Buchhaltung - Wien

FAQ zum Datenschutz für Bilanzbuchhaltungsberufe

Inklusive Informationen zu den Verhaltensregeln gemäß Artikel 40 DSGVO

Die konkrete Umsetzung der europäischen Datenschutz-Grundverordnung (DSGVO) ist bis heute für viele Unternehmen mit offenen Fragen verbunden. Der Fachverband Unternehmensberatung, Buchhaltung und IT (UBIT) hat diesbezüglich Unklarheiten für Bilanzbuchhaltungsberufe mit der österreichischen Datenschutzbehörde gelöst und eigene Verhaltensregeln (Code of Conduct) zum Datenschutz erstellt. Folgende „Häufig gestellte Fragen" (FAQ) fassen diese Themen zusammen und unterstützen Sie so bei der Einhaltung der Datenschutzregeln.

» Hier finden Sie die DSGVO-Verhaltensregeln für Bilanzbuchhaltungsberufe

---

---

1. Ich bin in einem Bilanzbuchhaltungsberuf tätig und mein Unternehmen hat sich bereits mit der Thematik beschäftigt und ich bin davon ausgegangen, dass mein Betrieb DSGVO-konform arbeitet. Betrifft mich diese Neuerung dann überhaupt?

Ja. Gerade in diesem Bereich waren bei der konkreten DSGVO-Umsetzung viele offene Fragen. Ein zentraler Punkt war etwa die Vorfrage nach der datenschutzrechtlichen Rollenverteilung: bin ich „Verantwortlicher" oder „Auftragsverarbeiter".

Daran sind je nach Beantwortung viele unterschiedliche Folgefragen geknüpft.

Die Datenschutzbehörde hat nun Klarheit geschaffen und bestätigt, dass Bilanzbuchhaltungsberufe die Datenverarbeitungen gemäß Bilanzbuchhaltungsgesetz (BiBuG) als Verantwortliche durchführen.

2. Bis jetzt bin ich immer davon ausgegangen, dass ich Auftragsverarbeiter bin. Diese Ansicht haben auch die Wirtschaftskammerorganisationen eine Zeit lang vertreten. Warum ist das nun anders?

Aufgrund eines Bescheids der Datenschutzbehörde aus dem Jahr 2005 war bisher davon auszugehen, dass Rechnungswesenberufe wohl gemäß DSGVO als Auftragsverarbeiter einzustufen sind.

In einer Entscheidung aus 2018 hat die Behörde nun bezüglich Steuerberatern entschieden, dass diese als Verantwortliche zu qualifizieren sind, sofern sie mit der Durchführung der Personalverrechnung beauftragt sind.

Begründet wurde dies unter anderem mit dem Umstand, dass Steuerberater gesetzlich verpflichtet sind, ihren Beruf „*eigenverantwortlich*" auszuüben (siehe § 71 Wirtschaftstreuhandberufsgesetz).

Da die Rechnungswesenberufe aber gemäß § 33 BiBuG auf dieselbe Weise zur eigenverantwortlichen Berufsausübung verpflichtet sind, lag nahe, dass diese nach Ansicht der Behörde ebenfalls gemäß DSGVO als Verantwortliche einzustufen sein werden.

3. Ich bin also gemäß DSGVO als Verantwortlicher einzustufen. Was bedeutet das konkret? Welche Änderungen bringt das im Unterschied zu meiner bisherigen Rolle als Auftragsverarbeiter?

Die Rolle als Verantwortlicher unterscheidet sich in einigen Punkten wesentlich von der des Auftragsverarbeiters. Hier finden sie unseren Leitfaden zur EU-Datenschutz-Grundverordnung (DSGVO) für ihre Pflichten als Verantwortlicher. Er fasst die wichtigsten Punkte zusammen und gibt konkrete Hilfestellung bei der Umsetzung.

4. Warum gibt es diese datenschutzrechtlichen Verhaltensregeln für Bilanzbuchhaltungsberufe? Welchen Nutzen haben Sie für mich?

Bisher bestanden zu einigen Punkten Rechtsunsicherheit. Um solche Fragen wie zB die datenschutzrechtliche Rolle der Bilanzbuchhaltungsberufe mit der Datenschutzbehörde zu klären (siehe Frage 1), hat der Fachverband UBIT diese Verhaltensregeln für Bilanzbuchhaltungsberufe erstellt und der Behörde zur Prüfung vorgelegt. Auch Vorgaben hinsichtlich Rechtsgrundlage (siehe Frage 11) und Informationspflichten (siehe Frage 10) konnten geklärt werden.

