FORUM

Datenschutz in der Buchhaltung und im Rechnungswesen – Wie schütze ich die Daten?

Finanzdaten DSGVO-konform sichern

Sehr geehrte Leser*innen,

wir freuen uns, dass Sie sich für dieses Whitepaper interessieren.

Nachfolgend erhalten Sie wertvolle Einblicke, Tipps und Handlungsempfehlungen für Ihren Job.

Informieren Sie sich über aktuelle, praxisnahe Trends und Impulse direkt von unseren Expert*innen.

Zusätzlich können Sie mit unserem Angebot an verschiedenen Weiterbildungen Ihr Fachwissen ausbauen und vertiefen.

Wir wünschen Ihnen viele neue Erkenntnisse beim Lesen.

Dieses Whitepaper wurde mit Hilfe von NotebookLM, Perplexity und ChatGPT erstellt.

Bedeutung des Datenschutzes im Rechnungswesen

Wer in einem Unternehmen für die Buchhaltung zuständig ist, verarbeitet täglich sensible Finanzdaten. Der Schutz dieser Informationen ist nicht nur eine **gesetzliche Pflicht**, sondern auch ein **entscheidender Vertrauensfaktor** gegenüber Mandanten, Geschäftspartnern und Behörden. Buchhaltungsdaten gehören zu den sensibelsten Informationen im Unternehmen. Ein durchdachter Datenschutz in der Buchhaltung ist unverzichtbar, stärkt die Compliance und das Vertrauen in Ihr Unternehmen.

Relevanz und aktuelle Herausforderungen

Die gesetzlichen Datenschutzanforderungen an Finanzdaten sind besonders streng, da sie im Sinne der Datenschutz-Grundverordnung (DSGVO) als personenbezogene Daten gelten.

Unternehmen stehen hier vor einer besonderen Herausforderung: Einerseits verlangt die DSGVO die Beschränkung der Verarbeitung personenbezogener Daten auf das Nötigste (Datenminimierung). Andererseits müssen Unternehmen die gesetzlichen Aufbewahrungspflichten beachten, die eine längere Speicherung vorschreiben. Klare Prozesse und fundierte Entscheidungen sind notwendig, um die Vorgaben der DSGVO und die Aufbewahrungspflichten in Einklang zu bringen. Angesichts der zunehmenden Digitalisierung von Buchhaltungsprozessen, beispielsweise durch die E-Rechnung, wird der Schutz dieser Daten zu einer großen Herausforderung.

Rechtlicher Rahmen

DSGVO-Grundsätze für die Buchhaltung

Für Buchhaltungsdaten sind insbesondere zwei Grundsätze der DSGVO relevant:

1. **Zweckbindung:** Unternehmen dürfen Buchhaltungsdaten nur zu vorab festgelegten Zwecken sammeln und verarbeiten. Eine willkürliche Datensammlung ist nicht erlaubt. Beispielsweise ist die Erfassung von Steuernummern und Bankverbindungen erlaubt, wenn sie zur Begleichung von Rechnungen oder zur Lohnzahlung dient.
2. **Speicherbegrenzung und Datenminimierung:** Die Verarbeitung personenbezogener Daten ist auf das Nötigste zu beschränken. Daten dürfen nur für einen bestimmten Zeitraum gespeichert werden. Ist der Zweck der Datenerfassung erfüllt, müssen die Informationen gelöscht werden.

Aufbewahrungspflichten vs. Datenschutz

Die Pflicht zur Löschung nach erfülltem Zweck wird durch gesetzliche Aufbewahrungspflichten, die in der Abgabenordnung (AO) und im Handelsgesetzbuch (HGB) festgelegt sind, in der Buchhaltung eingeschränkt.

