Auftragsverarbeitungs-vereinbarung

Conbool

Version 1.0 – Stand: März 2025

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Deutschland

info@conbool.com
https://conbool.com

Inhalt

Auftragsverarbeitungsvereinbarung

Gemäß Art. 28 Abs. 3 DSGVO ist es erforderlich, dass die Vertragsparteien ihre datenschutzrechtlichen Verpflichtungen durch eine Vereinbarung zur Auftragsverarbeitung regeln, um die Verarbeitung personenbezogener Daten (nachfolgend Daten) im Rahmen der AGB (nachfolgend Hauptvertrag) rechtssicher zu gestalten.

Die folgende Auftragsverarbeitungsvereinbarung findet Anwendung auf die Tätigkeiten, die mit dem Vertrag in Zusammenhand stehen und bei denen Beschäftigte der Conbool GmbH (nachfolgend Auftragnehmer) oder durch den Auftragnehmer Beauftrage Daten im Auftrag des Auftraggebers verarbeiten. Diese basiert auf der Vorlage des Bayerischen Landesamtes für Datenschutzaufsicht.

§ 1 Gegenstand und Dauer der Auftragsverarbeitung

1. Der Gegenstand dieser Vereinbarung sind die im Rahmen der Leistungserbringung gemäß Leistungsbeschreibung und Hauptvertrag geltenden Rechte und Pflichten der Parteien, soweit eine Datenverarbeitung durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die zur Erfüllung des Auftrages und die eine Auftragsverarbeitung durch den Auftragnehmer darstellen.
2. Die vertraglich vereinbarten Dienstleistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht, sofern nicht zur Erbringung der Leistung der Datentransfer in Drittstaaten erforderlich ist. Für den Fall, dass eine Übermittlung in einen Drittstaat erfolgt, stellt der Auftragnehmer sicher, dass die Voraussetzungen nach Art. 44 ff. DSGVO erfüllt sind.
3. Für die Erbringung bestimmter Dienstleistungen können personenbezogene Daten an Subunternehmer übermittelt werden, die außerhalb des Europäischen Wirtschaftsraums (EWR) ansässig sind. Die Verarbeitung personenbezogener Daten durch Subunternehmer wie Supabase erfolgt primär innerhalb des Europäischen Wirtschaftsraums (EWR). Sollte eine Übertragung in Drittländer notwendig sein, wird diese gemäß Art. 46 DSGVO durch Standardvertragsklauseln abgesichert.
4. Für Datenübertragungen in Drittländer stellt der Auftragnehmer sicher, dass geeignete Garantien gemäß Art. 46 DSGVO bestehen, insbesondere durch den Abschluss von Standardvertragsklauseln (SCCs). Zusätzlich werden technische Maßnahmen wie End-to-End-Verschlüsselung implementiert.
5. Mit dem Abschluss des Hauptvertrags beginnt die Verarbeitung der Daten und erfolgt auf unbestimmte Zeit bis zur Kündigung dieser Auftragsverarbeitungsvereinbarung oder des Hauptvertrags.
6. Der Auftraggeber hat das Recht den zugrundeliegenden Hauptvertrag sowie die Auftragsverarbeitungsvereinbarung jederzeit ohne Einhaltung einer Frist zu kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmung dieser Vereinbarung vorliegt.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen

Art und Zweck der Verarbeitung (entsprechend der Definition von Art. 4 Nr.2 DSGVO)

1. Die Datenverarbeitung umfasst alle Arten von Verarbeitung im Sinne der DSGVO zur Erfüllung des Auftrags.
2. Zweck der Verarbeitung ist die Erbringung der vereinbarten Leistungen aus dem Hauptvertrag, insbesondere die Bereitstellung eines SaaS-basierten E-Mail Security Gateways. Dabei umfasst die Verarbeitung unter anderem die Filterung und Analyse von E-Mails die Verschlüsselung, Entschlüsselung, Signierung und Validierung von E-Mails sowie die Anwendung von Sicherheitsrichtlinien zur Sicherstellung der Integrität und Vertraulichkeit der E-Mail-Kommunikation.

