Verzeichnis von Verarbeitungstätigkeiten

gemäß Artikel 30 Datenschutz-Grundverordnung

(individualisierte Musterempfehlung der Bundessteuer-beraterkammer und des Deutschen Steuerberaterverbandes)

1. Name und Kontaktdaten des Verantwortlichen

Aufgrund der Kanzleigröße ist kein Datenschutzbeauftragter zu bestellen, der Kanzleiinhaber ist gleichzeitig Verantwortlicher für den Datenschutz. Die Kontaktdaten zur Erreichbarkeit lauten:

Verantwortlicher Datenschutz von Steuerberater Norbert Reuter **Dipl.-Kfm. Norbert Reuter**	Telefon: +49 3733 6759466 Telefax: +49 3733 6759469 E-Mail: nrt@nr-stb.tax Web: nr-stb.tax Adresse: Schwarzenberger Straße 18 09487 Schlettau

2. Mandantenbezogene Verarbeitungstätigkeiten

2.1. Fremde Finanzbuchhaltung (Verarbeitungstätigkeit lfd. Nr. 1)

Zwecke der Verarbeitung	Erstellen von Finanz- und Anlagenbuchhaltung Erfüllung von finanzbehördlichen Verpflichtungen
Art der Verarbeitung	Einsatz der Buchhaltungssoftware ‚Finanzbuchhal-tung', ‚hmd.fibu' und ‚hmd.anlag' der hmd-software AG Andechs (DATEV-kompatibel)
Ort der Verarbeitung	EDV-System Steuerkanzlei
Rechtmäßigkeit der Verarbeitung	Erfüllen eines Vertrages (Artikel 6 Absatz 1 Unterab-satz 1 Buchstabe b DSGVO)
Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO)
Kategorien betroffener Personen	Mandanten Beschäftigte von Mandanten Debitoren von Mandanten Kreditoren von Mandanten Sonstige Kooperationspartner von Mandanten
Kategorien personenbezogener Daten	Stammdaten des Mandanten Bewegungsdaten des Mandanten im Rahmen der Fi-nanz- und Anlagenbuchhaltung Schriftverkehr

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Herkunft der Daten	Mandanten
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Mandanten Finanzbehörden Sonstige Dritte auf Wunsch der Mandanten
Ggfs. Datenübermittlung in Drittstaaten	Grundsätzlich keine; in Sonderfällen auf Wunsch im (zusätzlichen) Auftrag des Mandanten
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre für Stamm- und Bewegungsdaten (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technische und organisatorische Maßnahmen sowie verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

2.2. Fremde Lohnbuchhaltung (Verarbeitungstätigkeit lfd. Nr. 2)

Zwecke der Verarbeitung	Erstellen von Lohnbuchhaltung Erfüllung von behördlichen Verpflichtungen
Art der Verarbeitung	Einsatz der Personalabrechnungssoftware ‚ed-lohn' der eurodata AG Saarbrücken
Ort der Verarbeitung	Cloud Rechenzentrum Saarbrücken
Rechtmäßigkeit der Verarbeitung	Erfüllen eines Vertrages (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b DSGVO) Ausübung von Rechten und Erfüllung von Pflichten aus dem Arbeits- und Sozialrecht unter Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9 Absatz 2 Buchstabe b DSGVO)
Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO)
Kategorien betroffener Personen	Mandanten Beschäftigte von Mandanten
Kategorien personenbezogener Daten	Stammdaten des Mandanten Stammdaten von Beschäftigten des Mandanten Bewegungsdaten von Beschäftigten des Mandanten im Rahmen der Lohnbuchhaltung (Entgelte, Zeitaufzeichnungen, Arbeitsunfähigkeitsbescheinigungen) Schriftverkehr

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Herkunft der Daten	Mandanten Beschäftigte von Mandanten
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Mandanten Finanzbehörden Sozialversicherungsträger Unfallversicherungsträger Sonstige Dritte (Gerichte, Gläubiger, Finanzinstitute, Versicherungen) bei besonderen Umständen der Beschäftigten
Ggfs. Datenübermittlung in Drittstaaten	Keine
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre für Stamm- und Bewegungsdaten (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

