

Vertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen der

vertreten durch ihren Schulleiter,

-nachfolgend auch: „**Auftraggeber**“-

und der

studypilot UG (haftungsbeschränkt)

Ostpreußenstraße 21

90552 Röthenbach a. d. Pegnitz

vertreten durch einen ihrer Geschäftsführer,

Herrn Moritz Gößl oder Herrn Julian Wening

-nachfolgend auch: „**Auftragnehmer**“-

1 Einleitung, Geltungsbereich, Definitionen

- (1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
- (2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.
- (3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer übernimmt folgende Verarbeitungen: Die Speicherung, Bereitstellung und Zugriffsverwaltung von Nutzerdaten des vom Auftragnehmer angebotenen und vom Auftraggeber und dessen Schülern genutzten Softwareproduktes „studypilot Premium“.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Kontingent-Lizenzvertrag (im Folgenden „Hauptvertrag“).

2.2 Dauer

Die Verarbeitung beginnt am mit Inkrafttreten des Hauptvertrages und endet mit dessen Auslaufen.

3 Art, Zweck und Betroffene der Datenverarbeitung:

3.1 Art der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Übermittlung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

3.2 Zweck der Verarbeitung

Die Verarbeitung dient folgendem Zweck: Der Bereitstellung der Funktionen des vom Auftragnehmer angebotenen und vom Auftraggeber und dessen Schülern genutzten Softwareproduktes „studypilot Premium“ über vom Auftragnehmer bereitgestellte und vom Auftraggeber administrierte Nutzerzugänge.

3.3 Art der Daten

Es werden folgende Daten verarbeitet:

- Vorname(n),
- Nachname,
- vergebene Endnutzer-E-Mail-Adresse,
- Jahrgangsstufe,
- Klasse
- vom Nutzer in der Anwendung gespeicherte Daten

3.4 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Schüler des Auftraggebers

4 Rechte und Pflichten, Weisungsbefugnisse des Auftraggebers

- (1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
 - (2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
 - (3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
 - (4) Folgende Personen und Kommunikationswege werden benannt:
-

Weisungsberechtigte Personen des Auftraggebers sind:

_____, _____, _____

Weisungsempfänger beim Auftragnehmer sind:

Moritz Gößl, Geschäftsführer der studypilot UG (haftungsbeschränkt), +49 152 06111635

Für Weisung zu nutzende Kommunikationskanäle:

Adresse: Ostpreußenstr. 21, 90552 Röthenbach a.d.Pegn.

E-Mail: moritz@studypilot.app

Telefon: +49 152 06111635

- (5) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
- (6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
- (7) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.
- (8) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
- (9) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- (10) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
- (2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.
- (3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

- (4) Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
- (5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an folgende Stelle des Auftraggebers weiterzuleiten:
- _____, _____, _____
- (6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
- (7) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnigte Interessen des Auftragnehmers dem nicht entgegenstehen.
- (8) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
- (9) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechnigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).
- (10) Die Verarbeitung von Daten in Privatwohnungen ist gestattet. Die Maßnahmen nach Art. 32 DS-GVO sind sicherzustellen.
- (11) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.
- (12) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
- (13) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
- (14) Ein betrieblicher Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.
-

- (15) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

6 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

- (1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO.
- (2) Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- (1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- (2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

8 Unterauftragsverhältnisse

- (1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
- (2) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- (3) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt

dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

- (4) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).
- (5) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.
- (6) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
- (7) Zurzeit sind für den Auftragnehmer folgenden Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt:

Firma/Name:	Anschrift:	Auftragsinhalt:	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Hosting der App-Daten, einschließlich Speicherung personenbezogener Daten (z. B. Nutzerkonten, Logfiles, App-Inhalte) auf gemieteten Servern	
IONOS SE	Elgendorfer Str. 57 56410 Montabaur	Bereitstellung eines Cloud-Speicherdienstes zur Lagerung von Backup-Daten (inkl. Nutzerdaten, App-Inhalten)	
Mailgun Technologies Inc.	112 E. Pecan St. #1135 San Antonio, TX 78205 United States	Bereitstellung eines E-Mail-Versanddienstes für systemgenerierte E-Mails (z. B. Registrierungsbestätigungen)	Standardvertragsklauseln nach Art. 46 Abs. (2) lit. b DS-GVO

Google LLC (Firebase)	1600 Amphitheatre Parkway Mountain View, CA 94043 United States	Bereitstellung eines Authentifizierungs- dienstes mit Speicherung der Nutzerkonten (inkl. Name und E-Mail-Adresse)	Angemessenheits- beschluss der Kommission nach Art. 45 DS-GVO und Zertifizierung des Unterauftragneh- mers nach EU-US Data Privacy Framework Standardvertrag sklauseln nach Art. 46 Abs. (2) lit. b DS-GVO
--------------------------	---	---	--

Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

- (8) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

9 Beendigung des Auftrags

- (1) Nach Beendigung des Hauptvertrages hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht löschen bzw. zu vernichten/vernichten zu lassen.
- (2) Die Löschung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

11 Haftung

Auf Art. 82 DS-GVO wird verwiesen.

12 Sonderkündigungsrecht

- (1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

- (3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

13 Sonstiges

- (1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
- (2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Für Nebenabreden ist die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich.
- (4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer

Anhang technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Organisation - Organisatorische Maßnahmen sollen einen Schutz der Daten durch Struktur, Aufklärung, Schulung, Vorgaben und Verpflichtungen gewährleisten.