Art der Daten

- Personenstammdaten (z.B. Anrede, Vor- und Nachname, Anschrift)
- Vertragsstammdaten (z.B. Vertragsbeziehung, Produkte/Leistungen)
- Kommunikationsdaten (z.B. Telefonnummer, Mailadressen, Domains)
- Abrechnungs- und Zahlungsdaten
- Metadaten von E-Mails (z.B. Absender, Empfänger, Betreffzeilen)
- Inhaltsdaten von E-Mails (z.B. Textinhalte, Anhänge)

Kategorien betroffener Personen nach Definition von Art. 4 Nr.1 DSGVO

- Alle Personen, die Dienste aus dem Hauptvertrag nutzen
- Alle Personen, über die kommuniziert wird
- E-Mail-Absender und -Empfänger
- Mitarbeiter
- Kunden
- Interessenten
- Geschäftspartner und Lieferanten
- Handelsvertreter
- Ansprechpartner

§ 3 Verantwortlichkeit sowie Verarbeitung dokumentierter Weisungen

1. 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). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.
2. Die Weisungen werden initial durch den Hauptvertrag festgelegt und können vom Auftraggeber danach oder in Textform (z.B. E-Mail) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt und sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform vom Auftraggeber zu bestätigen.
3. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden und den Vertrag außerordentlich zu kündigen. Die Entgeltpflicht des Auftraggebers entfällt mit der Einstellung der Leistung durch den Auftragnehmer. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.
4. Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit kündigen, wenn der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

§ 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf 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 Artikel 28 Abs. 3 a) DSGVO vor und dessen Voraussetzungen werden gewahrt (z.B. Ermittlungen von Strafverfolgungsbehörden). 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.
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 gewährleistet, dass die zur Verarbeitung überlassenen Daten für keinen anderen, insbesondere nicht für eigene Zwecke, verwendet werden. Ferner gewährleistet der Auftragnehmer, dass sich die mit der Verarbeitung der personenbezogenen Daten zuständigen Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeits-verpflichtung auch nach Beendigung des Auftrags fortbesteht. Gleiches gilt für das

Sozialgeheimnis, das Fernmeldegeheimnis nach § 3 TTDSG und – in Kenntnis der Strafbarkeit – für die Wahrung von Geheimnissen der Berufsgeheimnisträger nach § 203 StGB.

4. 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. Die technischen und organisatorischen Maßnahmen werden vom Auftragnehmer unter Anlage 2 dokumentiert und dem Auftraggeber zur Prüfung bereitgestellt.
5. 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. Für diese Unterstützung kann der Auftragnehmer eine angemessene Vergütung verlangen, sofern die Anfrage nicht auf einem Vertragsverstoß des Auftragnehmers beruht.
6. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.
7. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
8. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt.
9. Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe oder, kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.
10. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen.

11. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO) durchzuführen. Der Auftragnehmer ist berechtigt, eine Verschwiegenheits-erklärung vom Auftraggeber und von dessen beauftragten Prüfer zu verlangen, welche dem Auftraggeber aber nicht daran hindern soll, selbst Nachweis gegenüber der für ihn zuständigen Aufsichtsbehörde zu erbringen. Unmittelbare Wettbewerber des Auftraggebers oder Personen, die für unmittelbare Wettbewerber des Auftraggebers tätig sind, kann der Auftragnehmer als Prüfer ablehnen.
12. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Für Informationen und Unterstützungshandlungen kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit die Kontrolle nicht wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.
13. Der Auftragnehmer stellt dem Auftraggeber, oder einem vom Auftragnehmer beauftragten Prüfer, alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.
14. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.
15. Machen betroffene Person Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützt der Auftragnehmer den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen, soweit die Schadensersatzansprüche nicht auf einem Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer beruhen.

§ 5 Rechte und Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO 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. Bei der Erfüllung seiner Pflichten befolgt der Auftragnehmer die Weisungen des Auftraggebers. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.
2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
3. Im Falle der Beendigung verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in den Diensten gespeichert hat.

4. Auf Anforderung des Auftragnehmers benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

5. 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.

§ 6 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

1. Weisungsberechtigte Personen des Auftraggebers: entsprechen den in den Stammdaten des Kundenaccounts genannten Personen.
2. Auftragnehmer Weisungsempfänger: alle Administratoren der Firma Conbool GmbH
3. Weisungen des Auftraggebers erfolgen schriftlich oder in Textform über die vereinbarten und auf der Website verfügbaren Kommunikationskanäle. In dringenden Fällen können Weisungen telefonisch erfolgen, müssen jedoch unverzüglich schriftlich bestätigt werden.
4. Im Falle eines Wechsels oder einer längerfristigen Verhinderung der Ansprechpartner ist der Vertragspartner unverzüglich und grundsätzlich in schriftlicher oder elektronischer Form über die Nachfolger bzw. Vertreter zu informieren.

