Vereinbarung

zur Auftragsverarbeitung

zwischen der

smartdocu Solutions GmbH
Mitterweg 1
83339 Chieming

- nachfolgend Auftragnehmer oder smartdocu genannt -

und

_____

_____

_____

- nachfolgend Auftraggeber oder Kunde genannt -

- beide gemeinsam nachfolgend Vertragsparteien genannt –

Präambel

Der Auftragnehmer stellt dem Auftraggeber das Produkt smartdocu cloud auf der Grundlage einer gesonderten Vereinbarung zur Nutzung zur Verfügung. In diesem Rahmen werden auch personenbezogene Daten zwischen dem Auftragnehmer und dem Auftraggeber übermittelt. Daher gehen die Vertragsparteien ein Auftragsverarbeitungsverhältnis gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) ein. Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1

Inhalt der Vereinbarung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Art. 28 DSGVO als Dienstleister ausgewählt. Eine inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.

(2) Dieser Vertrag enthält nach dem Willen der Vertragsparteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsdatenverarbeitung iSd. Art. 28 DSGVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(3) Sofern der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung, Anonymisieren, Pseudonymisieren, Verschlüsseln oder sonstige Nutzung von Daten.

§ 2

Gegenstand und Dauer der Auftragsverarbeitung

(1) Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer sind alle folgenden Kategorien von Daten und Dokumente:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten
- Protokolldaten

Bei Nutzung des Produkts digitale Notfallakte außerdem:

- Versicherungs- und Bankdaten
- Eigentumsverhältnisse

Bei Nutzung des Produkts Einkommensteuer-Vorerfassung außerdem:

- Steuerrelevante Daten und Belege

(2) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst die Kunden und ihre Mandanten.

(3) Der Zweck der vorgesehenen Verarbeitung personenbezogener Daten erfasst

- die Identifizierung als berechtigter Nutzer von smartdocu cloud;
- die Korrespondenz mit den berichtigten Nutzern;
- die Nutzung des Produktes smartdocu cloud im Rahmen der getroffenen Vereinbarung sowie
- die personenunabhängige und identitätsunabhängige Analyse und Auswertung der Nutzung von smartdocu cloud zur Verbesserung des Leistungsangebotes.

(4) Gleichzeitig erteilt der Auftraggeber dem Auftragnehmer die Weisung, personenbezogene Daten der Mandanten des Auftraggebers zu erheben und zu verarbeiten.

(5) Das Auftragsverhältnis besteht, solange der Auftraggeber ein Vertragsverhältnis mit dem Auftragnehmer zur Erbringung von Dienstleistungen und anderen Leistungen unterhält.

§ 3

Rechte und Pflichten des Auftraggebers, Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten sowie von etwaig überlassenen Datenträgern verlangen. Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen können von dem Auftraggeber danach in schriftlicher Form oder in Textform durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

Weisungsberechtigte Personen des Verantwortlichen sind:

_____

(Vorname, Name, Organisationseinheit, Telefon)

_____

(Vorname, Name, Organisationseinheit, Telefon)

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

(4) Alle erteilten Weisungen sind vom Auftraggeber und vom Auftragnehmer zu dokumentieren.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Die Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland statt. Eine Verlagerung in einen Staat außerhalb des Hoheitsgebiets der Bundesrepublik Deutschland bedarf der vorherigen Zustimmung des Auftraggebers.

§ 4
Pflichten des Auftragnehmers

(1) Neben den vertraglichen Regelungen dieser Vereinbarung treffen den Auftragnehmer die nachfolgenden gesetzlichen Pflichten.

(2) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter auf die Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 2 lit. b) DSGVO) verpflichtet und in die Schutzbestimmungen der DSGVO und des Bundesdatenschutzgesetzes (BDSG) eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(4) Der Auftragnehmer beachtet die Durchführungsbestimmungen und die Regelungen zur Datenschutzaufsicht des jeweils einschlägigen Datenschutzgesetzes.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten.

(6) Der Auftragnehmer verpflichtet sich, den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen.

