



## Vereinbarung zur Auftragsverarbeitung (AVV)

gemäß Art. 28 DSGVO

*Stand: August 2026*

zwischen dem Kunden der Plattform VAFE - nachfolgend **"Auftraggeber"** -

und

Felix Thor-Sippel, handelnd unter der Geschäftsbezeichnung VAFE, Ölbergstraße 14D, 37351  
Dingelstädt, OT Helmsdorf, Deutschland - nachfolgend **"Auftragnehmer"** -

---

### Präambel

Der Auftraggeber nutzt die Software-as-a-Service-Plattform VAFE (vafe.io) des Auftragnehmers zur automatisierten Erstellung und Veröffentlichung von Social-Media-Inhalten auf Grundlage der Allgemeinen Geschäftsbedingungen des Auftragnehmers ("Hauptvertrag"). Im Rahmen dieser Nutzung übermittelt der Auftraggeber Daten an die Plattform, die personenbezogene Daten Dritter enthalten können. Insoweit verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers im Sinne des Art. 28 DSGVO. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien.

Diese Vereinbarung wird durch Bezugnahme in den Allgemeinen Geschäftsbedingungen des Auftragnehmers Bestandteil des Hauptvertrags und gilt automatisch mit dessen Abschluss, ohne dass es einer gesonderten Unterzeichnung bedarf. Der Auftraggeber erkennt diese Vereinbarung mit Vertragsschluss als Teil der Allgemeinen Geschäftsbedingungen an.

Diese Vereinbarung findet Anwendung, soweit der Auftraggeber als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO personenbezogene Daten in die Plattform eingibt oder hochlädt und der Auftragnehmer diese Daten in seinem Auftrag verarbeitet.

---

### § 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand der Verarbeitung ist die Erbringung der im Hauptvertrag beschriebenen Leistungen: die automatisierte Erstellung von Bildbeiträgen für soziale Medien ("Inhalte") auf Basis der vom Auftraggeber bereitgestellten Daten sowie deren Veröffentlichung über die vom Auftraggeber angebundene Drittplattform.

**(2)** Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags. Sie endet mit dessen Beendigung, vorbehaltlich der Regelungen zur Löschung und Rückgabe in § 12 dieser Vereinbarung.

---

## **§ 2 Art und Zweck der Verarbeitung**

**(1)** Die Verarbeitung umfasst insbesondere folgende Verarbeitungstätigkeiten: Speicherung und Organisation der vom Auftraggeber eingegebenen oder hochgeladenen Daten; automatisierte Generierung von Textbestandteilen unter Einsatz von KI-Sprachmodellen; grafische Aufbereitung (Rendering) von Bildbeiträgen; Übermittlung freigegebener Inhalte an die vom Auftraggeber angebundene Drittplattform zum Zweck der Veröffentlichung; Bereitstellung der Inhalte zur Prüfung und Freigabe im Kundenkonto des Auftraggebers.

**(2)** Zweck der Verarbeitung ist ausschließlich die Erfüllung des Hauptvertrags. Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt.

**(3)** Die Verarbeitung erfolgt auf Servern in der Europäischen Union. Übermittlungen in Drittländer finden nur unter den in § 10 und Anhang 1 genannten Voraussetzungen statt (geeignete Garantien nach Kapitel V DSGVO, insbesondere Angemessenheitsbeschluss oder EU-Standardvertragsklauseln).

---

## **§ 3 Art der personenbezogenen Daten und Kategorien betroffener Personen**

**(1)** Gegenstand der Verarbeitung können insbesondere folgende Datenarten sein:

- Kontakt- und Identifikationsdaten (z. B. Namen, Telefonnummern, E-Mail-Adressen von Ansprechpartnern)
- Adress- und Objektdaten, soweit diese einen Personenbezug aufweisen (z. B. Adressen von Objekten natürlicher Personen)
- Bilddaten, soweit auf hochgeladenen Bildern Personen abgebildet oder identifizierbar sind
- Freitextangaben in Beschreibungen, soweit diese personenbezogene Angaben enthalten

**(2)** Von der Verarbeitung können insbesondere folgende Kategorien betroffener Personen erfasst sein:

- Ansprechpartner, Eigentümer, Verkäufer oder sonstige mit den verarbeiteten Objektdaten in Verbindung stehende Personen
- Mitarbeiter und Beauftragte des Auftraggebers
- Auf Bildmaterial abgebildete oder in Freitexten erwähnte Personen

**(3)** Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der vereinbarten Verarbeitung. Der Auftraggeber verpflichtet sich, solche Daten nicht in die Plattform einzugeben.