§ 7 Weitere Auftragsverarbeiter (Subunternehmer)

1. Der Auftraggeber gestattet dem Auftragnehmer generell weitere Subunternehmer im Sinne des Art. 28 DSGVO zur Vertragserfüllung zu Beauftragen. Der Auftragnehmer trägt dafür Sorge, dass mit diesen Dritten Vereinbarungen im erforderlichen Umfang getroffen werden, um angemessene Datenschutz und Informationssicherheitsmaßnahmen zu gewährleisten.
2. Die zurzeit eingesetzten weiteren Auftragsverarbeiter sind in Anlage 1 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.
3. Der Auftraggeber hat das Recht, innerhalb von 14 Tagen nach Mitteilung über den Einsatz eines neuen Subunternehmers Einspruch zu erheben, sofern ein sachlicher Grund vorliegt
4. Bei einem Einspruch hat der Auftragnehmer die Möglichkeit, die Leistung entweder ohne die vorgesehene Änderung zu erbringen oder – sofern es für ihn nicht zumutbar ist, dies zu tun – die von der Änderung betroffene Leistung dem Auftraggeber innerhalb einer angemessenen Frist (mindestens 14 Tage) nach Einspruchszugang einzustellen. Der Auftraggeber ist nicht mehr verpflichtet, eine Zahlung zu leisten, sobald der Auftragnehmer die Leistung eingestellt hat.
5. Der Auftragnehmer verpflichtet sich, regelmäßige Überprüfungen der Subunternehmer hinsichtlich der Einhaltung der datenschutzrechtlichen Anforderungen durchzuführen und dem Auftraggeber auf Anfrage Nachweise bereitzustellen.
6. Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen. Der Auftragnehmer stellt insbesondere durch regelmäßige

Überprüfungen sicher, dass die weiteren Auftragsverarbeiter die technischen und organisatorischen Maßnahmen einhalten.

7. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

§ 8 Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

1. Im Rahmen seines Verantwortungsbereichs setzt der Auftragnehmer geeignete technische und organisatorische Maßnahmen um, um sicherzustellen, dass die Verarbeitung den Anforderungen der DSGVO entspricht und den Schutz der Rechte und Freiheiten der betroffenen Person gewährleistet ist. Der Auftraggeber sorgt in seinem Verantwortungsbereich gemäß Art. 32 DSGVO für geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung langfristig zu gewährleisten.
2. Die derzeitigen technischen und organisatorischen Maßnahmen, die der Auftragnehmer ergriffen hat, können in Anlage 2 eingesehen werden. Der Auftragnehmer stellt klar, dass die technischen und organisatorischen Maßnahmen, die unter dem Link aufgeführt sind, lediglich technische Beschreibungen sind und nicht als Teil dieser Vereinbarung betrachtet werden sollten.
3. Der Auftragnehmer führt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen durch, um die Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO zu gewährleisten.
4. Im Lauf der Zeit nimmt der Auftragnehmer Anpassungen der getroffenen Maßnahmen vor, um Entwicklungen beim Stand der Technik und Veränderungen in der Risikolage Rechnung zu tragen. Der Auftragnehmer kann die getroffenen technischen und organisatorischen Maßnahmen ändern, solange dies nicht zu einem Schutzniveau führt, das unter dem nach Art. 32 DSGVO geforderten liegt.

§ 9 Haftung

1. Haftung und Schadenersatz sind in Art. 82 DSGVO geregelt.
2. Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen
3. „Im Falle einer Datenschutzverletzung gemäß Art. 33 DSGVO verpflichtet sich der Auftragnehmer:
    a. Den Auftraggeber unverzüglich zu informieren (spätestens innerhalb von 24 Stunden).
    b. Alle notwendigen Maßnahmen zur Eindämmung des Vorfalls und zur Vermeidung weiterer Verstöße zu ergreifen.
    c. Den Auftraggeber bei der Meldung an die zuständige Aufsichtsbehörde zu unterstützen.“