Unternehmer können auch eine formelle Anwendungserklärung der Verhaltensregeln abgeben (siehe Frage 6), und sich ein Zertifikat darüber ausstellen lassen. Geschieht dies, dann können Datenschutzanfragen von Betroffenen auch ohne Datenschutzbehörde gelöst werden. Bei Verfahren vor der Datenschutzbehörde berücksichtigt diese die Teilnahme an den Verhaltensregeln in der Regel strafmildernd bei der Geldbuße.

5. Was ist die rechtliche Grundlage für die Erstellung dieser Verhaltensregeln?

Artikel 40 DSGVO räumt Branchenverbänden diese Möglichkeit ein und der Fachverband UBIT hat sie genutzt.

6. Sind die neuen Verhaltensregeln nun automatisch auf mich anwendbar? Wie ist es, wenn ich zwar keine formelle Anwendungserklärung gemäß § 8 der Verhaltensregeln abgebe, die neuen Datenschutzregeln aber inhaltlich einhalte?

Grundsätzlich ist es so, dass die Verhaltensregeln nur dann unmittelbar anwendbar sind, wenn ein Berufsberechtigter eines Bilanzbuchhaltungsberufes gemäß § 8 der Verhaltensregeln formell gegenüber einer Überwachungsstelle (siehe Frage 7f) erklärt, diese bei der Verarbeitung personenbezogener Daten im Rahmen ihres Bilanzbuchhaltungsberufes einzuhalten.

Davon abgesehen sprechen aber gute Gründe dafür, dass die Datenschutzbehörde zwei idente Handlungen von zwei Unternehmen inhaltlich nicht unterschiedlich bewerten wird, nur weil das eine Unternehmen eine formelle Anwendungserklärung abgegeben hat und das andere nicht. Die Verhaltensregeln schaffen streng genommen nämlich kein neues Recht, sondern *„präzisieren"* nur das allgemein geltende Datenschutzrecht für eine bestimmte Branche.

Der Fachverband UBIT empfiehlt den Berufsberechtigten daher eindringlich, die **Inhalte der Verhaltensregeln umzusetzen, unabhängig davon, ob man eine formelle Anwendungserklärung abgibt oder nicht**.

Ein Unterschied ist, dass das **Beschwerdeverfahren der „Überwachungsstelle"** gemäß § 10 der Verhaltensregeln ausschließlich jenen offensteht, die sich den Verhaltensregeln formell unterwerfen.

7. Was ist das für eine „Überwachungsstelle", die die Einhaltung der Verhaltensregeln kontrolliert? Was ist der Vorteil, wenn ein Beschwerdeverfahren vor der Überwachungsstelle geführt wird?

Die Überwachungsstelle ist eine von der Datenschutzbehörde und dem Fachverband UBIT unabhängige externe Stelle, die für die Überwachung der Einhaltung der Verhaltensregeln zuständig ist. Die entscheidungsbefugten Personen innerhalb dieser Überwachungsstelle haben sowohl datenschutzrechtliches als auch branchenspezifisches Fachwissen aufzuweisen.

Personen, deren personenbezogene Daten von einem Berufsberechtigten eines Bilanzbuchhaltungsberufes verarbeitet werden, der den Verhaltensregeln zugestimmt hat, können bei der Überwachungsstelle Beschwerde erheben, wenn sie Verstöße gegen die Verhaltensregeln vermeinen. Die Überwachungsstelle wird aber auch von sich aus tätig und überprüft periodisch die Anwendung der Verhaltensregeln durch die Berufsberechtigten.

Der Vorteil ist, dass die Überwachungsstelle dabei keine Geldstrafen verhängen kann. Stattdessen kann sie bei Verstößen z.B. Auflagen erteilen, Anweisungen geben oder – im Falle der Wiederholung oder bei schwerwiegenden Verstößen – den Ausschluss von den Verhaltensregeln beschließen

Das Beschwerdeverfahren gemäß § 10 der Verhaltensregeln betrifft nur Verstöße gegen die Verhaltensregeln. Daneben haben Betroffene aber jederzeit auch das unmittelbare Recht, Beschwerde direkt bei der Datenschutzbehörde einzubringen (und zwar sowohl wegen Verstößen gegen die Verhaltensregeln als auch wegen sonstigen Beschwerden).

Nähere Informationen zur Überwachungsstelle und zum Beschwerdeverfahren finden Sie unter § 10 der Verhaltensregeln.

8. Welche Überwachungsstellen gibt es?

Zur Anwendbarkeit der Verhaltensregeln ist es erforderlich, dass sich eine Überwachungsstelle zuerst erfolgreich bei der Datenschutzbehörde akkreditiert.