- Es wurde geprüft, ob der Unternehmen gemäß der DSGVO einen Datenschutzbeauftragten benennen muss
- Verantwortlichkeiten zum Datenschutz wurden bestimmt
- Eine zuständige Ansprechperson für Datenschutz ist intern und extern kommuniziert
- Verantwortlichkeiten zur IT-Sicherheit und Administration von Software wurden bestimmt
- Alle mit der Datenverarbeitung Beschäftigten werden bei Aufnahme ihrer Tätigkeit schriftlich auf die Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten verpflichtet
- Alle mit der Datenverarbeitung Beschäftigten wurden über den Umgang mit Betroffenenrechten informiert
- Alle mit der Datenverarbeitung Beschäftigten wurden darüber informiert, was im Fall von Sicherheitsvorfällen und Datenschutzvorfällen zu tun ist
- Es gibt Regelungen zum Einsatz privater IT-Geräte und der Arbeit in privaten Räumlichkeiten (Home Office / Mobiles Arbeiten)
- Es gibt eine Regelung zum Speichern von Daten
- Es gibt eine Regelung zum Vernichten und Löschen von Dokumenten und Daten

2. Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

2.1 Zutritt - Die Maßnahmen zum Zutritt sollen einen unbefugten physikalischen Zutritt zu Räumlichkeiten verhindern, in denen personenbezogene Daten verarbeitet oder verwahrt werden.

- Der Zutritt in die Geschäftsräume erfolgt mit einem Transponderchip bzw. mit einem Schlüssel
- Die Tür zu den Geschäftsräumen ist verschlossen. Besucher müssen klingeln und werden während des Besuches durch die Geschäftsräume begleitet
- Der Zutritt zu den Büro-Arbeitsplätzen erfolgt nur mit Schlüssel zum Büro für die dafür befugten Personen

2.2 Zugang - Die Maßnahmen zum Zugang sollen einen unbefugten Zugang auf personenbezogene Daten und an Datenverarbeitungsgeräten verhindern.

- Die Anmeldung / Authentifizierung am Arbeitsplatz erfolgt mit einem individuellen Benutzernamen und Passwort
- Es existiert eine Passwortregelung, welche bei bestimmten Systemen um eine technisch erzwungene Passwortregelung unterstützt wird
- Einsatz von Firewalls
- Alle Aktenschränke sind grundsätzlich abschließbar und stehen in den jeweiligen Büros zur Verfügung
- Kopiergeräte und Multifunktionsgeräte sind grundsätzlich nicht für Dritte zugänglich

2.3 Zugriff - Die Maßnahmen zum Zugriff sollen den direkten auf die personenbezogenen Daten verhindern bzw. erschweren sollen.

- Die Anmeldung / Authentifizierung für die jeweilig genutzte Software erfolgt mit einem individuellen Benutzernamen und Passwort
- Für die Erteilung und Entziehung von Zugriffsrechten einzelner Softwareanwendungen existiert ein interner Freigabeprozess

2.4 Trennungskontrolle - Die Trennungskontrolle soll sicherstellen, dass Datenbestände für unterschiedliche Zwecke getrennt verarbeitet werden.

- Die eingesetzte Software verfügt über eine Mandantentrennung
- Unterschiedliche Personenkategorien werden in getrennten Datenbeständen verarbeitet (Beschäftigtendaten / Kundendaten)
- Unterschiedliche Verarbeitungszwecke werden mit eingegrenzten Zugriffsrechten durchgeführt und der Zugriff aus Daten wird minimiert

2.5 Pseudonymisierung - Bei einer Pseudonymisierung können die Daten nicht mehr einer spezifischen Person zugeordnet werden, ohne dass zusätzliche Informationen hinzugezogen werden müssen. Der Zugriff auf diese zusätzlichen Informationen ist entsprechend zu reglementieren.

- Im Falle einer Pseudonymisierung werden die Zuordnungsdaten in getrennten Systemen gespeichert und ein Zugriff reduziert

3. Maßnahmen zur Integrität

Weitergabekontrolle - Die Maßnahmen zur Weitergabekontrolle sollen sicherstellen, 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.

- Einsatz von VPN auf das Firmennetzwerk
- Bereitstellung verschlüsselter Internet-Verbindungen über SSL, HTTPS, SFTP

4. Maßnahmen zur Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

Diese Maßnahmen sollen sicherstellen, dass die Daten stets für die relevante Verarbeitung und auch in Stoßzeiten verfügbar sind und bei Verlust oder Zerstörung schnell wiederhergestellt werden können.

- Regelmäßiges Einspielen von Sicherheitssoftware (Patches)
- Regelmäßige Datenspeicherung auf Grundlage eines Back-Up-Konzeptes
- Unser IT-Dienstleister verfügt über eine ISO 27001 Zertifizierung

5. Maßnahmen der Unterauftragnehmer:

Die technischen und organisatorischen Maßnahmen der Unterauftragnehmer finden sich unter:

- Hetzner Online GmbH:
<https://www.hetzner.com/AV/TOM.pdf>
- IONOS SE:
https://www.ionos.de/terms-gtc/fileadmin/pdf/terms-gtc/DE/AVV/DE_AVV_TOM_v1.0.pdf
- Canny Inc.:
<https://drive.studypilot.app/s/w8JNkezzSAq7QoN>
- Mailgun Technologies Inc.:
<https://sinch.com/de/legal/terms-and-conditions/other-sinch-terms-conditions/data-protection-agreement/>
- Google LLC (Firebase):
<https://firebase.google.com/terms/data-processing-terms#appendix-2:-security-measures>