2.3. Fremder Jahresabschluss (Verarbeitungstätigkeit lfd. Nr. 3)

Zwecke der Verarbeitung	Erstellen von Jahresabschlüssen nach Handels- und Steuerrecht sowie von Gewinnermittlungen Erfüllung von behördlichen Verpflichtungen
Art der Verarbeitung	Einsatz der Buchhaltungssoftware ‚Jahresabschluss', ‚hmd.abschluss' und ‚hmd.anlag' der hmd-software AG Andechs (DATEV-kompatibel) Einsatz der Bürosoftware Microsoft Office
Ort der Verarbeitung	EDV-System Steuerkanzlei
Rechtmäßigkeit der Verarbeitung	Erfüllen eines Vertrages (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b DSGVO)
Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO)
Kategorien betroffener Personen	Mandanten Beschäftigte von Mandanten Debitoren von Mandanten Kreditoren von Mandanten Sonstige Kooperationspartner von Mandanten

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Kategorien personenbezogener Daten	Stammdaten des Mandanten Bewegungsdaten des Mandanten im Rahmen der Jahresabschlusstätigkeiten der Finanz- und Anlagenbuchhaltung, aus der bereits in der Kanzlei erstellten oder vom Mandanten übermittelten Finanz- und Anlagenbuchhaltung Schriftverkehr
Herkunft der Daten	Mandanten
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Mandanten Finanzbehörden Bundesanzeiger Sonstige Dritte (Finanzinstitute, Versicherungen) soweit vom Mandanten gewünscht oder durch die Dritten vom Mandanten gefordert
Ggfs. Datenübermittlung in Drittstaaten	Grundsätzlich keine; in Sonderfällen auf Wunsch im (zusätzlichen) Auftrag des Mandanten
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre für Stamm- und Bewegungsdaten (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

2.4. Fremde Steuererklärungen (Verarbeitungstätigkeit lfd. Nr. 4)

Zwecke der Verarbeitung	Erstellen von privaten Steuererklärungen Erstellen von betrieblichen Steuererklärungen
Art der Verarbeitung	Einsatz der Steuersoftware ‚hmd-est' und ‚hmd-steuern' der hmd-software AG Andechs Einsatz der Bürosoftware Microsoft Office
Ort der Verarbeitung	EDV-System Steuerkanzlei
Rechtmäßigkeit der Verarbeitung	Erfüllen eines Vertrages (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b DSGVO) Einwilligung der betroffenen Person für den festgelegten Zweck unter Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9 Absatz 2 Buchstabe a DSGVO

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO)
Kategorien betroffener Personen	Mandanten Beschäftigte von Mandanten Beschäftigte von Finanzbehörden
Kategorien personenbezogener Daten	Steuerliche Stammdaten des Mandanten Jahresbezogene Daten über steuerliche Sachverhalte des Mandanten Schriftverkehr
Herkunft der Daten	Mandanten Finanzbehörden
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Mandanten Finanzbehörden Sonstige Dritte auf Wunsch der Mandanten
Ggfs. Datenübermittlung in Drittstaaten	Keine
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre für Stamm- und Jahresdaten (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

2.5. Sonstige Mandantentätigkeiten (Verarbeitungstätigkeit lfd. Nr. 5)

Zwecke der Verarbeitung	Steuerrechtliche, wirtschaftliche Beratung und rechtliche (gemäß § 5 Absatz 1 RDG) Beratung Begleitung von Betriebsprüfungen der Finanzbehörden und Sozialversicherungsträger Führen von Rechtsbehelfen vor Finanzbehörden
Art der Verarbeitung	Einsatz der Bürosoftware Microsoft Office
Ort der Verarbeitung	EDV-System Steuerkanzlei
Rechtmäßigkeit der Verarbeitung	Einwilligung der betroffenen Person für den bestimmten Zweck (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a DSGVO) Erfüllen eines Vertrages (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b DSGVO)

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO)
Kategorien betroffener Personen	Mandanten Beschäftigte von Mandanten Sonstige Kooperationspartner von Mandanten Beschäftigte von Behörden
Kategorien personenbezogener Daten	Anlassbezogene Daten des Mandanten Schriftverkehr
Herkunft der Daten	Steuerkanzlei Mandanten (Finanz-)Behörden (anlassbezogen)
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Mandanten (Finanz-)Behörden (anlassbezogen) Sonstige Dritte (anlassbezogen)
Ggfs. Datenübermittlung in Drittstaaten	Grundsätzlich keine; in Sonderfällen auf Wunsch im (zusätzlichen) Auftrag des Mandanten
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre, wenn für die Besteuerung von Bedeutung (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre in sonstigen Fällen 10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

