Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem Verantwortlichen

Firma XY

- nachstehend Auftraggeber genannt -

und dem Auftragsverarbeiter

aicall.io GmbH ∠Seestr. 14 ∠14467 Potsdam

- nachstehend Auftragnehmer genannt-

Präambel

Die vorliegende Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Rahmen der Auftragsverarbeitung, welche im Vertrag vom beschrieben ist. Sie ist auf sämtliche Tätigkeiten anwendbar, die im Zusammenhang mit dem Vertrag stehen und bei denen Mitarbeiter oder beauftragte Dritte des Auftragnehmers personenbezogene Daten des Auftraggebers verarbeiten.

Die Vereinbarung gilt entsprechend für (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Aus der Anlage 1 und dem Vertrag ergeben sich Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung.

(2) Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn, die Parteien vereinbaren ausdrücklich etwas anderes.

2. Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses 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) Die Weisung wird durch Leistungsbeschreibung festgelegt und können vom Auftraggeber danach schriftlich oder in Textform (z.B. E-Mail) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform vom Auftraggeber zu bestätigen.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, 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 und dessen Voraussetzungen werden gewahrt.

(2) 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) Der Auftragnehmer 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 insbesondere technische und organisatorische Maßnahmen zu treffen, gemessen am Risiko für die Rechte und Freiheiten der betroffenen Personen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer gewährleisten. Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung zu dokumentieren und dem Auftraggeber zur Prüfung bereitzustellen. Die Einzelheiten dieser technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Diese sind vom Auftragnehmer entsprechend zu dokumentieren. Dabei darf das Sicherheitsniveau der in Anlage 3 genannten Maßnahmen nicht unterschritten werden.

(4) Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten.

(5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die mit der Verarbeitung der personenbezogenen Daten zuständigen Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrags fortbesteht

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:

- eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(7) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(8) Der Auftragnehmer gewährleistet, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen (Art. 32 Abs. 1 lit. d DSGVO).

(9) Während der Vertragslaufzeit berichtigt oder löscht der Auftragnehmer auf Weisung des Auftraggebers die vertragsgegenständlichen Daten. Sofern eine datenschutzkonforme Löschung dieser Daten nicht möglich ist, stellt der Auftragnehmer eine datenschutzkonforme Vernichtung der Datenträger und Unterlagen, die vertragsgegenständliche Daten enthalten, sicher.

Dem Auftragsverarbeiter vom Auftraggeber übergebene Datenträger und verarbeitete Daten einschließlich gefertigter Kopien. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der

Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die daten schutzkonforme 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, sofern nicht im Vertrag bereits vereinbart.

(10) Daten, Datenträger sowie sämtliche Dokumente sind nach Auftragsende auf Verlangen (schriftlich oder in Textform) des Auftraggebers entweder herauszugeben, sofern sie im Eigentum des Auftraggebers sind, oder zu löschen.

(11) Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

4. Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten feststellt.

(2) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO, gilt §3 Abs. 4 (Option) entsprechend.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15 bis 21 DSGVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang

6. Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art 32 DSGVO nachzuweisen

(2) Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT- Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- Selbstaudits
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701)
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO

- Vereinbarung zwischen Auftraggeber und Auftragnehmer, dass der Nachweis auch durch folgende Unterlagen / Zertifikate erbracht werden kann

(2) Kontrollrechte

a. Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen gemäß Art. 28 Abs. 3 Satz 2 lit. h DSGVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.

b. Die Prüfungen werden durch den Auftraggeber selbst oder einen von ihm beauftragten Dritten durchgeführt. Sollte der durch den Auftraggeber beauftragte Dritter in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen. Dies gilt insbesondere für die Abgabe von Erklärungen zur berufsrechtlichen oder gesetzlichen Verschwiegenheit.

c. Eine Prüfung kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch weitere Maßnahmen erfolgen. Zu den weiteren Maßnahmen zählen die Anforderung von Zertifizierungen, Berichte zu Datenschutzaudits und Inspektionen vor Ort. Inspektionen vor Ort nimmt der Auftraggeber mit angemessener Vorankündigung während der üblichen Geschäftszeiten vor. Die Prüfungen müssen ohne Störung des Betriebsablaufs sowie unter Wahrung der Sicherheits- und Vertraulichkeitsinteressen des Auftragnehmers durchgeführt und auf eine angemessene Anzahl beschränkt werden. Ausgenommen sind anlassbezogene Kontrollen. Jede Partei trägt die ihr entstandenen Kosten der Prüfungen in den vorgenannten Fällen (incl. Nachprüfungen) selbst.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in **Anlage 2** bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel der gemäß Anlage 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

8. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO.

