Auftragsverarbeitungsvertrag Taxy.io Plattform

Der nachfolgende Auftragsverarbeitungsvertrag i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (nachfolgend „**Auftragsverarbeitungsvertrag**“) konkretisiert die Verpflichtungen zum Datenschutz der Taxy.io GmbH Jülicher Straße 72a 52070 Aachen (nachfolgend „**Auftragnehmer**“) als Auftragnehmer, die sich aus der Auftragsverarbeitung gegenüber dem Kunden, der als Steuerberater/Kanzlei das vom Auftragnehmer vorgehaltene Angebot nutzt, (nachfolgend „**Auftraggeber**“) ergeben. Der Auftragsverarbeitungsvertrag findet Anwendung auf alle Tätigkeiten, die mit den zwischen den Parteien geschlossenen Hauptverträgen über die unter app.taxy.io vorgehaltenen Leistungen (nachfolgend Hauptverträge einzeln „**Vertrag**“ oder gemeinsam „**Verträge**“) in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachfolgend „**Daten**“) des Auftraggebers verarbeiten.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag sowie der Aufstellung in **Anlage 1** ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Die Laufzeit dieses Auftragsverarbeitungsvertrages richtet sich nach der Laufzeit des längstlaufenden Vertrages, sofern sich aus den Bestimmungen dieses Auftragsverarbeitungsvertrages nicht darüber hinausgehende Verpflichtungen ergeben.

2. Anwendungsbereich, Ort der Datenverarbeitung und Verantwortlichkeit

2.1. Der Auftragnehmer verarbeitet Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der obigen Beschreibung unter Ziffer 1

konkretisiert sind. Der Auftraggeber ist im Rahmen des Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

2.2. Die Datenverarbeitung der vertraglich geschuldeten Leistungen findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EU/EWR) statt. Jede Verlagerung der Datenverarbeitung oder Teilen der Datenverarbeitung in ein Drittland erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff.

DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standardvertragsklauseln, genehmigte Verhaltensregeln) und bedarf der vorherigen Zustimmung des Auftraggebers.

2.3. Die Weisungen werden anfänglich durch den jeweiligen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (nachfolgend „**Einzelweisung**“). Einzelweisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Einzelweisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3. Pflichten des Auftragnehmers

3.1. Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2. 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 zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Diese technischen und organisatorischen Maßnahmen sind in der beigefügten **Anlage 2** aufgelistet.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.3. Der Auftragnehmer unterstützt, soweit vereinbart, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten.

3.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des Auftraggebers bekannt werden.

3.6. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

3.8. Der Auftragnehmer berichtigt oder löscht die Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren.

3.9. Daten, Datenträger sowie sämtliche sonstigen Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

3.10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4. Pflichten des Auftraggebers

4.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt Ziffer 3.10 entsprechend.

4.3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten

6.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Auftragsverarbeitungsvertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

6.2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der

Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer seine übliche Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

6.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Ziffer 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

7. Sonderregelungen für Daten, die einem Berufsgeheimnis gemäß § 203 StGB unterliegen

7.1. Im Rahmen der Auftragsverarbeitung werden auch Daten verarbeitet, die unter ein Berufsgeheimnis im Sinne von § 203 StGB fallen. Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der dem Auftragnehmer zugewiesenen Aufgaben erforderlich ist. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen gemäß § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis

offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

7.2. Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftragnehmer wird etwaige Subunternehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer vorgesehenen Tätigkeit Kenntnis von Daten erhalten, die einem Berufsgeheimnis unterliegen, zur Geheimhaltung verpflichten und auf die Folgen der Verletzung der Geheimhaltung hinweisen.

7.3. Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

7.4. Der Auftragnehmer wird darauf hingewiesen, dass die in seinem Gewahrsam befindlichen Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer

Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

8. Subunternehmer

8.1. Der Auftragnehmer ist berechtigt, die in Anlage 3 angegebenen Subunternehmer für die Verarbeitung von Daten im Auftrag einzusetzen.