3. Kanzleibezogene Verarbeitungstätigkeiten

3.1. Eigenorganisation (Verarbeitungstätigkeit lfd. Nr. 6)

Zwecke der Verarbeitung	Posteingang und Postausgang Fristenkontrolle Fakturierung und Mahnwesen Sonstige Korrespondenz
Art der Verarbeitung	Einsatz der Kanzleisoftware ‚hmd-orga' der hmd-software AG Andechs Einsatz der Bürosoftware Microsoft Office
Ort der Verarbeitung	EDV-System Steuerkanzlei

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Rechtmäßigkeit der Verarbeitung	Erfüllen eines Vertrages (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe b DSGVO) Wahrung der berechtigten Kanzleiinteressen (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DSGVO)
Erforderlichkeit der Verarbeitung	Für festgelegten Zweck auf das notwendigste Maß beschränkt (Artikel 5 Absatz 1 Buchstabe c DSGVO)
Kategorien betroffener Personen	Beschäftigte der Steuerkanzlei Mandanten Beschäftigte von Mandanten Sonstige Kooperationspartner von Mandanten Beschäftigte von Behörden
Kategorien personenbezogener Daten	Anlassbezogene Daten der Kanzlei Anlassbezogene Daten des Mandanten Schriftverkehr
Herkunft der Daten	Steuerkanzlei Mandanten Behörden
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Mandanten Behörden
Ggfs. Datenübermittlung in Drittstaaten	Keine
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

3.2. Personalverwaltung (Verarbeitungstätigkeit lfd. Nr. 7)

Zwecke der Verarbeitung	Bewerbungsverfahren, Einstellen von Personal Verwaltung der Personalangelegenheiten (Abwicklung von Arbeitsverträgen, Erstellen der Lohnbuchhaltung Erfüllung von behördlichen Verpflichtungen)
Art der Verarbeitung	Einsatz der Personalabrechnungssoftware ‚ed-lohn' der eurodata AG Saarbrücken Einsatz der Bürosoftware Microsoft Office
Ort der Verarbeitung	Cloud Rechenzentrum Saarbrücken EDV-System Steuerkanzlei

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Rechtmäßigkeit der Verarbeitung	Erfüllung einer rechtlichen Verpflichtung (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe c DSGVO) Wahrung der berechtigten Kanzleiinteressen (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DSGVO) Ausübung von Rechten und Erfüllung von Pflichten aus dem Arbeits- und Sozialrecht unter Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9 Absatz 2 Buchstabe b DSGVO)
Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO) Für festgelegten Zweck auf das notwendigste Maß beschränkt (Artikel 5 Absatz 1 Buchstabe c DSGVO)
Kategorien betroffener Personen	Beschäftigte der Steuerkanzlei
Kategorien personenbezogener Daten	Bewerbungsunterlagen Stammdaten von Beschäftigten der Kanzlei Bewegungsdaten von Beschäftigten der Kanzlei im Rahmen der Lohnbuchhaltung (Entgelte, Zeitaufzeichnungen, Arbeitsunfähigkeitsbescheinigungen) Leistungsbeurteilungen Schriftverkehr
Herkunft der Daten	Beschäftigte der Steuerkanzlei
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Personalabteilung Rechnungswesen Finanzbehörden Sozialversicherungsträger Unfallversicherungsträger Sonstige Dritte (Gerichte, Gläubiger, Finanzinstitute, Versicherungen) bei besonderen Umständen der Beschäftigten
Ggfs. Datenübermittlung in Drittstaaten	Keine
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre für Stamm- und Bewegungsdaten (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre für allgemeinen Schriftverkehr 6 Monate für Unterlagen von abgelehnten Bewerbern Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

3.3. Eigenes Rechnungswesen (Verarbeitungstätigkeit lfd. Nr. 8)

Zwecke der Verarbeitung	Erstellen von Finanz- und Anlagenbuchhaltung sowie der Gewinnermittlung der Steuerkanzlei Erfüllung von finanzbehördlichen Verpflichtungen
Art der Verarbeitung	Einsatz der Buchhaltungssoftware ‚Finanzbuchhaltung', ‚hmd.fibu', ‚Jahresabschluss', ‚hmd.abschluss' und ‚hmd.anlag' der hmd-software AG Andechs (DATEV-kompatibel) Einsatz der Bürosoftware Microsoft Office
Ort der Verarbeitung	EDV-System Steuerkanzlei
Rechtmäßigkeit der Verarbeitung	Erfüllung einer rechtlichen Verpflichtung (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe c DSGVO)
Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO)
Kategorien betroffener Personen	Beschäftigte der Steuerkanzlei Debitoren der Steuerkanzlei (Mandanten) Kreditoren der Steuerkanzlei Sonstige Kooperationspartner der Steuerkanzlei
Kategorien personenbezogener Daten	Stammdaten der Steuerkanzlei Bewegungsdaten der Steuerkanzlei im Rahmen der Finanz- und Anlagenbuchhaltung sowie der Jahresabschlusserstellung Schriftverkehr
Herkunft der Daten	Steuerkanzlei
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Finanzbehörden
Ggfs. Datenübermittlung in Drittstaaten	Keine
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre für Stamm- und Bewegungsdaten (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