---

## **§ 4 Verantwortlichkeit und Verarbeitung auf dokumentierte Weisung**

**(1)** Der Auftraggeber ist im Rahmen dieser Vereinbarung Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Bestehen einer Rechtsgrundlage für die von ihm eingegebenen personenbezogenen Daten Dritter, allein verantwortlich.

**(2)** Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

**(3)** Die Nutzung der Funktionen der Plattform durch den Auftraggeber (insbesondere das Eingeben und Hochladen von Daten, das Auslösen der Inhaltserstellung sowie die Freigabe von Inhalten zur Veröffentlichung) gilt als dokumentierte Weisung im Sinne dieser Vereinbarung. Weisungen außerhalb des in der Plattform vorgesehenen Funktionsumfangs bedürfen der Textform und können vom Auftragnehmer abgelehnt werden, soweit sie technisch nicht umsetzbar oder vom Hauptvertrag nicht gedeckt sind.

**(4)** Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung bis zu ihrer Bestätigung oder Änderung durch den Auftraggeber auszusetzen.

---

## **§ 5 Pflichten des Auftragnehmers**

**(1)** Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeitspflicht besteht auch nach Beendigung dieser Vereinbarung fort.

**(2)** Der Auftragnehmer ergreift alle nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses bestehenden Maßnahmen sind in Anhang 2 beschrieben. Der Auftragnehmer darf diese Maßnahmen fortentwickeln und durch gleichwertige oder bessere Maßnahmen ersetzen, solange das vereinbarte Schutzniveau nicht unterschritten wird.

**(3)** Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen dabei, seinen Pflichten zur Beantwortung von Anträgen betroffener Personen (Kapitel III DSGVO) nachzukommen (§ 7 dieser Vereinbarung).

**(4)** Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten, Benachrichtigung betroffener Personen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

**(5)** Der Auftragnehmer meldet dem Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die den Auftraggeber betrifft. Die Meldung enthält, soweit möglich, die in Art. 33 Abs. 3 DSGVO genannten Informationen. Die Meldung erfolgt an die im Kundenkonto hinterlegte E-Mail-Adresse des Auftraggebers.

(6) Ein Datenschutzbeauftragter ist beim Auftragnehmer nicht bestellt, da die gesetzlichen Voraussetzungen für eine Benennungspflicht (Art. 37 DSGVO, § 38 BDSG) derzeit nicht vorliegen. Ansprechpartner für alle datenschutzrechtlichen Belange ist der Auftragnehmer selbst (kontakt@vafe.io). Sollten die Voraussetzungen einer Benennungspflicht künftig eintreten, wird der Auftragnehmer einen Datenschutzbeauftragten benennen und den Auftraggeber informieren.

(7) Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt; hiervon ausgenommen sind technische Sicherungskopien (Backups), soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

---

## **§ 6 Pflichten des Auftraggebers**

(1) Der Auftraggeber ist als Verantwortlicher für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich. Er stellt insbesondere sicher, dass für die von ihm in die Plattform eingegebenen personenbezogenen Daten Dritter eine tragfähige Rechtsgrundlage besteht und die betroffenen Personen, soweit erforderlich, nach Art. 13, 14 DSGVO informiert wurden.

(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder im Zusammenhang mit der Verarbeitung feststellt.

(3) Der Auftraggeber benennt dem Auftragnehmer auf Anfrage einen Ansprechpartner für die im Rahmen dieser Vereinbarung anfallenden datenschutzrechtlichen Fragen. Standardmäßig gilt die im Kundenkonto hinterlegte E-Mail-Adresse als Kontaktweg.

(4) Der Auftraggeber gibt keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) und keine Daten über strafrechtliche Verurteilungen (Art. 10 DSGVO) zur Verarbeitung in die Plattform ein.

