortung im Betrieb

4.1. 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 (Auftragsverarbeiter, andere Verantwortliche, sonstige 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 Auftragsverarbeiter für Ihre Kunden tätig werden, in dieser Rolle jeweils für Ihren Kunden führen!

Der Umfang der Dokumentationspflicht ist für Sie als Verantwortlicher umfassender als für 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!

4.2. Risikoanalyse & Datenschutzfolgenabschätzung

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

5. Datenschutzbeauftragter

Es ist 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

Bilanzbuchhalter/Buchhalter/Personalverrechner 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 Bilanzbuchhalter/Buchhalter/Personalverrechner standardmäßig Datenschutzbeauftragte benötigen werden. Im Einzelfall könnte aber dennoch die Bestellung eines solchen notwendig werden (zB Spezialisierung im Unternehmen,...).

6. Auftragsverarbeitervertrag

Sie müssen mit 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 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 des Verantwortlichen.

Tipp: Verwenden Sie unser Muster auf wko.at!

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

7. Sub-Auftragsverarbeiter

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

8. Informationspflichten

Als Verantwortlicher sind Sie grundsätzlich dazu verpflichtet, die Betroffenen im Voraus über die **Details Ihrer Datenverarbeitungen zu informieren** (siehe Artikel 13 und 14 DSGVO).

Da die Erfüllung dieser Informationspflicht für viele Berufsberechtige aber oftmals mit einem unverhältnismäßigen Aufwand verbunden wäre (Sie müssten gegebenenfalls jeweils alle Arbeitnehmer, Lieferanten und Geschäftspartner sämtlicher Ihrer Kunden informieren), **sind die Berufsberechtigten regelmäßig von dieser Informationspflicht befreit** (siehe Artikel 14 Abs. 5 lit b DSGVO). Weitere Informationen hierzu finden Sie unter § 7 der Verhaltensregeln sowie auf der Webseite der WKO.

Hinweis: Ihre Kunden selbst werden dabei nicht von ihrer eigenen Informationspflicht befreit, die sie gegebenenfalls gegenüber den Betroffenen erbringen müssen! In diesem Rahmen sind die Betroffenen auch über Ihr Unternehmen (also den Berufsberechtigten!) als Empfänger gem. Artikel 13 Abs. 1 lit e DSGVO zu informieren.

9. Sonstige Betroffenenrechte

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

- Informationspflicht (siehe Punkt 8.)
- 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!

10. Aufbewahrungsfristen

Gemäß dem Grundsatz der „Datenminimierung" müssen Datenverarbeitungen auf jenes Maß eingeschränkt werden, das für die Erfüllung des jeweiligen Zwecks erforderlich ist (siehe Artikel 5 Abs. 1 lit c DSGVO). Das bedeutet, dass die Verarbeitung und Speicherung von Daten nur so lange und in dem Umfang erlaubt ist, wie es unbedingt erforderlich ist.

Im konkreten Fall müssen Berufsberechtige die Speicherdauer in Entsprechung des Datenminimierungsgrundsatzes eigenständig und eigenverantwortlich festlegen. Regelmäßig sind die Berufsberechtigten, die von Unternehmen mit der Bearbeitung und Aufbewahrung von Dokumenten beauftragt werden, in Erfüllung ihres Mandats zur eigenverantwortlichen Verarbeitung und Speicherung von Daten verpflichtet, wie beispielsweise:

- gem. § 52c BiBuG für eine Dauer von 5 Jahren, sofern andere Vorschriften keine längere Aufbewahrungsfrist erfordern,
- gem. § 132 BAO für eine Dauer von 7 Jahren, wobei die Frist mit Ablauf des Kalenderjahres zu laufen beginnt,
- gem. § 207 BAO für eine Dauer von 10 Jahren, wobei die Frist mit Ablauf des Kalenderjahres beginnt, in dem die Abgabenverkürzung geendet hat (gem. § 209 BAO verlängert sich diese Verjährungsfrist, wenn nach außen erkennbare Amtshandlungen zur Geltendmachung des Abgabenanspruches oder zur Feststellung des Abgabepflichtigen unternommen werden, um deren Dauer),
- gem. § 11 Abs. 2 letzter Satz UStG für eine Dauer von 7 Jahren,
- gem. § 18 Abs. 10 UStG für eine Dauer von 22 Jahren,
- gem. § 212 UGB für eine Dauer von 7 Jahren, wobei die Frist mit Ablauf des Kalenderjahres zu laufen beginnt (davon umfasst sind auch „Geschäftsbriefe", also etwa geschäftliche E-Mail-Korrespondenz),
- gem. § 41a ASVG für die in der BAO normierten Aufbewahrungsfristen,
- gem. GlBG für eine Dauer von 7 Monaten, die zur Abwehr von etwaigen Rechtsansprüchen wegen Diskriminierung erforderlich sind.

Darüber hinaus müssen Daten solange aufbewahrt werden, wie sie für ein **drohendes oder anhängiges gerichtliches oder behördliches Verfahren**, in dem der Unternehmer oder der Berufsberechtigte Parteistellung hat, von Bedeutung sind (z.B. bei einer Außenprüfung gem. §§ 147 ff BAO oder bei Beschwerdeverfahren gegen Bescheide gem. § 92 BAO).

Unzulässig sind pauschale, nicht näher begründete Aufbewahrungsfristen (wie z.B. „30 Jahre Speicherdauer gemäß allgemeiner Verjährungsfrist nach dem Allgemeinen Bürgerlichen Gesetzbuch"). Gewählte Speicherdauern müssen im Einzelfall durch einen konkreten Anspruch dargelegt werden können. Weitere Informationen zu Speicherfristen finden Sie in den Verhaltensregeln und auf der Webseite der WKO.

11. 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 ein Verantwortlicher (oder mehr als ein Auftragsverarbeiter) oder sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie für einen Schaden verantwortlich, haftet jede Verantwortliche / jeder Verantwortliche (oder 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.

12. 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.

› FAQs zur Datenschutz-Grundverordnung für Bilanzbuchhalter, Buchhalter, Personalverrechner