3.4. Eigene Steuererklärungen (Verarbeitungstätigkeit lfd. Nr. 9)

Zwecke der Verarbeitung	Erstellen der Kanzlei-Steuererklärungen und der persönlichen Steuererklärungen des Kanzleiinhabers
Art der Verarbeitung	Einsatz der Steuersoftware ‚hmd-est' und ‚hmd-steuern' der hmd-software AG Andechs Einsatz der Bürosoftware Microsoft Office
Ort der Verarbeitung	EDV-System Steuerkanzlei
Rechtmäßigkeit der Verarbeitung	Erfüllung einer rechtlichen Verpflichtung (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe c DSGVO)
Erforderlichkeit der Verarbeitung	Für festgelegten Zweck unerlässlich (Artikel 5 Absatz 1 Buchstabe b DSGVO)
Kategorien betroffener Personen	Inhaber der Steuerkanzlei und dessen Angehörige
Kategorien personenbezogener Daten	Steuerliche Stammdaten des Kanzleiinhabers Jahresbezogene Daten über steuerliche Sachverhalte des Kanzleiinhabers Schriftverkehr
Herkunft der Daten	Steuerkanzlei Finanzbehörden
Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt werden	Finanzbehörden
Ggfs. Datenübermittlung in Drittstaaten	Keine
Fristen, nach welcher die Löschung der Datenkategorien vorgesehen sind	14 Jahre für Stamm- und Jahresdaten (die Frist beginnt bei Dauersachverhalten erst nach dem Ende der Vertragsdauer), einzelfallbezogen auch länger 10 Jahre für allgemeinen Schriftverkehr Siehe auch Punkt 4. Allgemeine Löschhinweise
Technisch und organisatorische Maßnahmen und verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	Siehe hierzu Punkt 5. Technische und organisatorische Maßnahmen
Datenschutz-Folgenabschätzung	Nicht notwendig, da kein hohes Risiko (im Sinne von Artikel 35 Absatz 1 DSGVO) bei der Datenverarbeitung besteht

4. Allgemeine Löschhinweise *(individualisierter Musterhinweis der Bundessteuerberaterkammer)*

Die Aufbewahrungsfristen richten sich nach dem Zweck der Verarbeitung. Diese können sich aus den rechtlichen Aufbewahrungspflichten, den Einwilligungen der betroffenen Personen sowie aus der Erforderlichkeit zur Vertragsabwicklung ergeben.

Die Aufbewahrungspflichten ergeben sich zunächst aus dem Steuer- und Handelsrecht. Regelmäßig werden dabei die Aufbewahrungspflichten des Mandanten im Rahmen des Auftrages vom Steuerberater übernommen.

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Die Aufbewahrungsfrist läuft nicht ab, solange die Unterlagen für Steuern von Bedeutung sind, deren Festsetzungsfrist noch nicht abgelaufen ist (Ablaufhemmung).

Schriftstücke (Daten), die der Verantwortliche aus Anlass seiner beruflichen Tätigkeit vom Mandanten oder für ihn erhalten hat (Handakte gemäß § 66 StBerG), sind grundsätzlich für die Dauer von 10 Jahren nach Auftragsbeendigung aufzubewahren.

Somit ist eine Aufbewahrungsfrist von mindestens 10 Jahren unabdingbar. Aus Gründen der Ablaufhemmung wird noch ein pauschaler Sicherheitszuschlag von 4 Jahren vorgenommen. Somit ergibt sich die bei den einzelnen Verarbeitungstätigkeiten genannte vorgesehene Löschfrist von regelmäßig 14 Jahren.

Nach diesem Zeitraum von 14 Jahren ist zusätzlich einzelfallbezogen zu prüfen, ob Rechtfertigungsgründe für eine weitere Aufbewahrung vorliegen. Dabei muss ggfs. auch eine längere Verjährungsfrist (zB. nach BGB) beachtet werden.

