

## Vergabeverfahren Lohnbuchhaltung und steuerrechtliche Beratung

**Verzeichnis von Verarbeitungstätigkeiten der  
Steuerberatungskanzlei im Sinne von Art. 30 Abs. 1 Datenschutz-  
Grundverordnung (DSGVO) - Mustervorlage**

Anlage-09

**(Stand: tt.mm.jjjj)** – Erst nach Zuschlagserteilung vom Auftragnehmer auszufüllen.

<b>Verantwortlicher</b>	
Name bzw. Firma der verantwortlichen natürlichen oder juristischen Person	
Ansprechperson	
Postadresse	
Telefon	
E-Mail-Adresse	

<b>Datenschutzbeauftragter</b> [soweit DSB benannt wurde]	
Nachname, Vorname [Funktion ausreichend, z. B. Datenschutzbeauftragter]	
Kontaktdaten wie z.B. Postadresse, Telefon oder E-Mail-Adresse [Funktionsadresse genügt, z. B. Datenschutzbeauftragter@Kanzlei.de]	

<b>Verarbeitungstätigkeit lfd. Nr. 1: Lohnbuchhaltung von Mandanten</b>	
Zwecke der Verarbeitung	Erstellung der Lohnbuchhaltung, insb. <ul style="list-style-type: none"><li>• Berechnung der Lohn- und Gehaltsansprüche</li><li>• Berechnung von Abgaben und Steuern</li><li>• Erstellung und Bereitstellung der Lohn- und Gehaltsnachweise</li><li>• Beratung zur steuerlichen Gestaltung arbeitsrechtlicher Sachverhalte</li></ul>
Kategorien betroffener Personen	Beschäftigte von Mandanten

## Vergabeverfahren Lohnbuchhaltung und steuerrechtliche Beratung

Kategorien von personenbezogenen Daten	<p>Stammdaten der Beschäftigten, inkl. Angaben zu Familienstand, Schwerbehinderteneigenschaften und Kirchensteuerpflicht sowie Sozialdaten</p> <p>Ansprechpersonen im erforderlichen Schriftverkehr mit externen Stellen</p> <p>Zeitaufzeichnungen für Abrechnungserstellung</p> <p>Zeitaufzeichnungen für Abrechnungserstellung</p>
Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden	<ul style="list-style-type: none"> <li>• Personalabteilung</li> <li>• Rechnungswesen</li> <li>• Sozialversicherungsträger</li> <li>• Finanzbehörden</li> <li>• Kreditinstitute</li> <li>• Versicherungen</li> <li>• Gerichte</li> <li>• Gläubiger</li> <li>• IT-Dienstleister [soweit vorhanden]</li> </ul>
Ggf. Datenübermittlung in Drittstaaten	keine
Fristen für die Löschung der Datenkategorien	siehe Löschkonzept
Technische und organisatorische Maßnahmen	siehe IT-Sicherheitskonzept

### Verarbeitungstätigkeit lfd. Nr. 2: Finanzbuchhaltung (siehe Prozess im QM-/QS-Handbuch)

Zwecke der Verarbeitung	Erstellen von Finanzbuchhaltung und Nebenbüchern sowie Übermittlung an Behörden und andere Stellen
Kategorien betroffener Personen	<ul style="list-style-type: none"> <li>• Mandanten</li> <li>• Beschäftigte von Mandanten</li> <li>• Debitoren von Mandanten</li> <li>• Kreditoren von Mandanten</li> <li>• Beschäftigte der Behörden</li> <li>• Kooperationspartner und deren Beschäftigte</li> <li>• Beschäftigte von Versicherungen</li> </ul>
Datenkategorien	<ul style="list-style-type: none"> <li>• Stammdaten des Mandanten</li> <li>• Bewegungsdaten im Rahmen der Finanzbuchhaltung</li> <li>• Schriftverkehr</li> </ul>
Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden	<ul style="list-style-type: none"> <li>• Behörden</li> <li>• Mandanten</li> <li>• Sonstige Dritte auf Wunsch der Mandanten</li> <li>• IT-Dienstleister [soweit vorhanden]</li> </ul>

**Vergabeverfahren Lohnbuchhaltung und steuerrechtliche Beratung**

Ggf. Datenübermittlung in Drittstaaten	Grundsätzlich keine; in Sonderfällen im (zusätzlichen) Auftrag des Mandanten
Fristen für die Löschung der Datenkategorien	Siehe Löschkonzept
Technische und organisatorische Maßnahmen	Siehe IT-Sicherheitskonzept

**Weitere Verarbeitungstätigkeiten ergänzen:****Verarbeitungstätigkeit lfd. Nr. ....:**

Zwecke der Verarbeitung	
Kategorien betroffener Personen	
Datenkategorien	
Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden	
Ggf. Datenübermittlung in Drittstaaten	
Fristen für die Löschung der Datenkategorien	
Technische und organisatorische Maßnahmen	

## Vergabeverfahren Lohnbuchhaltung und steuerrechtliche Beratung

---

**Im IT-Sicherheitskonzept sollte zumindest auf folgende Aspekte eingegangen werden:**

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle/Berechtigungskonzepte
  - Trennungskontrolle
  - Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) in Ausnahmefällen
2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)
  - Weitergabekontrolle
  - Eingabekontrolle
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
  - Verfügbarkeitskontrolle
  - Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
  - Datenschutz-Management
  - Incident-Response-Management
  - Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
  - Auftragskontrolle