Wichtige Aufbewahrungsfristen (Beispiele):

Unterlage	Frist	Quelle(n)
Jahresabschlüsse, Eröffnungsbilanz, Bücher	10 Jahre	
Buchungsbelege (Rechnungen, Lohn-/Reisekostenabrechnungen)	8 Jahre (seit 2025) oder 10 Jahre	
Geschäftsbriefe, steuerlich relevante Unterlagen	6 Jahre	

Die Aufbewahrungspflicht hat Vorrang vor dem Löschungsverlangen eines Betroffenen. Erst wenn diese gesetzlichen Pflichten erfüllt sind, greifen die Löschfristen der DSGVO. Eine Verlängerung der Fristen ist möglich, wenn Dokumente im Zusammenhang mit einem Gerichts- oder Steuerverfahren benötigt werden.

Die **Archivierung** kann digital erfolgen, außer bei Jahresabschlüssen und der Eröffnungsbilanz, die in gedruckter Form vorliegen müssen. Verantwortliche müssen sicherstellen, dass digital archivierte Daten DSGVO-konform gespeichert sind.

Rollen & Verantwortlichkeiten

Datenschutz in der Buchhaltung ist eine zentrale Aufgabe für Datenschutzbeauftragte und Mitarbeiter im Rechnungswesen und stellt einen wichtigen Teil der unternehmerischen Sorgfaltspflicht dar.

Wird die Buchhaltung ausgelagert, verbleibt die **datenschutzrechtliche Verantwortung** in jedem Fall beim auftraggebenden Unternehmen. Auch wenn Aufgaben ausgelagert werden, sollte das Unternehmen darauf achten, dass die geregelten Zugriffe auf Buchhaltungsdaten aktuell und "wasserdicht" sind.

Typische Risiken & Datenarten in der Buchhaltung

Arten personenbezogener Daten

In der Buchhaltung werden täglich große Mengen sensibler und personenbezogener Daten verarbeitet. Dazu zählen:

- **Gehaltsdaten:** Löhne, Sozialversicherungsnummern und Bankverbindungen.
- **Geschäftsdaten:** Verträge, steuerrelevante Informationen.
- **Personenbezogene Angaben in Rechnungen:** Name und Anschrift des Leistungserbringers oder -empfängers, Steuernummer oder Umsatzsteuer-Identifikationsnummer.
- **Kunden- und Lieferantendaten**.

Häufige Risiken

Sind diese Informationen nicht ausreichend geschützt, drohen hohe DSGVO-Bußgelder, Imageschäden oder juristische Schritte.

Typische Herausforderungen und Risiken sind:

- **Mangelndes Zugriffsmanagement:** In Buchhaltungsabteilungen mangelt es oft an klar geregelten Zugriffsrechten, was zu ungewolltem Datenzugang führen kann.
- **Cyberangriffe:** Kriminelle verschaffen sich mit Phishing-Angriffen Zugang zu Buchhaltungsdaten.
- **Unsichere Datenübermittlung:** Werden Rechnungen oder Verträge **unverschlüsselt per E-Mail** versendet, haben Hacker leichtes Spiel, und es droht ein Verstoß gegen die DSGVO. Die Übermittlung über verschlüsselte Verbindungen ist daher essenziell.
- **Nicht DSGVO-konforme Archivierung:** Viele Archivierungslösungen sind nicht konform oder erlauben keine sichere Löschung. Eine reine Ablage auf einem Laufwerk oder Ähnlichem ist nicht ausreichend.
- **Cloud-Nutzung:** Bei ausgelagerten Buchhaltungsdienstleistungen (z. B. Cloud-Anwendungen) kann die Kontrolle schwerfallen. Obwohl die Nutzung von Cloud-Anbietern aus Deutschland und der EU grundsätzlich zulässig ist, müssen bei Diensten aus den USA die Zertifizierungen nach dem EU-US Data Privacy Framework (nach dem 3. Angemessenheitsbeschluss vom Juli 2023) beachtet werden, um vorerst Rechtssicherheit zu gewährleisten.

Best Practices zum Datenschutz in der Buchhaltung

Zur Sicherstellung der DSGVO-Konformität in der Buchhaltung sollten technische und organisatorische Maßnahmen implementiert werden.

Technische Maßnahmen

Ziel der technischen Maßnahmen ist es, die Vertraulichkeit, Integrität und Verfügbarkeit der Buchhaltungsdaten zu gewährleisten.