(7) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust gemäß Art. 32 DSGVO treffen; dies beinhaltet insbesondere

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle);
b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle);
c) dafür Sorge zu tragen, 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 (Zugriffskontrolle);
d) dafür Sorge zu tragen, 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 (Weitergabekontrolle);
e) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle);
f) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle);

g) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle);

h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

Eine Maßnahme nach Buchstaben b) bis d) ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

(8) Die Erfüllung der vorgenannten Pflichten ist vom Auftraggeber zu kontrollieren und in geeigneter Weise nachzuweisen. Hierzu wird der Auftragnehmer dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

(9) Der Auftraggeber kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.

§ 5

Mitteilung bei Verstößen durch den Auftragnehmer

Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

§ 6

Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung des Auftraggebers, hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

(3) Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 7

Subunternehmer

(1) Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers vergeben werden. Als

zustimmungspflichtige Aufträge im Sinne dieser Regelung gelten, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Hauptvertrag vereinbarten Leistung beauftragt, die sich unmittelbar auf die Erbringung der Hauptleistung bezieht. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen.

(2) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden.

(3) Dem Auftraggeber sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

(4) Die Genehmigung zur Einschaltung der Subunternehmer in **Anlage 2** gilt als erteilt, sofern die vorstehenden Anforderungen erfüllt sind.

§ 8
Nebenleistungen

Die §§ 1 bis 7 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 9

Datenschutzkontrolle

Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.

§ 10

Schlussbestimmungen

(1) Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Änderung oder Aufhebung des Schriftformgebotes.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Die Vertragsparteien verpflichten sich für diesen Fall, eine dem wirtschaftlichen Zweck der unwirksamen oder undurchführbaren Bestimmung entsprechende Regelung zu treffen. Dasselbe gilt auch im Fall einer Lücke dieser Vereinbarung.

(3) Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus und in Zusammenhang mit dieser Vereinbarung ist, soweit gesetzlich zulässig, München Stadt.

Chieming, den 10.01.2024 Datum, Ort

_____ _____

Für smartdocu Solutions GmbH:
Marcus Römer (Geschäftsführer)

Anlage 1

Datensicherheits- und Datenschutzkonzept

Technische und Organisatorische Maßnahmen (TOM)

1. Geltungsbereich

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechende Verantwortlichkeit bei der smartdocu Solutions GmbH. Alle Mitarbeiter sind zur Einhaltung dieser Richtlinie verpflichtet.
Sie richtet sich insbesondere an Organisationseinheiten und Gesellschaften der smartdocu Solutions GmbH.

2. Grundsätze des Datenschutzes und Begriffsdefinitionen

a) Aufzählung der sieben Grundsätze des Datenschutzes

Bei der Verarbeitung personenbezogener Daten sind die Grundsätze des Datenschutzes einzuhalten. Dabei handelt es sich um das Prinzip der Rechtmäßigkeit der Verarbeitung nach Treu und Glauben bei Beachtung von Transparenz, dem Prinzip der Zweckbindung, der Datenminimierung, Richtigkeit der Verarbeitung, Speicherbegrenzung, Integrität und Vertraulichkeit, sowie dem Prinzip der Rechenschaftspflicht.

b) Begriffsdefinitionen

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

„Verarbeitung“ stellt jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

„Verantwortlicher“ ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten

vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

3. Der betriebliche Datenschutzbeauftragte

Der Auftragnehmer bestätigt, dass er gemäß § 38 Abs. 1 BDSG keinen Datenschutzbeauftragten bestellen muss.

4. Erheben, Verarbeiten und Nutzen pbD

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen werden geeignete technische und organisatorische Maßnahmen ergriffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;

Dies umfasst insbesondere die folgenden Maßnahmen:

5. Vertraulichkeit

a) Zutrittskontrolle

Die Zutrittskontrolle zu den Büroräumen der smartdocu Solutions GmbH wird durch ein Schlüsselsystem gewährleistet, um Unbefugten den Zutritt zu verwehren. Es besteht eine Dienstanweisung für alle Mitarbeiter, die das Verschließen der Diensträume bei Abwesenheit vorsieht. Die Schlüsselvergabe an Mitarbeiter wird dokumentiert. Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines smartdocu Solutions GmbH Mitarbeiters. Es wird ein Besucherbuch/Protokoll geführt. Der Ein- und Ausgang innerhalb der Räumlichkeiten der smartdocu Solutions GmbH ist mit einer Alarmanlage ausgestattet. Daten und Dokumente in ausgedruckter Form sind in abschließbaren Schränken gesichert. Die smartdocu Solutions GmbH selbst betreibt innerhalb Ihrer Räumlichkeiten keine Server und lagert auch keine Backups etc. in physikalischer Form (siehe VA). Telekommunikationsanlagen und Netzwerktechnik sind befinden sich nicht am Sitz der Gesellschaft.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Alarmanlage		Schlüsselregelung/Liste
	Manuelles Schließsystem		Besucherbuch/Protokoll der Besucher
	Sicherheitsschlösser		Besucher in Begleitung durch Mitarbeiter
	Abschließbare Behältnisse		Dienstanweisung für Mitarbeiter
	Keine Server in den eigenen Räumlichkeiten – rein cloud-basiert		

b) Zugangskontrolle

Die smartdocu Solutions GmbH hat technische und organisatorische Maßnahmen getroffen, die gemeinsam für eine ausreichende Zugangskontrolle sorgen. Systeme der Mitarbeiter (Notebooks, PCs) sind mit einer Benutzererkennung und einem dazugehörigen Passwort / biometrisch geschützt. Es bestehen Passwortrichtlinien. Passwörter müssen eine mindestlänge haben und komplex (Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen) sein. Die Passwörter werden in regelmäßigen Abständen erneuert. Die Zugänge zu den cloud-basierten Systemen (siehe VA) werden zusätzlich durch die Nutzung einer Multifaktor-Authentifizierung abgesichert. Es besteht eine Dienstanweisung für alle Mitarbeiter, die das Sperren des eigenen Rechners beim Verlassen des Arbeitsplatzes vorsieht. Rechner sperren nach einer definierten Zeit ohne Interaktion des Benutzers automatisch. Die Festplatten der Systeme sind verschlüsselt. Die zentrale Benutzer- und Rechteverwaltung (Login-Daten, Netzlaufwerk) erfolgt in cloud-basierten Systemen (siehe VA) über Portale durch einen Administrator. Alle Systeme sind zusätzlich mit einer Software für Antivirus, Antispyware, E-Mail-Schutz sowie Firewall geschützt. Die Richtlinien-Verwaltung und Überwachung aller Systeme erfolgt zentral in cloud-basierten Systemen (siehe VA). Eine Deaktivierung des Schutzes durch den Mitarbeiter ist ausgeschlossen. Mobile Endgeräte sind standardmäßig verschlüsselt und verfügen über eine Anti-Viren-Software. Die Entsperrung erfolgt durch einen Code oder Touch-ID.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Login mit Benutzername + Passwort		Verwalten von Benutzerberechtigungen
	Login mit biometrischen Daten		Erstellen von Benutzerprofilen
	Regelmäßige Passworterneuerung		Dienstanweisung Desktopsperre
	Anti-Virus-/Anti-Spyware/Email-Schutz Software Clients		Zentrale Passwortvergabe
	Anti-Virus mobile Geräte		Richtlinie „Sicheres Passwort“
	Verschlüsselung von Datenträgern/Smartphones		
	Automatische Desktopsperre		
	Verschlüsselung von Notebooks/Tablet		
	Cloud Multifaktor-Authentifizierung		

c) Zugriffskontrolle

smartdocu Solutions GmbH gewährleistet die ausreichende Zugriffskontrolle durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten sicherstellen. Innerhalb der für die jeweilige Aufgabe genutzten Anwendungen auf cloud-basierten Systemen (siehe VA) sind Mechanismen implementiert, die den unberechtigten Zugriff verhindern und fehlgeschlagene Zugriffsversuche protokollieren. Dies ist durch ein personen- und aufgabenbezogenes Rollen- und Berechtigungskonzept sichergestellt. Ausschließlich Berechtigte haben Zugriff auf Ihrer Zugriffsberechtigung