Momentan gibt es drei Stellen, die dies getan haben:

- DSGVO Datenschutz Ziviltechniker GmbH
- Austrian Standards plus GmbH
- DR Datenschutz-Compliance eG

9. Muss ich den Verhaltensregeln beitreten, damit sie für mein Unternehmen gelten?

Kurz gesagt: ja. Wie bereits aber unter Frage 6 ausgeführt, **empfiehlt** der Fachverband UBIT **eindringlich** bereits jetzt, **die Inhalte der Verhaltensregeln - unabhängig vom Beitritt - umzusetzen**. Diese sind von der Behörde bestätigt und bieten somit eine gute Basis für ein rechtssicheres Arbeiten!

10. Welche Informationspflichten muss ich einhalten?

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 Berufsberechtigen von Bilanzbuchhaltungsberufen 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.

11. Wann darf ich personenbezogene Daten verarbeiten?

Grundsätzlich dürfen personenbezogene Daten nur verarbeitet werden, wenn dies auf eine Rechtsgrundlage gestützt wird (z.B. auf eine Einwilligung des Betroffenen). Besonders „sensible" Daten (z.B. Gesundheitsdaten, Religionsdaten) benötigen dafür eine Rechtsgrundlage gemäß Artikel 9 DSGVO. Die Verarbeitung sonstiger allgemeiner Daten muss auf eine Rechtsgrundlage gemäß Artikel 6 DSGVO gestützt werden.

Für Auftragsverarbeiter gilt: Für die Weitergabe von Daten von einem Verantwortlichen an einen Auftragsverarbeiter braucht es regelmäßig keine weitere Rechtsgrundlage. Es reicht also die Rechtsgrundlage, auf die der Verantwortliche die Datenverarbeitung selbst stützt (z.B. die Einwilligung, die ein Betroffener dem Verantwortlichen erteilt hat).

Auf welche Rechtsgrundlage können Sie als Verantwortlicher Ihre Datenverarbeitungen nun also stützen? Hier 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 den DSGVO-Verhaltensregeln 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.

12. Als Verantwortlicher bin ich selbst für die Festlegung der Speicherfristen verantwortlich. Welche konkreten Zeiträume sind hier laut Gesetz oder Verhaltensregeln zulässig?

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.

13. Welche Sicherheitsvorkehrungen habe ich bei der Datenspeicherung zu beachten? Wie sieht es mit Backup-Speicherung aus?

Um die Verfügbarkeit von Systemen, Diensten und personenbezogenen Daten auch bei physischen oder technischen Zwischenfällen zu gewährleisten, müssen Berufsberechtigte **regelmäßig Datensicherungen durchführen und ein Wiederherstellungskonzept definieren**.

Insbesondere bei Sicherungen ist die Einhaltung zulässiger Speicherdauern regelmäßig mit erheblichen Schwierigkeiten verbunden, da eine nach Informationsinhalten differenzierte Löschung von Datensätzen in den Sicherungen oftmals mit großem organisatorischen und technischen Aufwand verbunden ist.

Löschungen von automationsunterstützt verarbeiteten personenbezogenen Daten müssen dementsprechend gem. § 4 Abs. 2 Datenschutzgesetz (DSG) **nicht** unverzüglich vorgenommen werden, wenn sie aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden können.

Die Verarbeitung der so über die eigentlich zulässige Speicherdauer hinaus erfassten Daten muss dabei jedoch mit Wirkung nach Artikel 18 Abs. 2 DSGVO eingeschränkt werden.

14. Reicht es zur Einhaltung der Speicherfristen auch aus, wenn ich Daten anonymisiere?

Mit Ablauf der zulässigen Speicherdauer sind betroffene Datenverarbeitungen einzustellen und gespeicherte Daten zum technisch nächstmöglichen Zeitpunkt zu löschen. Als gelöscht gelten auch solche Daten, die durch Entfernung des Personenbezugs anonymisiert wurden.

Festzuhalten ist, dass personenbezogene Daten grundsätzlich nur dann als anonymisiert gelten, wenn der Personenbezug tatsächlich nicht mehr wiederhergestellt werden kann. Da aber selten gänzlich ausschließbar ist, dass Daten denkunmöglich jemals wieder der entsprechenden Person zugeordnet werden können, reicht es für eine Anonymisierung (und damit für die Einhaltung einer Speicherbegrenzung) aus, wenn die Rekonstruktion des Personenbezugs nur mit unverhältnismäßigem Aufwand möglich wäre.