Rechtfertigungsgründe könnten sich u.a. aus den folgenden Sachverhalten ergeben:

- Dokumentation einer Geschäftsaufgabeerklärung (Folgewirkung auch für Erben),
- Pensionszusage,
- Grundstückskaufvertrag,
- Absicherung der Verfolgungsmöglichkeit von titulierten Vergütungsansprüchen,
- Änderung aufgrund neuer Tatsachen,
- Verteidigungsmöglichkeiten gegen denkbare Haftungsforderungen des Mandanten wegen erst zukünftig eintretender Schäden.

Für allgemeinen Schriftverkehr ist ein pauschaler Sicherheitszuschlag nicht notwendig. Somit ergibt sich hier die bei den einzelnen Verarbeitungstätigkeiten genannte vorgesehene Löschfrist von regelmäßig 10 Jahren.

Sollten Dokumente mit personenbezogenen Daten weder nach Steuer- und Handelsrecht noch nach Berufsrecht aufbewahrungspflichtig sein (zB. Bewerbungsunterlagen) ergibt sich kein Rechtfertigungsgrund für eine längere Aufbewahrung. Kanzleiseitig ist für diese Dokumente eine Löschfrist nach 6 Monaten vorgesehen. In dieser Zeit werden die Dokumente noch aus organisatorischen Gründen und für eventuelle Rückfragen vorgehalten.

Wegen der berufsrechtlichen Aufbewahrungspflicht ist gemäß § 66 Absatz 1 Satz 2 StBerG ergänzend darauf hinzuweisen, dass diese Verpflichtung bei Übergabe der Handakten an den Mandanten erlischt, die Aufbewahrungspflicht erlischt zudem 6 Monate, nachdem der Mandant die Aufforderung erhalten hat, die Handakten in Empfang zu nehmen.

5. Technische und organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Steuerkanzlei erfüllt diesen Anspruch durch folgende Maßnahmen:

5.1. Vertraulichkeit gemäß Artikel 32 Absatz 1 Buchstabe b DSGVO

5.1.1. Zutrittskontrolle

Es handelt sich um Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Manuelles Schließsystem	☑ Schlüsselregelung / Liste
☑ Sicherheitsschlösser	

5.1.2. Zugangskontrolle

Es handelt sich um Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Login mit Benutzername + Passwort	☑ Verwalten von Benutzerberechtigungen
☑ Anti-Viren-Software Server	☑ Erstellen von Benutzerprofilen
☑ Anti-Virus-Software Clients	☑ Zentrale Passwortvergabe
☑ Anti-Virus-Software mobile Geräte	☑ Richtlinie „Löschen / Vernichten“
☑ Firewall	☑ Richtlinie „Clean Desk“
☑ Intrusion Detection Systeme (IDS)	☑ Allgemeine Richtlinie Datenschutz
☑ Einsatz VPN bei Remote-Zugriffen	☑ Allgemeine Richtlinie Datensicherheit
☑ Automatische Desktopsperre	☑ Anleitung „Manuelle Desktopsperre“

5.1.3. Zugriffskontrolle

Es handelt sich um Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Ordnungsgemäße Aktenvernichtung (DIN 66399)	☑ Einsatz Berechtigungskonzepte
☑ Physische Löschung von Datenträgern	☑ Minimale Anzahl an Administratoren
☑ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☑ Verwaltung Benutzerrechte durch Administratoren
	☑ Einsatz von zertifizierten Dienstleistern zur Akten- und Datenvernichtung

5.1.4. Trennungskontrolle

Es handelt sich um Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Trennung von Produktiv- und Testumgebung	☑ Steuerung über Berechtigungskonzept

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☑ Festlegung von Datenbankrechten
☑ Mandantenfähigkeit relevanter Anwendungen	☑ Logische Mandantentrennung
	☑ Datensätze sind mit Zweckattributen versehen

5.1.5. Pseudonymisierung gemäß Artikel 32 Absatz 1 Buchstabe a DSGVO

Es handelt sich um Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	☑ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

5.2. Integrität gemäß Artikel 32 Absatz 1 Buchstabe b DSGVO

5.2.1. Weitergabekontrolle

Es handelt sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Einsatz von VPN	☑ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☑ Protokollierung der Zugriffe und Abrufe	☑ Persönliche Übergabe mit Protokoll
☑ Sichere Transportbehälter	
☑ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☑ Nutzung von Signaturverfahren	

5.2.2. Eingabekontrolle

Es handelt sich um Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☑ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☑ Manuelle Kontrolle der Protokolle	☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☑ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☑ Klare Zuständigkeiten für Löschungen