§ 10 Sonstiges

1. Sollte das Eigentum oder die Daten des Auftraggebers, die verarbeitet werden sollen, beim Auftragnehmer durch Maßnahmen Dritter (wie Pfändung oder Beschlagnahme), durch Insolvenz- oder Vergleichsverfahren oder durch andere Ereignisse in Gefahr geraten, muss der Auftragnehmer den Auftraggeber ohne Verzögerung informieren.
2. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
3. Der Auftragnehmer ist berechtigt, diese Vereinbarung anzupassen, wenn dies aufgrund gesetzlicher Änderungen erforderlich ist oder um neue technische Standards umzusetzen. Der Auftraggeber wird mindestens vier Wochen vor Inkrafttreten schriftlich informiert und hat das Recht, innerhalb dieser Frist Einspruch zu erheben. Im Falle eines Widerspruchs durch den Auftraggeber, steht dem Auftragnehmer ein außerordentliches Kündigungsrecht zu.
4. Der Auftraggeber akzeptiert diese Vereinbarung als Teil der AGB für die von ihm gebuchten Produkte. Im Falle von Widersprüchen haben die Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung Vorrang vor den Bestimmungen des Hauptvertrags.
5. Sollten wesentliche Änderungen bei den eingesetzten Subunternehmern oder deren Datenschutzmaßnahmen auftreten, informiert der Auftragnehmer den Auftraggeber unverzüglich und passt diese Vereinbarung entsprechend an
6. Es gilt deutsches Recht.

Anlage 1 Weitere Auftragsverarbeiter

1. **IONOS SE**

- **Adresse:** Elgendorfer Straße 7, 56410 Montabaur, Deutschland

- **Beschreibung der Teilleistung:**
  Bereitstellung, Betrieb und Wartung von Produkten; insbesondere:
  a. Betrieb, Wartung und Pflege der Produkte
  b. Bereitstellung der physischen Umgebung für den Betrieb der Conbool GmbH Website und Anwendung
  c. Betrieb der Plattform und Bereitstellung von dedizierten und virtuellen Servern sowie Cloud Lösungen.

2. **Supabase Inc.**

- **Adresse:** 970 Toa Payoh North #07-04, Singapore
- **Beschreibung der Teilleistung:**
  Backend Datenbank, welche zur Speicherung und Verarbeitung Dienst-relevanter Daten sowie zur Nutzerverwaltung und Authentifizierung verwendet wird

- Die Datenverarbeitung erfolgt primär auf Servern innerhalb der Europäischen Union (z. B. Frankfurt am Main)

- Supabase gewährleistet durch geeignete technische und organisatorische Maßnahmen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten personenbezogenen Daten sichergestellt ist. Dazu gehören unter anderem Verschlüsselung der Daten bei Übertragung und Speicherung sowie Zugriffskontrollen gemäß den Vorgaben der DSGVO.

- Sollte eine Übertragung in Drittländer erforderlich sein, stellt Supabase sicher, dass alle datenschutzrechtlichen Anforderungen gemäß Art. 44 ff. DSGVO erfüllt werden, insbesondere durch den Abschluss von Standardvertragsklauseln (SCCs).

- Eine entsprechender Auftragsverarbeitungsvertrag wurde mit Supabase Inc. geschlossen.

- Der Auftragnehmer überprüft regelmäßig die Einhaltung der vertraglich vereinbarten Datenschutzmaßnahmen durch Supabase, insbesondere hinsichtlich der Datenübertragung in Drittländer

Anlage 2 Technische und organisatorische Maßnahmen (TOMs)

1. Vertraulichkeit

Maßnahmen zur Sicherstellung, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben:

Zutrittskontrolle (physischer Zugang IONOS Rechenzentrum)

- Sicherheitsschleusen und Videoüberwachung in den Rechenzentren von IONOS (zertifiziert nach ISO 27001).
- Zutritt nur für autorisierte Personen durch elektronische Zugangskontrollen (z. B. Transponder, biometrische Scanner).
- Besucherregistrierung und Begleitung durch autorisiertes Personal.
- Regelmäßige Überprüfung und Protokollierung der Zugriffsrechte.

Zugangskontrolle (digitaler Zugang)

- Multi-Faktor-Authentifizierung (MFA) für alle administrativen Zugänge.
- Strenge Passwortrichtlinien (regelmäßige Änderungen, Mindestkomplexität).
- VPN-Verbindungen für Remote-Zugriffe auf interne Systeme.
- Verschlüsselung mobiler Datenträger und Endgeräte.

