Datenschutz-Folgenabschätzung
für Verarbeitungstätigkeiten für Klienten

Inhalt

I. Allgemeine Information zur Kanzlei

1. Name und Kontaktdaten der Kanzlei	
Name/Firmenwortlaut der Kanzlei:	Steuerberater Franz Schmid
Adresse:	Kirchgasse 10, 6200 Jenbach
E-Mail-Adresse:	franz.schmid@schmid-stb.at
2. Name und Kontaktdaten des Datenschutzbeauftragten (sofern bestellt)	
Name:	
Adresse:	
E-Mail-Adresse:	
Telefonnummer:	

II. Beschreibung der Verarbeitungstätigkeit

Bezeichnung der Verarbeitungstätigkeit	Die Verarbeitungstätigkeiten sind • Steuerberatung, • die Lohnverrechnung für Klienten und • Finanz- und Geschäftsbuchhaltung für Klienten.
Datenkategorien, Verarbeitungszwecke, Übermittlungsempfänger, Speicherdauer	Siehe beiliegendes Verzeichnis der Verarbeitungstätigkeiten.
Art, Umfang und Kontext der Verarbeitung	Kontext der Verarbeitung ist die Ausübung des freien Berufes des Verantwortlichen nach Maßgabe des WTBG 2017. Art und Umfang der Verarbeitung ergeben sich zwingend aus dem standesrechtlichen Berechtigungsumfang des Verantwortlichen gem. §§ 2 f WTBG 2017. Die Anzahl der Betroffenen entspricht der Anzahl der Klienten des Verantwortlichen zuzüglich der Anzahl jener Personen, deren personenbezogene Daten dem Verantwortlichen von seinen Klienten übermittelt werden. Derzeit hat der Verantwortliche 132 Klienten und führt 2 Personen in der Lohnverrechnung.
Funktionale Beschreibung der Datenverarbeitung	Der Verantwortliche verarbeitet die gegenständlichen personenbezogenen Daten im Rahmen des regulären Kanzleibetriebs eines Berufsträgers, wozu auch die im Berechtigungsumfang des Verantwortlichen gem. §§ 2 f WTBG 2017 implizit vorgesehenen Übermittlungen an Gerichte und Behörden zählen. Die Verarbeitung in der Kanzlei des Verantwortlichen erfolgt vor allem mittels Standard-Büro-Software (z.B. Microsoft Word, Microsoft Outlook) sowie spezialisierter Standard-Software für Wirtschaftstreuhänder. Darüber hinaus erfolgt eine im Stand der Wirtschaftstreuhänder übliche Aktenführung für alle Klienten.
Verwendete Ressourcen (Software, Hardware, Personal)	Der Verantwortliche setzt folgende Ressourcen zur Verarbeitung der gegenständlichen personenbezogenen Daten ein:

	– Hardware
	  – PCs bzw. Laptops;
	  – Computer-Peripherie (z.B. Drucker, Scanner)
	  – Internet-Zugangsgerät (z.B. Modem)
	– Software
	  – Standard-Büro-Software
	  – spezialisierte Standard-Software für Wirtschaftstreuhänder
	  – externe Datenbank zur Durchführung der Geldwäscheprüfung (World-Check von Thomson Reuters)
	– Personal
	  – Kanzleipartner
	  – Sekretariatskräfte
	  – Substituten, je nach Bedarf