- **Verschlüsselung:** Daten müssen mithilfe mathematischer Algorithmen so umgewandelt werden, dass sie für Unbefugte unlesbar sind. Die Verschlüsselung betrifft sowohl **gespeicherte Daten** (auf Servern oder in der Cloud) als auch **übertragene Daten** (z. B. über HTTPS oder SFTP). Für E-Mail-Kommunikation wird oft die asymmetrische Verschlüsselung genutzt, die besonders sicher ist.
- **Zugriffskontrolle und Berechtigungskonzepte:** Es muss ein Berechtigungskonzept implementiert werden, das durch **Rollen- und Rechtemanagement** in der Buchhaltungssoftware sicherstellt, dass wirklich nur berechtigte Personen Zugriff auf die Daten haben.

- **Authentifizierung:** Der Einsatz von **Mehrstufiger Authentifizierung** (z. B. Zwei-Faktor-Authentifizierung) erschwert unbefugten Zugriff erheblich.
- **Backups:** Regelmäßige, verschlüsselte Datensicherungen schützen vor Datenverlust durch Hardwaredefekte oder Cyberangriffe.
- **Protokollierung:** Alle Zugriffe und Änderungen an Buchhaltungsdaten müssen dokumentiert werden.
- **Sicherheitsupdates:** Regelmäßige Sicherheitsupdates für die IT-Systeme sind notwendig.

Organisatorische Maßnahmen

Organisatorische Maßnahmen sorgen für klare Prozesse und Verantwortlichkeiten.

- **Dokumentation und Rechenschaftspflicht:** Eine DSGVO-konforme Dokumentation ist Pflicht. Unternehmen müssen nachweisen können, wann, warum und wie Finanzdaten verarbeitet werden. Das Verzeichnis für Verarbeitungstätigkeiten (VVT) enthält diese Informationen.
- **Löschkonzepte und -strategie:** Nach Ablauf der gesetzlichen Aufbewahrungsfristen müssen Buchführungsdaten gelöscht werden, um die Grundsätze der Speicherbegrenzung zu erfüllen. Die Löschfristen sollten im Konzept festgehalten werden.
- **Sichere Datenlöschung:** Nach Ablauf der Frist müssen sämtliche Daten (analog und digital, inklusive Kopien) **vollständig und unwiderruflich** entfernt werden, sodass keine Möglichkeit zur Wiederherstellung besteht. Für digitale Daten sind entsprechende technische Lösungen zu bevorzugen.
- **Schulung der Mitarbeitenden:** Mitarbeitende in der Buchhaltung müssen geschult und für den Datenschutz sensibilisiert werden, insbesondere im Umgang mit sensiblen Daten sowie gegenüber Risiken wie Phishing und Social Engineering.
- **Datenschutz-Folgenabschätzung (DSFA):** Eine DSFA ist notwendig, wenn systematisch besonders schutzbedürftige Daten verarbeitet oder neue Technologien eingesetzt werden. Sie dient dazu, Risiken zu beschreiben, zu bewerten und klare, den Prozess sicherer machende Maßnahmen festzulegen.

Besonderheiten bei externer Zusammenarbeit

Wenn Buchhaltungsprozesse ausgelagert werden (z. B. an Steuerberater oder Softwareanbieter), bleibt das Unternehmen rechtlich verantwortlich.

- **Auftragsverarbeitungsvertrag (AVV):** Externe Dienstleister agieren als Auftragsverarbeiter und müssen vertraglich verpflichtet werden. Ein AVV muss erstellt und abgeschlossen werden.
- **Kontrolle des Dienstleisters:** Unternehmen sollten Dienstleister sorgfältig prüfen. Im AVV sollte das Recht zur Prüfung der DSGVO-Konformität des externen Partners festgelegt

sein. Statt regelmäßiger Vor-Ort-Kontrollen kann alternativ auch die Vorlage eines **Datensicherheitskonzepts** des Dienstleisters verlangt werden.