☒ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

☐ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland. In der **Anlage 2** werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

9. Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

10. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers 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.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht

Ansprechpartner des Auftraggebers: _____

Datenschutzbeauftragter des Auftraggebers: _____

Ansprechpartner des Auftragnehmers: _____

_____ , den _____ , den _____

_____ _____

Auftragnehmer *Auftraggeber*

Anlage 1 -Details zur Auftragsverarbeitung

aicall.io ∠Seestr. 14 ∠14467 Potsdam

Gegenstand und Dauer der Auftragsverarbeitung, die wie folgt spezifiziert wird:

Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO

Verantwortlicher ist: Der Auftraggeber

Übersicht über Daten und Verarbeitungstätigkeiten

1. Kategorien betroffener Personen
   - ☒ Beschäftigte
   - ☒ Hotelgäste
   - ☒ Interessenten
   - ☒ Dienstleister/Lieferanten und deren Beschäftigte
2. Art der personenbezogenen Daten
   - ☒ Personenstammdaten (Name und Vorname eines Ansprechpartners)
   - ☒ Kommunikationsdaten (Telefon, E-Mail)
   - ☒ Vertragsstammdaten (Vertragsbeziehung, Vertragsinteresse)
   - ☒ Nutzungsdaten (IP-Adressen, Log-Files)
3. Beschreibung des Zwecks und der Art der Verarbeitung personenbezogener Daten

Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Kunden in dessen Auftrag und nach dessen Weisung im Zusammenhang mit der Bereitstellung von aicall.io. als „Software as a Service“ (SaaS) inklusive Cloud-Hosting, Betrieb und Support.

Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Implementierung, Integration und Konfiguration von aicall.io,
- sowie die ergänzende Leistungen der Beratung und Anpassung (Customizing) der Anwendung
- und die Erbringung von Support- und Wartungsleistungen (Behebung von technischen Problemen, Aktualisierung und Wartung der Software)

Anlage 2 - Genehmigte Unterauftragsverhältnisse

aicall.io GmbH ∠Seestr. 14∠14467 Potsdam

Unterauftragsverhältnisse

(1) Der Einsatz von Unterauftragnehmer als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Unterauftragsverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgenden Unterauftragnehmer durchgeführt:

Name und Anschrift des Unterauftragnehmers	Beschreibung der Leistungen	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
Microsoft Ireland South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Irland	Azure	
Google Ireland Limited Gordon House, Barrow Street 4, Dublin, Ireland	Google Firebase Authentication	DPA inkl. Standardvertragsklauseln
Twilio, Inc., 101 Spear St San Francisco, California 94105	Cloud-Kommunikationsplattform	AVV inkl. Standardvertragsklauseln

(3) Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen.

Anlage 3 - Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

aicall.io GmbH ∠Seestr. 14 ∠14467 Potsdam

Folgende technische und organisatorische Maßnahmen wurden getroffen:

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

1. Technische Maßnahmen

Alarmanlage	☐
Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)	☒
Schlüsselregelung (Schlüsselverwaltung, Schlüsselausgabe etc.)	☒
Sicherheitsschlösser	☐

2. Organisatorische Maßnahmen

Protokollierung der Besucher / Besucherbuch	☒
Schlüsselregelung / Schlüsselbuch	☐
Videoüberwachung der Zugänge	☐

Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (insbesondere durch den Einsatz von Verschlüsselungsverfahren, die dem jeweils aktuellen Stand der Technik entsprechen).

1. Technische Maßnahmen

Authentifikation mit Benutzer + Passwort	☒
Aktuelle Anti-Viren-Software	☒
Aktuelle Firewall	☐
VPN-Technologie	☐
Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung	☒
E-Mail-Verschlüsselung	☒
Verschlüsselung von Datenträgern	☒

1. Organisatorische Maßnahmen

Zuordnung und Verwaltung der Benutzerberechtigungen	☒
Erstellen von Benutzerprofilen	☐
Passwortvergabe / Passwortregeln (inkl. regelmäßigen Änderungen)	☒
Automatische Sperrung des Arbeitsplatzes	☒
Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	☐
Protokollierung von Übermittlungen	☐
Erstellung einer Übersicht von Datenträgern, Aus- und Eingang	☐

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1. Technische Maßnahmen

Einsatz von Aktenvernichter	☐
Einsatz von Datenträgervernichter	☐
Einsatz von Dienstleistern unter Beachtung von DIN 66399	☐
Ordnungsgemäßer Vernichtung von Ii (DIN 32757)	☐
Verschlüsselung von Datenträgern	☒
	☒

