
## Buchhaltung

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

Antworten auf häufig gestellte Fragen

**1. Benötige ich als Bilanzbuchhalter/Buchhalter/Personalverrechner nach BiBuG einen Datenschutzbeauftragten?**
Als Bilanzbuchhalter/Buchhalter/Personalverrechner werden Sie in der Regel keinen Datenschutzbeauftragten benötigen. Mehr dazu.

**2. Muss ich, wenn ich mit mehreren Buchhaltungen und Jahresabschlüsse von Kunden mache, einen Datenschutzbeauftragten haben?**
In einem solchen Fall benötigt man keinen Datenschutzbeauftragten.

**3. Benötigt man als Bilanzbuchhalter/Buchhalter einen Datenschutzbeauftragten, wenn man durch die Buchhaltung eines Arztes Zugang zu den Patientenhonoraren hat?**
Da vertreten wird, dass ein einzelner Arzt keinen Datenschutzbeauftragten benötigt, da bei ihm die umfangreiche Verarbeitung nicht vorliegt, wird dies wohl ebenso für den Steuerberater gelten. Anderes könnte gelten, wenn Sie für sehr viele Ärzte beratend tätig sind und auch sensible Daten wie Gesundheitsdaten verarbeiten.

**4. Fallen auch die Daten der MitarbeiterInnen, die man bei einer neuen Anstellung benötigt (Adresse, Kontodaten, SVNr. der Mitarbeiter etc) unter personenbezogene Daten?**
Ja. Die Verordnung regelt den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die aufgezählten Daten sind personenbezogene Daten und unterliegen daher der DSGVO.

**5. Wenn ich für ein ausländisches Unternehmen arbeite und mit Daten auf einem Schweizer Server arbeite (es geht um Buchhaltung, Ressourcenbestand und andere Daten rund um das Unternehmen) - Bin ich als Einzelunternehmer verpflichtet mich um den Datenschutz zu kümmern oder müssen es die Dienstleister in der Schweiz oder das eigentliche Unternehmen aus Asien?**
Die DSGVO findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der EU erfolgt, unabhängig davon, ob die Verarbeitung in der EU stattfindet.

**6. Kann ich mich darauf verlassen, dass alle Anbieter, die Cloudservices in Österreich anbieten (Apple. Evernote, Microsoft), sich an die DSGVO halten müssen und ich diese Services daher nutzen darf?**
Es sollten sich alle Anbieter in der EU an die DSGVO halten. Sie müssen mit Ihren Dienstleistern (Auftragsverarbeitern) schriftlich einen Vertrag abschließen, in welchem u.a. auch gewährleistet ist, dass der Anbieter die Bestimmungen einhält und Datensicherheitsmaßnahmen implementiert hat.

**7. Muss ich als Bilanzbuchhalter/Buchhalter/Personalverrechner gewährleisten, dass Mitarbeiter nicht mittels USB Stick illegal Daten absaugen können? Also die Möglichkeit generell sperren?**

Ja. Sie sind verpflichtet, dafür zu sorgen, dass die Bestimmungen des Datenschutzrechtes eingehalten werden. Zumindest sollten die Mitarbeiter geschult sein, Sie sollten Sie über das Datengeheimnis entsprechend aufklären und zumindest zumutbare Maßnahmen treffen. Manche Unternehmen unterbinden die Möglichkeit USB-Sticks zu verwenden, dies ist aber rechtlich nicht verpflichtend. Überdies finden Mitarbeiter mit kriminellen Absichten zweifellos auch andere Methoden um Daten „abzusaugen". Hier hilft nur eine entsprechende Sorgfalt bei der Personalauswahl und entsprechende Schulungsmaßnahmen und entsprechende Rechtevergabe (wer darf was).