III. Prüfung der Rechtmäßigkeit

1. Grundsätze der Datenverarbeitung einschließlich Rechtsgrundlage für die Verarbeitung	
Rechtmäßigkeit – Welche Rechtsgrundlage?	Der Verantwortliche verarbeitet die gegenständlichen personenbezogenen Daten gestützt auf folgende Rechtsgrundlagen: – der Notwendigkeit zur Erfüllung der vom Verantwortlichen mit seinen Klienten (als Betroffene) geschlossenen Verträge (Art. 6 Abs. 1 lit. b DSGVO); – das überwiegende berechtigte Interesses des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DSGVO; Art. 10 DSGVO i.V.m. § 4 Abs. 3 Z. 2 DSG); – soweit es sich um sensible Daten handelt auf der gesetzlichen Grundlage des WTBG 2017 (i.V.m. Art. 9 Abs. 2 lit. g DSGVO).
Zweckbindung	Der Verantwortliche unterliegt dem WTBG 2017 einschließlich den Richtlinien für die Ausübung der Wirtschaftstreuhandberufe (WT-Ausübungsrichtlinien gemäß § 72 WTBG 2017). Insbesondere die standesrechtlichen Regelungen zur Befangenheit und der Interessenskollision (§§ 14 f WT-AARL 2017-KSW) wirken einer zweckwidrigen Verwendung personenbezogener Daten von Klienten entgegen. Darüber hinaus hat der Verantwortliche seine Mitarbeiter dazu angewiesen, die von einem Klienten erhaltenen personenbezogenen Daten ausschließlich für die Zwecke der Bearbeitung des Mandates zu verwenden und insbesondere die standesrechtliche Verschwiegenheit zu wahren.
Datenminimierung	Der Verantwortliche handelt stets im Interesse seiner Klienten und erhebt personenbezogene Daten ausschließlich in jener Art und in jenem Umfang, die für die erfolgreiche Bearbeitung eines Mandats erforderlich sind. Der Verantwortliche hat seine Mitarbeiter außerdem instruiert personenbezogene Daten im Rahmen eines Mandates immer nur zu erheben, soweit dies im Interesse des Klienten geboten ist.

Datenminimierung	Der Verantwortliche handelt stets im Interesse seiner Klienten und erhebt personenbezogene Daten ausschließlich in jener Art und in jenem Umfang, die für die erfolgreiche Bearbeitung eines Mandats erforderlich sind. Der Verantwortliche hat seine Mitarbeiter außerdem instruiert personenbezogene Daten im Rahmen eines Mandates immer nur zu erheben, soweit dies im Interesse des Klienten geboten ist.
Speicherbegrenzung	Personenbezogene Daten werden nur solange aufbewahrt bis zum Ablauf der einschlägigen Verjährungs- und Aufbewahrungsfristen; darüber hinaus bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden.
Sicherheit	Die vom Verantwortlichen implementierten technischen und organisatorischen Maßnahmen befinden sich im Anhang. Diese gewährleisten eine angemessene Sicherheit aller vom Verantwortlichen personenbezogenen Daten. Der Verantwortliche schließt zudem mit seinen Auftragsverarbeitern Auftragsverarbeitervereinbarungen ab, welche die Auftragsverarbeiter ebenso zur Gewährleistung einer angemessenen Datensicherheit verpflichten.
2. Eingesetzte Auftragsverarbeiter	
Welche Auftragsverarbeiter und Sub-Auftragsverarbeiter werden eingesetzt und (i) hat sich der Verantwortliche von ihrer Zuverlässigkeit überzeugt und (ii) sind rechtskonforme Auftragsverarbeiter-vereinbarungen geschlossen worden?	Der Verantwortliche bedient sich zur Verarbeitung der gegenständlichen personenbezogenen Daten folgenden Auftragsverarbeiter: • Florian Reitmeir, Maria Theresienstr. 47 6020 Innsbruck • Software Studio GmbH, Grabenweg 72, 6020 Innsbruck • RZL Software GmbH, Hannesgrub Nord 35, 4911 Tumeltsham • Schweighofer Software GmbH, Hannesgrub Nord 35, 4911 Tumeltsham Der Verantwortliche hat im Rahmen der Auswahl der Auftragsverarbeiter insbesondere durch Einholung von Informationen aus dem Markt eine