2. Organisatorische Maßnahmen

Verwaltung der Benutzerrechte durch System-Administrator	☐
Anzahl der Administratoren auf das "Notwendigste" reduziert	☐
Erstellung eines Berechtigungsplans	☐
Passwortrichtlinie inkl. Länge und Wechsel	☒
Sichere Aufbewahrung von Datenträgern	☒
Ordnungsgemäße Vernichtung von Datenträgern	☐
Löschungskonzept für Daten	☒
Protokollierung der Vernichtung voiiiiin Daten	☐
Protokollieren von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☐

Weitergabekontrolle

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 werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

1. Technische Maßnahmen

Einrichtungen von VPN-Tunneln	☐
E-Mail-Verschlüsselung	☒

2. Organisatorische Maßnahmen

Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	☐
Erstellung einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen	☐
Weitergabe von Daten in anonymisierter oder pseudonymisierter Form	☐

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind und Vertragsdaten jederzeit ihrem Ursprung zugeordnet werden können (Authentizitätskontrolle).

1. Technische Maßnahmen

Protokollierung der Eingabe, Änderung und Löschung von Daten	☐

2. Organisatorische Maßnahmen

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	☒
Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden	☐
Protokollauswertungsroutinen/-systeme vorhanden	☐
Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden	☐

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können und erhaltene Weisungen unverzüglich umgesetzt werden.

1. Technische Maßnahmen

	☐

2. Organisatorische Maßnahmen

Vorhandene Vereinbarungen zur Auftragsverarbeitung	☒

Kontrolle der Vertragsausführung	☒
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	☒

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies umfasst insbesondere die Gewährleistung der Belastbarkeit der Systeme und Dienste, die Verwahrung der Vertragsdaten nach den Grundsätzen einer ordnungsgemäßen Datensicherung sowie regelmäßige Datensicherungen, einschließlich regelmäßiger Back-ups, im erforderlichen Umfang.

1. Technische Maßnahmen

Unterbrechungsfreie Stromversorgung (USV)	☐
Überspannungsschutz	☐
Schutz gegen Umwelteinflüsse (Sturm, Wasser)	☐
Feuer- und Rauchmeldeanlagen	☐
Feuerlöscher in Serverraum	☐
Klimaanlage in Serverraum	☐
Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverraum	☐
Schutzsteckdosen in Serverraum	☐

2. Organisatorische Maßnahmen

Erstellen eines Notfallplans	☐
Alarmmeldung bei unberechtigten Zutritten zu Serverraum	☐
Testen von Datenwiederherstellung	☐
Serverraum nicht unter sanitären Anlagen	☐
Serverraum über Wassergrenze (in Hochwassergebiet)	☐
Erstellen eines Backup- (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort) und Recoverykonzepts	☒
Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	☒
Spiegelung von Festplatten (z. B. RAID-Verfahren)	☐

Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

1. Technische Maßnahmen

Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	☒
Bei pseudonymisierten Daten: Trennung der Zuordnungsdaten und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	☐

2. Organisatorische Maßnahmen

Festlegung Technologie von Datenbankrechten	☐
Festlegung von Datenbankrechten	☐
Erstellung eines Berechtigungskonzepts	☐

Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

3. Technische Maßnahmen

	☐

4. Organisatorische Maßnahmen

Führung eines Verarbeitungsverzeichnisses	☒
Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration	☒
Erstellung eines Berechtigungskonzepts	☒

Allgemeine Maßnahmen

Ist ein Datenschutzbeauftragter bestellt?

Nein, da gesetzlich nicht vorgeschrieben	☒
Ja	☐

	Name:	Bastian Schlarp
	Funktion	GF
	E-Mail:	info@aicall.io

Mitarbeiter wurden über Datenschutzrecht und Datensicherheit geschult	☒
Alle Mitarbeiter sind auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.	☒
Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen	☒
Ein Datensicherheitskonzept / Informationssicherheitsmanagement ist vorhanden.	☐
Ein Datenschutzkonzept ist vorhanden.	☐
Eine Auditierung / Zertifizierung ist vorhanden	☐
Verhaltensregeln nach Art. 40 DSGVO sind vorhanden	☐
Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.	☒

Ausgefüllt für die Organisation durch:

Name: Bastian Schlarp

Funktion Geschäftsführer

E-Mail: Info@aicall.io

Telefon: 033176997110