Zugriffskontrolle (Datenzugriff)

- Rollenbasiertes Berechtigungskonzept nach dem Prinzip der minimalen Rechtevergabe („Need-to-Know-Prinzip“).
- Trennung von Anwendungs- und Administrationszugängen.
- E-Mail-Inhalte werden ausschließlich im Stream verarbeitet und nicht gespeichert.
- Protokollierung und Überwachung aller Zugriffsversuche auf personenbezogene Daten.
- Zugriffe auf personenbezogene Daten oder Metadaten erfolgen ausschließlich durch autorisierte Mitarbeiter mit rollenbasierten Berechtigungen.

Pseudonymisierung

- Pseudonymisierung personenbezogener Daten, wo immer möglich.

Datenverschlüsselung

- Verschlüsselung aller gespeicherten Daten.

Vertraulichkeitsvereinbarungen:

- Verpflichtung aller Mitarbeiter auf Vertraulichkeit und Datenschutz gemäß Art. 28 Abs. 3 DSGVO.

2. Integrität

Maßnahmen zur Sicherstellung der Unveränderbarkeit und Konsistenz von Daten:

Datenintegrität:

- Einsatz von Prüfsummen und Hashing-Verfahren zur Validierung der Datenintegrität.

Weitergabekontrolle

- Verschlüsselung aller Datenübertragungen mittels TLS 1.2 oder höher.
- Nutzung sicherer Kommunikationsprotokolle wie SFTP für den Datenaustausch.
- Dokumentation aller Datenweitergaben an Subunternehmer wie Supabase.

Eingabekontrolle

- Schutz der Logs vor Manipulation durch Zugriffsbeschränkungen und Verschlüsselung.
- Individuelle Benutzerkennungen zur Nachvollziehbarkeit von Änderungen.

3. Verfügbarkeit und Belastbarkeit

Maßnahmen zur Sicherstellung der Verfügbarkeit von Systemen und Diensten:

Ausfallsicherheit

- Nutzung hochverfügbarer Cloud-Infrastrukturen bei IONOS mit redundanten Servern.
- Failover-Systeme zur Minimierung von Ausfallzeiten.
- Notfallpläne für den Betrieb bei technischen Störungen.

Belastbarkeit

- Lasttests zur Überprüfung der Systemstabilität unter Spitzenbelastungen.
- Skalierbare Cloud-Infrastruktur durch Supabase und IONOS, um dynamisch auf erhöhte Anforderungen zu reagieren.

Monitoring

- Permanente Überwachung der Systemressourcen und automatisierte Alarme bei Anomalien.

4. Transparenz

Maßnahmen zur Nachvollziehbarkeit der Verarbeitung:

Dokumentation

- Führen eines Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
- Regelmäßige Datenschutz-Folgenabschätzungen (DSFA) bei neuen Verarbeitungstätigkeiten.

5. Datenschutz durch Technikgestaltung („Privacy by Design“)

Maßnahmen zur Integration des Datenschutzes in die Entwicklung:

Standard-Datenschutzeinstellungen („Privacy by Default“)

- Voreinstellungen für maximale Datensparsamkeit in allen Diensten.

Datenminimierung

- Erhebung nur der Daten, die für den jeweiligen Zweck erforderlich sind.
- Automatische Löschung nicht mehr benötigter Daten nach festgelegten Fristen.

6. Schulungen und Sensibilisierung

Organisatorische Maßnahmen zur Förderung des Datenschutzbewusstseins:

- Regelmäßige Schulungen aller Mitarbeiter zu Datenschutzrichtlinien und IT-Sicherheit.
- Sensibilisierung für den Umgang mit Phishing-Angriffen und Social Engineering.

7. Incident Response Management

Maßnahmen zur Bewältigung von Sicherheitsvorfällen:

- Dokumentierter Prozess zur Erkennung, Meldung und Behebung von Datenschutzverletzungen.
- Benachrichtigung des Auftraggebers innerhalb von 24 Stunden bei einem Vorfall gemäß Art. 33 DSGVO.
- Zusammenarbeit mit externen Experten bei schwerwiegenden Sicherheitsvorfällen.

8. Organisatorische Maßnahmen

Maßnahmen zur Sicherstellung klarer Verantwortlichkeiten:

- Regelmäßige interne Audits zur Überprüfung der Einhaltung datenschutzrechtlicher Vorgaben.
- Laufende Aktualisierung der Sicherheitsmaßnahmen entsprechend dem Stand der Technik.
- Verfahren zur Wahrnehmung von Betroffenenrechten gemäß Kap. III DSGVO.