	Überprüfung der Zuverlässigkeit der Auftragsverarbeiter vorgenommen. Der Verantwortliche hat die Rechtmäßigkeit der mit seinen Auftragsverarbeitern geschlossenen Auftragsverarbeitervereinbarungen gemäß Art. 28 DSGVO geprüft und hat keine Defizite hierbei festgestellt.
3. Internationale Datenübermittlungen	
Gibt es Datenübermittlungen in Drittländer oder an internationale Organisationen?	Es erfolgen keine Datenübermittlungen in Länder außerhalb der EU bzw. des EWR.
4. Datenschutzmitteilung an Betroffene	
Ist die entworfene Datenschutzmitteilung rechtskonform?	Die Datenschutzmitteilung des Verantwortlichen basiert auf einem von der Kammer der Steuerberater und Wirtschaftsprüfer zur Verfügung gestellten Musters, welches den Anforderungen der DSGVO entspricht. Der Verantwortliche hat diese auf seine Bedürfnisse hin angepasst und seinen Klienten zugänglich gemacht.
5. Betriebsvereinbarung	
Ist eine Betriebsvereinbarung erforderlich?	Eine Betriebsvereinbarung ist nicht erforderlich, da kein Betriebsrat besteht.
6. Möglichkeit für die Betroffenen, ihre Rechte geltend zu machen	
Wie sieht der Prozess zur Geltendmachung der Betroffenenrechte und ihrer Umsetzung beim Verantwortlichen aus?	In der Datenschutzerklärung des Verantwortlichen sind die Kontaktdaten für Anfragen von betroffenen Personen angegeben. Diese Anfragen werden unverzüglich an die Partner der Kanzlei weitergeleitet und einer umgehenden Bearbeitung zugeführt.

IV. Involvierung des Datenschutzbeauftragten und der Betroffenen

In welcher Form wurde der Datenschutzbeauftragte involviert?	Der Verantwortliche ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet und hat eine solche Bestellung auch nicht freiwillig vorgenommen.

In welcher Form wurde der Standpunkt der Betroffenen erhoben und berücksichtigt?	Der Verantwortliche hat mit ausgewählten Klienten das Gespräch zu Fragen des Datenschutzes gesucht und durch offene Fragen die Befindlichkeiten, Anliegen und Sorgen seiner Klienten erhoben.

V. Risiken für die Betroffenen

1. Identifikation und vorläufige Bewertung der Risiken für die Betroffenen		
Beschreibung des Risikos	Vorläufige Bewertung (niedrig/mittel/hoch)	Risikominderungsmaßnahme (allenfalls mit Umsetzungsfrist)
Verlust der Verfügbarkeit, Vertraulichkeit oder Integrität der gegenschändlichen personenbezogenen Daten durch Schadsoftware (z.B. Spyware oder Ransomware) bzw. Hacker	mittel	Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt. Alle eingehenden E-Mails werden automatisch auf Schadsoftware gescannt. Die eingesetzte Anti-Viren-Software verfügt über die Funktion, Schadsoftware automatische zu entfernen. Weiters werden hoch-kritische Sicherheitsupdates für Software binnen 3 Arbeitstagen installiert (zu diesem Zweck ist die automatische Installation von Software-Updates grundsätzlich aktiviert); Sicherheits-Updates mittlerer Kritikalität werden grundsätzlich binnen 25 Arbeitstagen und Updates geringer Kritikalität binnen 40 Arbeitstagen installiert.
Verlust der Verfügbarkeit der Daten durch Hardwarefehler oder Naturkatastrophen	niedrig bis mittel	Es werden regelmäßig Datensicherungen (Backups) erstellt und sicher aufbewahrt. Es wird ein Konzept zur raschen Wiederherstellung von Datensicherungen entwickelt, um nach einer Sicherheitsverletzung zeitnah den regulären Betrieb wieder herstellen zu können.
Verlust der Vertraulichkeit der Daten durch unsichere Datenentsorgung	niedrig bis mittel	Papier, welches personenbezogene Daten enthält, wird grundsätzlich geschreddert bzw. einem externen Dienstleister zur sicheren Vernichtung übergeben. Datenträger werden vor ihrer Entsorgung vollständig überschrieben oder physisch zerstört, sodass die darauf