**8. Ich bin ein EPU und verarbeite normale personenbezogene Daten (gespeicherte Aufträge, Adressen...). Frage: Genügt es diese Daten mit einer Verschlüsselungssoftware zu schützen?**

Es ist sicher ein guter Schritt, er hilft Ihnen allerdings nichts im Hinblick auf Beschädigungen oder Datenverlust. Datensicherung ist auch ein sehr wesentliches Thema! Einen sehr guten Überblick über den Stand der Technik und Marktüblichkeit können Sie sich unter http://www.it-safe.at/ verschaffen. Weitere Informationen dazu finden Sie im IT-Sicherheitshandbuch für KMU .

**9. Wie wird das Risiko bewertet, dass Kunden- bzw. Buchhaltungsdaten - wie bei so vielen (Home-)Office - offen bzw. in einem unversperrten Schrank stehen (kein Kundenverkehr)? Stichwort Einbruch aber auch generell. Wobei: Ein versperrter Schrank wohl mehr Aufmerksamkeit auf sich ziehen würde.**

Sie müssen dafür Sorge tragen, dass kein Unbefugter (zB Putzfrau, ev. auch Familienmitglieder, Besuch, etc.) an die Daten gelangt. Auch für Einbruch, Feuer oder Wasserschaden ist Vorsorge zu tragen. Vergessen Sie auch nicht auf die Datensicherung (räumlich getrennt von den ursprünglichen Daten). Ein versperrter Schrank kann zB der Einsicht durch nicht befugte Mitarbeiter, Reinigungskräften uÄ entgegenwirken.
Einen sehr guten Überblick über den Stand der Technik und Marktüblichkeit können Sie sich unter http://www.it-safe.at/ verschaffen.

**10. Darf mein Bilanzbuchhalter/Buchhalter/Personalverrechner meinen Buchhaltungs/Personalakt überhaupt noch per E-Mail versenden?**
Emails müssen auf Basis der DSGVO nicht zwingend verschlüsselt werden, das ist so nirgends ausgewiesen. Unverschlüsselte e-mails bieten keine Datensicherheit und können von Unbefugten leicht „mitgelesen" werden. Unbedingt anzuraten ist daher die Verschlüsselung bei der Handhabe mit heiklen Daten wie Bankverbindungen, Kreditkartendaten usw, aber natürlich auch bei der Handhabe mit sensiblen oder strafrechtlich relevanten Daten.

**11. Wie muss ich Daten/ Adressen sichern, die in schriftlicher Form festgehalten werden?**
Schriftlich meint hier wohl auf Papier. Versperrbare Schränke, Zutrittsberechtigungen, Zugriffsberechtigungen etc. wären hier anzudenken. Denken Sie dabei auch im eigenen Interesse an Datensicherung und daran, diese räumlich getrennt (zB zur Vorsorge bei Feuer) aufzubewahren. Einen sehr guten Überblick über den Stand der Technik und Marktüblichkeit können Sie sich unter http://www.it-safe.at/ verschaffen.

**12. Wenn ich von Kunden gefragt werde, ob wir uns an die neue Verordnung halten, gibt es Musterbriefe, die man versenden kann, in denen man bestätigt, dass man sich an die Gesetze hält?**
Es gibt ein Muster zum Auskunftsersuchen. Einen Musterbrief für die Bestätigung der Einhaltung der DSGVO haben wir nicht formuliert.

**13. Was ist bei der Personalverwaltung intern zu beachten?**
Auch die Datenverarbeitung personenbezogener Daten von Mitarbeitern fällt unter die DSGVO. Es sollte hier geprüft werden, auf welcher Grundlage Daten verarbeitet werden (gesetzliche Verpflichtung, für die Dienstvertragserfüllung notwendig, Einwilligung?). Diese Verarbeitung ist genauso wie jede andere im Verarbeitungsverzeichnis auszuweisen.

**14. Muss ein Bilanzbuchhalter, Buchhalter oder Personalverrechner das Einverständnis zur Datenspeicherung vom jeweiligen Mitarbeiter des Auftraggebers einholen?**
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"-Datenschutz-Verhaltensregeln.