5.3. Verfügbarkeit und Belastbarkeit gemäß Artikel 32 Absatz 1 Buchstabe b DSGVO

5.3.1. Verfügbarkeitskontrolle

Es handelt sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Feuerlöscher Serverraum	☑ Backup & Recovery-Konzept
☑ Schutzsteckdosenleisten Serverraum	☑ Kontrolle des Sicherungsvorgangs
☑ RAID System / Festplattenspiegelung	☑ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
	☑ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
	☑ Getrennte Partitionen für Betriebssysteme und Daten
	☑ Keine sanitären Anschlüsse im oder oberhalb des Serverraums

5.3.2. Belastbarkeitskontrolle

Es handelt sich um Maßnahmen, die gewährleisten, dass technische Systeme bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Mit vertretbarem Aufwand nicht umsetzbar	☑ Fortwährende Überprüfung geeigneter Testmöglichkeiten

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

5.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gemäß Artikel 32 Absatz 1 Buchstabe d DSGVO iVm. Artikel 25 Absatz 1 DSGVO

5.4.1. Datenschutz-Management

Es handelt sich um allgemeine Maßnahmen zur Erfüllung der datenschutzrechtlichen Vorgaben.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt	☑ Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
	☑ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	☑ Die (derzeit nicht notwendige) Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☑ Die Organisation kommt den Informationspflichten nach Artikel 13 und 14 DSGVO nach
	☑ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

5.4.2. Störungs-Management (Incident Response)

Es handelt sich um allgemeine Maßnahmen zur vorbeugenden Verhinderung von Störungen und Datenpannen und zur Vorgehensweise bei Sicherheitsvorfällen und Datenpannen.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Einsatz von Firewall und regelmäßige Aktualisierung	☑ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☑ Einsatz von Spamfilter und regelmäßige Aktualisierung	☑ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☑ Einsatz von Virenscanner und regelmäßige Aktualisierung	☑ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☑ Intrusion Detection System (IDS)	
☑ Intrusion Prevention System (IPS)	

5.4.3. Datenschutzfreundliche Voreinstellungen gemäß Artikel 25 Absatz 2 DSGVO (Privacy by Design / Privacy by Default)

Es handelt sich um allgemeine Maßnahmen zur Erfüllung der datenschutzrechtlichen Vorgaben, welche durch Voreinstellungen verhindern sollen, dass eine größere Datenmenge erhoben, verarbeitet und gespeichert wird, als für die Verarbeitungszwecke erforderlich ist.

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☑ Verhinderung, dass die erhobenen Daten einer unbestimmten Anzahl von Personen zugänglich gemacht werden	
☑ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

5.4.4. Auftragskontrolle (Outsourcing an Dritte)

Es handelt sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	☑ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	☑ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
	☑ Schriftliche Weisungen an den Auftragnehmer
	☑ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☑ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	☑ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☑ Regelung zum Einsatz weiterer Subunternehmer
	☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☑ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

5.5. Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zweck der Datenverarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax

Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat die Steuerkanzlei mit den unter Punkt 5.1. bis 5.4. dargestellten technischen und organisatorischen Maßnahmen die geeigneten TOM getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten gemäß Artikel 32 Absatz 1 DSGVO zu gewährleisten.

Ein verbleibendes Restrisiko - insbesondere durch kriminelle oder terroristische Handlungen - kann naturgemäß nicht vollständig ausgeschlossen werden. Die Implementierungskosten von technischen Maßnahmen zur weiteren Minimierung dieses Restrisikos würden jedoch in keinem Verhältnis zur Kanzleigröße und derer Wirtschaftlichkeit stehen.

6. Stand und Aktualisierung dieses Verzeichnisses

Dieses Verzeichnis von Verarbeitungstätigkeiten hat den Stand vom 25. Mai 2018. Ich behalte mir vor, dieses Verzeichnis zu gegebener Zeit zu aktualisieren, um den Datenschutz zu verbessern und/oder an geänderte Verarbeitungstätigkeiten, Behördenpraxis oder Rechtsprechung anzupassen.

Gesetzeslegende	BGB Bürgerliches Gesetzbuch	DSGVO Datenschutzgrundverordnung
	RDG Rechtsdienstleistungsgesetz	StBerG Steuerberatungsgesetz

Steuerberater Norbert Reuter
09487 Schlettau
Schwarzenberger Straße 18
Telefon: 03733 / 6759465
E-Mail: info@nr-stb.tax