unterliegende Daten und können diese im Rahmen der Verarbeitung nutzen, protokolliert verändern oder speichern. Netzzugriffe sind unter anderem durch Firewalls, etc. geschützt. Durch regelmäßige Sicherheitsupdates z.B. des Betriebssystems wird sichergestellt, dass unberechtigte Zugriffe verhindert werden. Ein Administrator prüft die Vergabe und den Entzug der Berechtigungen (z.B. bei Einstellung eines neuen Mitarbeiters, Wechsel des Arbeitsplatzes/Aufgabenbereichs, Beendigung des Arbeitsverhältnisses) und dokumentiert diese. Die Anzahl der Administratoren ist auf ein absolut nötiges Minimum beschränkt.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Protokollierung von Zugriff auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten		Einsatz Berechtigungskonzepte
	Regelmäßige Sicherheitsupdates		Minimale Anzahl an Administratoren
	Firewalls		Verwaltung Benutzerrechte durch Administratoren

d) Trennungskontrolle

smartdocu Solutions GmbH gewährleistet die ausreichende Trennungskontrolle dadurch, dass Daten physisch oder logisch von anderen Daten getrennt auf verschiedenen cloud-basierten Systemen (siehe VA) gespeichert werden. Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten cloud-basierten System (siehe VA).

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Physikalische Trennung (Systeme/Datenbanken/Datenträger)		Festlegung von Datenbankrechten
	Trennung von Entwicklungs-, Produktiv- und Testumgebung		Festlegung von Cloudrechten

e) Pseudonymisierung

smartdocu Solutions GmbH stellt im Falle der Pseudonymisierung die Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten cloud-basierten System (siehe VA) sicher. Es besteht eine Interne Anweisung, dass personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist zu anonymisieren/pseudonymisieren sind.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Im Falle der Pseudonymisierung: Trennung der		Interne Anweisung: personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der

	Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen (möglichst verschlüsselt)		gesetzlichen Löschfrist zu anonymisieren/pseudonymisieren

6. Integrität

a) Weitergabekontrolle

smartdocu Solutions GmbH gewährleistet die Einhaltung, indem Medien z.B. verschlüsselt sind, ausgehende Datenströme verschlüsselt und Datenträger datenschutzgerecht vernichtet werden. Alle Mitarbeiter der smartdocu Solutions GmbH sind unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen. Verschlüsselte Datenübertragung von Daten (u.a. E-Mail Verschlüsselung, Signaturverfahren) sowie Dokumentation der Datenempfänger und die Dauer der geplanten Überlassung bzw. der Löschfristen sind über Lösungen abgebildet. Die datenschutzgerechte Löschung der Daten nach Auftragsbeendigung wird sichergestellt. Zugriffe und Abrufe werden protokolliert.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	E-Mail Verschlüsselung		Dokumentation der Datenempfänger sowie die Dauer der geplanten Überlassung bzw. der Löschfristen
	Protokollierung der Zugriffe und Abrufe		Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
	Sichere Transportbehälter		Weitergabe in anonymisierter oder pseudonymisierter Form
	Nutzung von Signaturverfahren		Persönliche Übergabe mit Protokoll

b) Eingangskontrolle

Die Nachvollziehbarkeit und Dokumentation der Datenpflege bzw. Datenverwaltung gewährleistet die smartdocu Solutions GmbH durch eine cloud/softwaregestützte Zugriffsprotokollierung der cloud-basierten Systeme (siehe VA). Notwendige Änderungen, die über den eigenen Verantwortungsbereich hinausgehen, müssen protokolliert autorisiert werden. Durch ein Berechtigungskonzept werden Rechte zur Eingabe, Änderung und Löschung vergeben.

	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 oder automatisierte Kontrolle der Protokolle		Klare Zuständigkeiten für Löschungen

			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

7. Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Komponenten in cloud-basierten Systemen sind bei der smartdocu Solutions GmbH ebenso wie die cloud-basierten Systeme (siehe VA) z.B. selbst redundant ausgelegt. Zwischen den Systemen greifen Mechanismen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust gesichert sind.
Zusätzlich sind Datensicherungskonzepte etabliert und umgesetzt, anhand derer eine Rekonstruktion auch in dem Fall möglich ist, wenn durch einen Verarbeitungsschritt die Konsistenz der Daten gefährdet ist.

