**Verzeichnis von Verarbeitungstätigkeiten der Steuerberatungskanzlei**

**im Sinne von Art. 30 Abs. 1 Datenschutz-Grundverordnung (DSGVO)**

**(Stand: tt.mm.jjjj)**

|  |
| --- |
| **Verantwortlicher** |
| Name bzw. Firma der verantwortlichen natürlichen oder juristischen Person |  |
| Ansprechperson |  |
| Postadresse |  |
| Telefon |  |
| E-Mail-Adresse |  |

|  |
| --- |
| **Datenschutzbeauftragter** [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] |  |

|  |
| --- |
| **Verarbeitungstätigkeit lfd. Nr. 1: Lohnbuchhaltung von Mandanten** |
| Zwecke der Verarbeitung | Erstellung der Lohnbuchhaltung, insb.* Berechnung der Lohn- und Gehaltsansprüche
* Berechnung von Abgaben und Steuern
* Erstellung und Bereitstellung der Lohn- und Gehaltsnachweise
* Beratung zur steuerlichen Gestaltung arbeitsrechtlicher Sachverhalte
 |
| Kategorien betroffener Personen | Beschäftigte von Mandanten |
| Kategorien von personenbezogenen Daten | Stammdaten der Beschäftigten, inkl. Angaben zu Familienstand, Schwerbehinderteneigenschaften und Kirchensteuerpflicht sowieSozialdatenAnsprechpersonen im erforderlichen Schriftverkehr mit externen StellenZeitaufzeichnungen für AbrechnungserstellungZeitaufzeichnungen für Abrechnungserstellung |
| Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden | * Personalabteilung
* Rechnungswesen
* Sozialversicherungsträger
* Finanzbehörden
* Kreditinstitute
* Versicherungen
* Gerichte
* Gläubiger
* IT-Dienstleister [soweit vorhanden]
 |
| 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 | * Mandanten
* Beschäftigte von Mandanten
* Debitoren von Mandanten
* Kreditoren von Mandanten
* Beschäftigte der Behörden
* Kooperationspartner und deren Beschäftigte
* Beschäftigte von Versicherungen
 |
| Datenkategorien | * Stammdaten des Mandanten
* Bewegungsdaten im Rahmen der Finanzbuchhaltung
* Schriftverkehr
 |
| Kategorien der Empfänger, denen personenbezogene Daten übermittelt werden | * Behörden
* Mandanten
* Sonstige Dritte auf Wunsch der Mandanten
* IT-Dienstleister [soweit vorhanden]
 |
| 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 |  |

**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