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

**15. Gibt es Ausnahmen beim Schutz von Mitarbeiterdaten?**
Ausnahmen iSv Ausnahmen von der DSGVO bestehen nur dann, wenn Daten anonymisiert verarbeitet werden, dh kein Personenbezug zum konkreten Mitarbeiter herstellbar ist.

**16. Wenn ich von meinen Mitarbeitern das Religionsbekenntnis und die Gewerkschaftszugehörigkeit für die Lohnverrechnung abspeichere und verarbeite, habe ich dann bereits sensible Daten? Was sind die Folgen?**
Ja, das sind sensible Daten. Für die Verarbeitung derartiger Daten brauchen Sie entweder eine ausdrückliche Einwilligung vom betroffenen Mitarbeiter oder das Erfordernis der Erfüllung gesetzlicher Verpflichtungen. Ersucht etwa der AN den Gewerkschaftsbeitrag über die Lohnverrechnung abzurechnen, sollten Sie von ihm eine entsprechende Einwilligung einholen. Gleiches gilt, wenn der AN bspw sein Religionsbekenntnis „Evangelisch" bekanntgibt, um den Karfreitag als Feiertag iSd Arbeitsruhegesetzes zu erhalten.

**17. Bewerberunterlagen werden von Personalunternehmen geschickt - ist die Verschlüsselung hier nötig?**
Emails müssen auf Basis der DSGVO nicht zwingend verschlüsselt werden, das ist so nirgends ausgewiesen. Man kann sich aber aus Gründen der Datensicherheit dafür entschließen. Sinnvoll ist die Verschlüsselung jedenfalls bei der Handhabe mit heiklen Daten wie Bankverbindungen, Kreditkartendaten usw, aber natürlich auch bei der Handhabe mit sensiblen oder strafrechtlich relevanten Daten.

**18. Personenbezogene Daten betreffen ja auch Daten von Mitarbeitern. Reicht es aus, wenn ich z.B. im Anstellungsvertrag darauf hinweise, "dass Daten elektronisch verarbeitet werden" und der Mitarbeiter mit dem Vertrag dem zustimmt?**
Wohl eher nicht, allein schon deshalb, weil die Einwilligung sehr pauschal abgeholt wird und nicht auf konkrete Datenarten, Zwecke der Verarbeitung etc verwiesen wird. Viele der Verarbeitungsvorgänge im Zusammenhang mit Mitarbeiterdaten werden Ihnen durch Arbeits- und Sozialrecht bzw Kollektivverträge vorgegeben, sind somit „zur Erfüllung einer rechtlichen Verpflichtung erforderlich" und rechtmäßig gemäß Art 6 DSGVO.

**19. Wir nutzen intern Fahrzeugtracking. Die Daten werden im Betrieb gespeichert. Es ist dadurch nachvollziehbar wann ein Mitarbeiter mit seinem Fahrzeug wo war. Fallen diese Daten unter "sensible" Daten?**
Es sind personenbezogene Daten, allerdings keine sensiblen Datensätze.

**20. Gibt es Vorschriften zur Archivierung der Personaldaten?**
Es gibt einige Vorschriften im Arbeitsrecht, wie lange Daten aufbewahrt werden müssen (zB Dienstzeugnisses nach § 1163 iVm § 1478 ABGB: 30 Jahre). Wie Daten archiviert werden, gibt das Gesetz allerdings nicht vor.

**21. Was kann/muss im Dienstvertrag datenschutzrechtlich berücksichtigt werden? Zustimmung zur Datenverarbeitung? Widerrufsrecht bzw Löschungsrecht (im Ausmaß der gesetzlichen Frist?)?**
In dieser Generalität nicht zu beantworten. Die wesentlichen Punkte der Datenverarbeitung, zB zu Zwecken der Personalverrechnung, sind gesetzlich legitimiert und bedürfen keiner weiteren Zustimmung. Die allenfalls notwendigen Zustimmungserklärungen hängen von der Situation im Einzelfall ab.