8.2. Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Subunternehmers oder bei geplanter Beauftragung eines weiteren Subunternehmers rechtzeitig, spätestens aber vier (4) Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren (nachfolgend „**Information**“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Subunternehmers unter Angabe einer Begründung in Textform binnen drei (3) Wochen nach Zugang der Information zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Wenn kein Widerspruch des Auftraggebers binnen drei (3) Wochen nach Zugang der Information erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Subunternehmers.

8.3. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Auftragsverarbeitungsvertrag dem Subunternehmer zu übertragen. Der Auftragnehmer hat mit dem Subunternehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Subunternehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

8.4. Der Auftragnehmer kann geschuldete Leistungen durch Subunternehmer ganz oder teilweise von einem Standort außerhalb der EU/EWR erbringen lassen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standardvertragsklauseln, genehmigte Verhaltensregeln).

8.5. Nicht als Subunternehmer i.S.d. dieser Ziffer 8 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um seine Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, sowie

Post-/Transportdienstleistungen,. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Subunternehmerverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

9. Informationspflichten, Rechtswahl

9.1. Sollten die Daten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DSGVO liegen.

9.2. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsverarbeitungsvertrages zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieses Auftragsverarbeitungsvertrages unwirksam sein, so berührt dies die Wirksamkeit des Auftragsverarbeitungsvertrages im Übrigen nicht.

9.3. Es gilt deutsches Recht.

10. Haftung und Schadensersatz

Der Auftragnehmer haftet gemäß den im Vertrag festgelegten Haftungsregelungen.

11. Änderung dieses Auftragsverarbeitungsvertrages

11.1. Der Auftragnehmer behält sich vor, diesen Auftragsverarbeitungsvertrag einseitig zu ändern, wenn dies sachlich gerechtfertigt erscheint. Sachlich gerechtfertigt sind Änderungen beispielsweise bei einer Erweiterung oder Änderung der Funktionen von http://www.smartgrundsteuer.de , einer Änderung der Rechts- oder Gesetzeslage (etwa, wenn die Rechtsprechung eine Klausel für unwirksam erklärt) oder wenn durch unvorhersehbare Änderungen, die der Auftragnehmer nicht veranlasst und auf die der Auftragnehmer auch keinen Einfluss hat, das bei Vertragsschluss bestehende Äquivalenzverhältnis in nicht unbedeutendem Maße gestört wird. Voraussetzung einer Änderung ist stets, dass diese dem Auftraggeber zumutbar ist und nicht in sein bestehendes Weisungsrecht eingreift.

11.2. Dem Auftraggeber werden Änderungen des Auftragsverarbeitungsvertrages bekannt gegeben. Sie gelten als genehmigt, wenn der Auftraggeber der Geltung des geänderten Auftragsverarbeitungsvertrages nicht innerhalb von vier (4) Wochen schriftlich oder per E-Mail gegenüber dem Auftragnehmer widersprochen hat und der Auftragnehmer auf die Rechtsfolgen eines unterbliebenen Widerspruches hingewiesen hat.

Anlage 1

Art und Zweck der Verarbeitung

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

Mandanten der Kanzlei, Mitarbeiter der Kanzlei

.....

Kategorien von Daten

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):

Mandantenstammdaten, Mandantenkommunikation, Mitarbeiterkontaktdaten

.....

Kategorien von sensiblen Daten (falls zutreffend)

Die übermittelten personenbezogenen Daten umfassen folgende sensiblen Daten:

Keine

.....

Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen

Die übermittelten personenbezogenen Daten werden folgenden grundlegenden

Verarbeitungsmaßnahmen unterzogen:

Gegenstand der Verarbeitung sind alle Verarbeitungsmaßnahmen, die der Auftragsverarbeiter gemäß den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen mit dem Verantwortlichen (Geschäftsbedingungen des

Auftragsverarbeiters, Bestellungen von Standardprodukten und Verträge über individuelle Leistungen wie z.B. Softwarewartungs- und Supportverträge, Premium/Professional Service Verträge) erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern die Leistungsbeschreibungen und die jeweiligen vertraglichen Vereinbarungen nicht ausdrücklich Bezug nehmen auf diese

Vereinbarung zur Auftragsverarbeitung. Die Leistungsbeschreibungen sind Bestandteil dieser Vereinbarung und bleiben unberührt.

.....

Verarbeitungszwecke

Die übermittelten personenbezogenen Daten werden zu folgenden Zwecken des Verantwortlichen verarbeitet:

Die Klassifizierung erfolgt mit dem Zweck der individualisierten Mandantenberatung

.....

Anlage 2

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (vgl. Ziffer 3.2 des Auftragsverarbeitungsvertrages)

1. Zugangskontrolle (zu Datenverarbeitungssystemen) a. Technische Maßnahmen

☒ Automatisches Sperren von Rechnern bei Inaktivität
☒ Einsatz von Anti-Viren-Programmen, insbesondere E-Mail und Internet Gateway
☒ Einsatz von Firewalls
☒ Einsatz von Intrusion-Detection-Systemen
☒ Mobile-Device-Management
☒ Verschlüsselung von Smartphones
☒ Verschlüsselung von Datenträgern
☒ Einsatz von VPN bei Remote-Zugriffen
☒ W-Lan-Verschlüsselung entspricht dem aktuellsten Stand der Technik

(WPA2/WPA2-PSK)

b. Organisatorische Maßnahmen

☒ Passwortverfahren
☒ Vorgabe für Länge
☒ Vorgabe für Zeichen
☒ Aufforderung zur Änderung nach Erstanmeldung ☒ Regelmäßiges Ändern des Passwortes

☒ Alte Passwörter können nicht noch einmal genutzt werden
☒ Verschlüsselte Ablage der Passwörter
☒ Zweifaktorauthentifizierung
☒ Anweisung zum manuellen Sperren des Rechners bei Abwesenheit ☒ Andere Verfahren zur Abmeldung

☒ Clean-Desk-Richtlinie
☒ Bring-Your-Own-Device-Richtlinie (BYOD)
☒ IT-Sicherheits-Richtlinie
☒ Verpflichtung der Beschäftigte auf Vertraulichkeit

2. Zugriffskontrolle

c. Technische Maßnahmen

☒ Verschlüsselung von Festplatten in Laptops

d. Organisatorische Maßnahmen

☒ Berechtigungskonzept, Zugriffsrechte sowie deren Überwachung und Protokollierung

☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert ☒ Verwaltung der Rechte durch Systemadministrator
☒ Incident Reponse Management
☒ Richtlinie zur Meldung von Datenschutzverletzungen

3. Weitergabekontrolle von Daten e. Technische Maßnahmen

☒ Verschlüsselung bei der Übertragung von Daten
☒ Fernwartung wird im Auftrag für Dritte durchgeführt ☒ Eigene Systeme werden durch Fernwartung gewartet

f. Organisatorische Maßnahmen

☒ Weitergabe/Empfangen von Daten findet statt ☒ Innerhalb des Unternehmens

☒ Zur Auslagerung
☒ Zwischen Auftraggeber und Auftragnehmer bei

Auftragsdatenverarbeitung
Wie werden die Daten transportiert? ☒ Datenleitung

☒ E-Mail
☒ Post
☒ Keine Weiterleitung von Mails (insbesondere an Privatkonten) ☒ Anlegen des Verzeichnisses von Verarbeitungstätigkeiten