Praxisbeispiele & Handlungsempfehlungen

Um den Datenschutz in der Buchhaltung effizient und DSGVO-konform umzusetzen, empfiehlt sich ein strukturierter Ansatz:

1. **Bestandsaufnahme:** Erfassen Sie, welche Finanzdaten verarbeitet werden.
2. **Verantwortlichkeiten klären:** Legen Sie fest, wer für welche Datenschutzvorgänge zuständig ist.
3. **Dienstleister prüfen:** Prüfen oder schließen Sie Auftragsverarbeitungsverträge (AVV) mit externen Partnern ab.
4. **Berechtigungskonzepte umsetzen:** Regeln Sie Zugriffe durch technische Maßnahmen und Berechtigungskonzepte, um unerlaubten Zugriff zu verhindern.
5. **Dokumentation aktuell halten:** Pflegen Sie die Datenschutzdokumentation (z. B. das Verarbeitungsverzeichnis).
6. **Archivierung und Löschung sicherstellen:** Nutzen Sie eine DSGVO-konforme Archivierungslösung, die sowohl die Aufbewahrungspflichten als auch die unwiederherstellbare Löschung gewährleistet.
7. **Mitarbeiter schulen:** Sensibilisieren und schulen Sie Mitarbeitende in der Buchhaltung regelmäßig für den sicheren Umgang mit sensiblen Daten.

Fazit

Zentrale Erkenntnisse in Stichpunkten

- **Sensibilität der Daten:** Finanzdaten zählen zu den sensibelsten Unternehmensinformationen und erfordern strengen Schutz nach DSGVO.
- **Spannungsfeld:** Datenschutz muss mit den gesetzlichen Aufbewahrungspflichten aus AO und HGB in Einklang gebracht werden.
- **Risiken:** Die größten Risiken sind fehlende Zugriffskontrolle, unsichere Übertragungswege (unverschlüsselte E-Mails) und mangelhafte Archivierungs- und Löschkonzepte.
- **Technische Maßnahmen:** Verschlüsselung, Zugriffsbeschränkungen und regelmäßige, verschlüsselte Backups sind unverzichtbar.
- **Organisatorische Maßnahmen:** Pflicht sind DSGVO-konforme Dokumentation, klare Löschstrategien und die regelmäßige Schulung der Mitarbeiter.
- **Externe Partner:** Die datenschutzrechtliche Verantwortung bleibt beim Unternehmen; der Abschluss eines AVV und die sorgfältige Prüfung des Dienstleisters sind zwingend.

- **Mehrwert:** Ein durchdachter Datenschutz stärkt das Vertrauen, verbessert die Compliance und kann als strategischer Wettbewerbsvorteil dienen.

Quellenverzeichnis

Proliance.ai. Auszüge aus „Datenschutz in der Buchhaltung: Finanzdaten DSGVO-konform sichern.“

WEKO Informatik GmbH. Auszüge aus „Datenschutz in der Buchhaltung: Ein Überblick für Unternehmen.“

Buchhaltung.de A-Z e. K. Auszüge aus „Verschlüsselung und Datensicherheit in der Buchhaltung!“

FORUM Institut. Auszüge aus „e-Learning: Datenschutzrecht – FORUM Institut.“

Passende Weiterbildungen finden Sie hier:

Seminare im Rechnungswesen

Die täglichen Anforderungen im Beruf erfordern aktuelles Wissen und praxisnahe Lösungen. Für Fach- und Führungskräfte bieten wir ein vielseitiges und anwendungsorientiertes Weiterbildungsangebot in unterschiedlichen Themenbereichen. Unsere erfahrenen Referent*innen vermitteln fundiertes Know-how mit direktem Praxisbezug. Mit unseren ISO-Zertifizierungen nach 9001 und 21001 stehen wir für geprüfte Qualität in der Weiterbildung. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt informieren und testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH · Vangerowstraße 18 · 69115 Heidelberg · Germany
Telefon: +49 6221 500-500 · Fax: +49 6221 500-555 · www.forum-institut.de