		gespeicherten Daten nicht wieder hergestellt werden können.
Verlust der Vertraulichkeit durch Diebstahl von Computer-Hardware	mittel	Der Zugang zu Räumlichkeiten, in denen sich Computer befinden, auf denen die gegenständlichen Daten gespeichert sind, ist durch Zugangskontrollmaßnahmen gesichert. Schlüssel, welchen den Zugang zu den Kanzleiräumlichkeiten oder Teilen derselben ermöglichen, werden nur an besonders vertrauenswürdige Personen ausgehändigt und dies auch nur soweit und solange diese Personen tatsächlich einen eigenen Schlüssel benötigen.
Zugriff durch unbefugtes kanzleiinternes Personal auf Daten	niedrig	Jede Person hat ihren eigenen Benutzer-Account – das Teilen von Benutzer-Accounts ist untersagt. Die Vergabe von Zugriffsberechtigungen erfolgt nach dem „Need-to-Know“-Prinzip.
Zugriff durch unbefugte kanzleiexterne Personen auf Daten	mittel	Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung. Soweit Passwörter zur Authentifizierung eingesetzt werden, sind diese mindestens 8 Zeichen lang und bestehen aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen. Passwörter werden ausschließlich verschlüsselt gespeichert. Mobile Endgeräte und mobile Datenträger werden

		verschlüsselt, zumindest soweit auf diesen Geräten Daten der Lohnverrechnung oder sensible Daten gespeichert werden.
Zugriff ehemaliger Mitarbeiter auf Daten	mittel	Mitarbeiter des Verantwortlichen werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden sie dazu verpflichtet, personenbezogene Daten nur auf ausdrücklicher Anweisung eines Vorgesetzten an Dritte zu übermitteln. Bei Ausscheiden eines Mitarbeiters werden seine Benutzerkonten inaktiv gesetzt oder gelöscht.
Verlust der Vertraulichkeit und Integrität der Daten am Übertragungsweg	mittel	Personenbezogene Daten werden auf dem Übertragungsweg über das Internet verschlüsselt, zumindest soweit es sich um Daten der Lohnverrechnung oder sensible Daten handelt. Die E-Mail-Kommunikation erfolgt insofern grundsätzlich verschlüsselt, dass der Mail-Server des Verantwortlichen per Default unter Verwendung des Protokolls Transport Layer Security (TLS) mit anderen Mail-Servern kommuniziert.
Zugriff durch unbefugte kanzleiexterne Personen auf das interne Netzwerk des Verantwortlichen	mittel	Es wird eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit angemessen – eingehenden Netzwerkverkehr blockiert.
Weitergabe von Zugangsdaten an unbefugte Dritte	mittel	Die Mitarbeiter des Verantwortlichen werden zu Fragen der Datensicherheit geschult und angemessen über Fragen der Datensicherheit informiert (z.B. Passwortsicherheit, Passwortweitergabe).

Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit durch Lücken in technischen und organisatorischen Maßnahmen des Verantwortlichen	mittel	Der Verantwortliche evaluiert in regelmäßigen Abständen seine technischen und organisatorischen Maßnahmen.
Verletzung des Datengeheimnisses durch Auftragsverarbeiter	mittel bis hoch	Es wurden Auftragsverarbeiter-vereinbarungen mit allen Auftragsverarbeitern geschlossen.

2. Bewertung des Restrisikos

Risikoklassifizierung (niedrig/mittel/hoch)	**Mittel – Eine Konsultation der Datenschutzbehörde ist nicht erforderlich.**
Erläuterung der Risikoklassifizierung	Aufgrund der bereits implementierten Sicherheitsmaßnahmen ist das verbleibende Restrisiko als mittel einzustufen.

_____

_____

Ort, Datum
Verantwortlichen

_____

Unterschrift namens des