4. Eingabekontrolle

Maßnahmen zur nachträglichen Überprüfung von Dateneingaben, -änderungen und -löschungen

g. Technische Maßnahmen

☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

h. Organisatorische Maßnahmen

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis

eines Berechtigungskonzepts

5. Auftragskontrolle bei Auftragsdatenverarbeitung als Auftraggeber

Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer

i. Organisatorische Maßnahmen

☒ Sorgfältige Auswahl des Auftragnehmers hinsichtlich der Datensicherheit ☒ Vorherige Überprüfung des Auftragnehmers

☒ Auftragsdatenverarbeitungs-Vereinbarungen werden geschlossen
☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis ☒ Vereinbarung, dass Anweisungen nur schriftlich erfolgen

6. Trennungsgebot

Maßnahmen zur getrennten Verarbeitung (Speicherung, Übermittlung, Veränderung und Löschung) von Daten mit unterschiedlichen Zwecken

j. Technische Maßnahmen

☒ Trennung von Produktiv- und Testsystem
☒ Physikalische Trennung durch Systeme oder Datenträger ☒ Logische Mandantentrennung (softwareseitig)

7. Zusätzliche Maßnahmen entsprechend Art. 32 DSGVO

☒ Grundsätzliche Prüfung eines jeden Prozesses vor/bei Aufnahme hinsichtlich des Risikos auf die Rechte und Freiheiten des Betroffenen und die Eintrittswahrscheinlichkeit eines Schadens in Bezug auf die Daten. Ggfs. erfolgt hieraus eine Ableitung zu einer Datenschutz-Folgeabschätzung und sich daran anschließender Maßnahmen

☒ Dauerhaftes Monitoring der gesamten Systeme durch aktive Überwachung unter anderem aller Server, Volumes und Netzwerke mit sofortiger Fehlermeldung

☒ Dauerhafte aktive Überprüfung von externen Systemen auf Verfügbarkeit

☒ Dauerhafte Beobachtung eventuell auftretender Security Probleme und deren Einstufung auf eine eventuelle Bedrohung mit Einleitung entsprechender Maßnahmen

☒ Betrieb eines IT-Wikis
☒ Sensibilisierung der Beschäftigten in Hinsicht auf Datenschutz
☒ Sensibilisierung der Beschäftigten in Hinsicht auf Informationssicherheit

Anlage 3

Eingesetzte Subunternehmer

Name und Anschrift des Subunternehmers	**Beschreibung der Teilleistungen**
Auth0, Inc, 10800 NE 8th Street, Suite 700, Bellevue, WA 98004, USA Serverstandort: EU	Authentifizierungsdienst
DATEV eG, Paumgartnerstr. 6-14, 90429 Nürnberg Serverstandort: Deutschland	Authentifizierung per DATEV Login Schnittstelle und Nutzung von DATEV Schnittstellen
Fortinet, Inc. Global Headquarters 899 Kifer Road Sunnyvale, CA 94086 USA Serverstandort: EU	Web Application Firewall
HubSpot, Inc., 25 First St., 2nd floor, Cambridge, Massachusetts 02141, USA Serverstandort: EU	Kundenverwaltung, Prozess- und Vertriebsunterstützung, Newsletterversand
Mailjet SAS,13-13 bis, rue de l’Aubrac, 75012 Paris, Frankreich Serverstandort: EU	E-Mail-Versand von Benachrichtigungen über Status der Erklärungen undneue Ereignisse
Microsoft Ireland Operations Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland Serverstandort: EU	Cloudspeicher und Cloudinfrastrukturdienste

pcvisit Software AG, Manfred-von-Ardenne-Ring 20, 01099 Dresden Serverstandort: Deutschland	Fernwartungssoftware für Kundensupport
Sleekplan GmbH, Georgenstrasse 66, 80799, München Serverstandort: EU	Nutzerfeedback
Stripe Payments Europe Limited 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland Serverstandort: USA	Zahlungsdienstleister
Wolters Kluwer Software und Service GmbH, Stuttgarter Straße 35 in 71638 Ludwigsburg Serverstandort: Deutschland	Authentifizierung per ADDISON Single Sign On und Nutzung von OneClick Schnittstellen