b) Wiederherstellung

Durch Backupkonzepte, redundante Systeme sowie durch ein Business Continuity Management in Verbindung mit IT Recovery-Plänen der cloud-basierten Systeme (siehe VA), wird eine Wiederherstellung nach einem physischen oder technischen Zwischenfall gewährleistet.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Siehe TOMS VA		Kontrolle des Sicherungsvorgangs
			Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
			Existenz eines Notfallplans

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a) Datenschutz-Maßnahmen

Die smartdocu Solutions GmbH führt z.B. regelmäßig eine Prüfung der Dokumentation der technischen und organisatorischen Maßnahmen durch. Soweit Änderungsbedürfnisse identifiziert werden, werden diese entsprechend umgesetzt. Verfahren zur Meldung eines Sicherheitsvorfalls sind dokumentiert und etabliert. Zur Schulung der Mitarbeiter zur Einhaltung des Datenschutzrechts, werden regelmäßig Schulungen durchgeführt. Konzepte werden kontinuierlich, wie beispielsweise auf Basis von Erfahrungen, Best Practices, regulatorischer Veränderungen weiter angepasst.

	Technische Maßnahmen		Organisatorische Maßnahmen
	dokumentiertes Sicherheitskonzept		Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
	Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt		Mitarbeiter geschult auf Vertraulichkeit/Datengeheimnis
			Datenschutzfolgeabschätzung
			Die Organisation kommt den Informationspflichten nach Art. 13 und Art. 14 DSGVO nach
			Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

b) Incident-Response-Management

	Technische Maßnahmen		Organisatorische Maßnahmen
	Einsatz von Firewall und regelmäßige Aktualisierung		Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber der Aufsichtsbehörde)
	Einsatz von Spamfiltern 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)		

c) Datenschutzfreundliche Voreinstellungen

	Technische Maßnahmen		Organisatorische Maßnahmen
	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind		Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt
	Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen		

d) Auftragskontrolle (Outsourcing an Dritte)

Die Mitarbeiter der smartdocu Solutions GmbH werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die smartdocu Solutions GmbH gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort, als auch per Fernwartung.

	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 Vereinbarungen zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
			Schriftliche Weisungen an den Auftragnehmer
			Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
			Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der 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

9. Vertraulichkeitsverpflichtung der befugten Personen

Die smartdocu Solutions GmbH wird gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Konzepte werden kontinuierlich, wie beispielsweise auf Basis von Erfahrungen, Best Practices, regulatorischer Veränderungen weiter angepasst.

10. Verarbeitungsverzeichnis

Es wird ein schriftliches oder elektronisches Verzeichnis über alle Verarbeitungstätigkeiten geführt. Dieses Verarbeitungsverzeichnis enthält die in Artikel 30 Absatz 2 DSGVO genannten Angaben.

11. Übermittlungen von Daten an Drittländer und internationale Organisationen

smartdocu Solutions GmbH beachtet die Beschränkungen für Datenübermittlungen an Unternehmen in Drittländern und internationale Organisationen gem. Art. 44 ff. DSGVO. Personenbezogene Daten werden nur dann übermittelt, wenn die Verarbeitung insgesamt den Anforderungen der DSGVO genügt und im Empfängerland vergleichbare datenschutzrelevante Schutzmechanismen für Betroffene vorgesehen sind.

Chieming, den 10.01.2024

Marcus Römer, Geschäftsführer

Anlage 2

Übersicht der Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 7:

Dienstleister 1:

Unternehmen mit Namen, Rechtsform:	Hetzner Online GmbH
Anschrift:	Industriestr. 25, 91710 Gunzenhausen
Art der Dienstleistung:	Hosting, Bereitstellung Server

Dienstleister 2:

Unternehmen mit Namen, Rechtsform:	xenthics Solutions GmbH,
Anschrift:	Alte Landstr. 25, 85521 Ottobrunn
Art der Dienstleistung:	Software-Programmierung

Dienstleister 3:

Unternehmen mit Namen, Rechtsform:	Claudio Wabner
Anschrift:	Frühlingstrasse 36, 83435 Bad Reichenhall
Art der Dienstleistung:	Unternehmensberatung, Kundenservice
Telefon:	08651-9042826