**22. Ich bin eine HR Mitarbeiterin und arbeite mit allen Personaldaten (ua. Bankdaten etc) und gebe diese an ein externes Lohnbüro weiter, was muss ich hierbei beachten?**
Sie müssen keinen Auftragsverarbeitungsvertrag abschließen, da Externe im Rahmen Ihrer Tätigkeit als Bilanzbuchhalter, Buchhalter und Personalverrechner selbst Verantwortliche sind. Ihr Unternehmen ist in diesem Fall jedoch in der Regel dazu verpflichtet, die Betroffenen über das externe Lohnbüro als Datenempfänger zu informieren (Artikel 13 Abs. 1 lit e DSGVO).

**23. Ich bin ein externes Lohnbüro und erhalte Mitarbeiterdaten eines Auftraggebers aus der EU zur Bearbeitung und Erledigung von verschiedenen Aufgaben. Was muss ich beachten?**
Sie müssen keinen Auftragsverarbeitungsvertrag abschließen, da Externe im Rahmen Ihrer Tätigkeit als Bilanzbuchhalter, Buchhalter und Personalverrechner selbst Verantwortliche sind. Ihr Auftraggeber ist in diesem Fall jedoch in der Regel dazu verpflichtet, die Betroffenen über Ihr externes Lohnbüro als Datenempfänger zu informieren (Artikel 13 Abs. 1 lit e DSGVO).

**24. Muss ich die Mitarbeiterdaten (Lohnzettel, Lebensläufe, Zeugnisse u.ä.) speziell schützen?**
Es sind keine speziellen Datenschutzmaßnahmen im Arbeitsrecht vorgeschrieben. Bei heiklen, aber v.a. sensiblen Daten wäre aber natürlich das Augenmerk auf die Sicherheit der Daten zu erhöhen.

**25. Müssen Arbeitsverträge von Mitarbeitern auch datenschutzrechtliche Einwilligungen enthalten?**
Hier ist je nach konkretem Fall zu unterscheiden. Die Datenverarbeitungen könnten z.B. zur Vertragserfüllung, aufgrund einer Einwilligung oder aufgrund eines sonstigen berechtigten Interesses erlaubt sein. Bei Einwilligungen ist insbesondere darauf zu achten, dass diese auch tatsächlich freiwillig abgegeben werden und nicht gegen das sogenannte „Kopplungsverbot" verstoßen. Detaillierte Informationen hierzu finden Sie in diesen Datenschutz-

FAQ für Mitarbeiterdaten.

**26. Wir haben als Unternehmer natürlich Kontakt mit Mitarbeitern von Kunden. Müssen wir mit jedem Mitarbeiter des Kunden Vereinbarungen treffen, dass seine Daten bei uns gespeichert werden (Mail, etc), oder reicht eine Vereinbarung mit dem Kunden, welcher Sie auf seine Mitarbeiter überbindet?**
Es reicht eine Vereinbarung mit Ihrem Kunden.

**27. Zählen Gehaltsangaben zu den "sensiblen Daten"?**
Nein.

**28. Gibt es die gesetzliche Pflicht, die Mitarbeiter nachweislich zu schulen?**
Die Belehrung von Mitarbeitern über das Datengeheimnis ist in § 6 des österreichischen Datenschutz-Anpassungsgesetzes konkret angesprochen. Wie diese Belehrung auszusehen hat, bzw welche Schulungsmaßnahmen sinnvoll sind, ergibt sich aus dem jeweiligen Unternehmen selbst. Tipps und Vergleiche können Sie sich unter www.it-safe.at holen! Wir empfehlen auch, sich das Mitarbeiter-Handbuch auf www.it-safe.at zumindest herunter zu laden und den Mitarbeitern zur Verfügung zu stellen. Auch interne Regelungen wären sinnvoll (zB private Internetnutzung, wohin soll sich der Mitarbeiter mit datenschutzrechtlichen Fragen wenden, usw).

Stand: 22.01.2020