---

## **§ 7 Anfragen betroffener Personen**

(1) Wendet sich eine betroffene Person mit Anträgen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit oder Widerspruch unmittelbar an den Auftragnehmer, leitet dieser den Antrag unverzüglich an den Auftraggeber weiter, sofern eine Zuordnung zum Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer beantwortet solche Anträge nicht selbst, sondern verweist die betroffene Person an den Auftraggeber, soweit eine Zuordnung möglich ist.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Anträge betroffener Personen im Rahmen des technisch Möglichen, insbesondere durch die in der Plattform vorhandenen Funktionen zur Einsicht, Berichtigung, zum Export und zur Löschung von Daten. Ein darüber hinausgehender Unterstützungsaufwand kann nach vorheriger Ankündigung angemessen vergütet werden, soweit er nicht auf einem Verschulden des Auftragnehmers beruht.

---

## § 8 Maßnahmen zur Sicherheit der Verarbeitung (Art. 32 DSGVO)

(1) Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die konkreten Maßnahmen sind in **Anhang 2 (Technische und organisatorische Maßnahmen)** beschrieben, der Bestandteil dieser Vereinbarung ist.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer ist berechtigt, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau der in Anhang 2 festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

---

## § 9 Nachweis und Überprüfung

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

(2) Der Nachweis erfolgt vorrangig durch die Vorlage geeigneter Dokumentation, insbesondere der Beschreibung der technischen und organisatorischen Maßnahmen (Anhang 2), aktueller Bescheinigungen oder Berichte der eingesetzten Subunternehmer (z. B. Zertifizierungen, Auditberichte der Infrastrukturanbieter) sowie Eigenauskünften des Auftragnehmers.

(3) Der Auftraggeber ist berechtigt, Überprüfungen - einschließlich Inspektionen - durchzuführen oder durch einen im Einzelfall zu benennenden, zur Verschwiegenheit verpflichteten Prüfer durchführen zu lassen, soweit die Dokumentation nach Abs. 2 im Einzelfall keinen hinreichenden Nachweis erbringt. Überprüfungen vor Ort erfolgen nach angemessener Vorankündigung (in der Regel mindestens 14 Kalendertage), zu üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und höchstens einmal pro Kalenderjahr, soweit kein konkreter Anlass (z. B. eine Datenschutzverletzung) eine weitere Überprüfung erfordert. Angesichts der Größe des Auftragnehmers als Einzelunternehmer erfolgt die Terminabstimmung für Vor-Ort-Kontrollen unter angemessener Berücksichtigung der betrieblichen Kapazitäten. Der Auftragnehmer kann für die Unterstützung von Überprüfungen, die über den Nachweis nach Abs. 2 hinausgehen und nicht durch einen Verstoß des Auftragnehmers veranlasst sind, eine angemessene Vergütung verlangen.

(4) Wettbewerber des Auftragnehmers sind als Prüfer ausgeschlossen.

---

## § 10 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung zur Einschaltung weiterer Auftragsverarbeiter ("Subunternehmer") im Sinne des Art. 28 Abs. 2 DSGVO. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Subunternehmer sind in **Anhang 1** aufgeführt, der Bestandteil dieser Vereinbarung ist.

(2) Der Auftragnehmer stellt durch vertragliche Vereinbarungen nach Maßgabe des Art. 28 Abs. 2–4 DSGVO sicher, dass jedem Subunternehmer dieselben Datenschutzpflichten auferlegt werden, die in dieser Vereinbarung festgelegt sind. Erfolgt die Verarbeitung durch einen Subunternehmer in einem Drittland, stellt der Auftragnehmer die Zulässigkeit der Übermittlung durch geeignete

Garantien nach Kapitel V DSGVO sicher (insbesondere Angemessenheitsbeschluss nach Art. 45 DSGVO oder EU-Standardvertragsklauseln nach Art. 46 DSGVO). Der jeweilige Übermittlungsmechanismus ist in Anhang 1 ausgewiesen.

**(3)** Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Subunternehmern mindestens **vier Wochen** vor deren Wirksamwerden in Textform (z. B. per E-Mail an die im Kundenkonto hinterlegte Adresse oder durch Hinweis im Kundenkonto). Der Auftraggeber kann der Änderung aus wichtigem datenschutzrechtlichem Grund widersprechen. Im Fall eines Widerspruchs sind beide Parteien berechtigt, den Hauptvertrag und diese Vereinbarung außerordentlich zum Zeitpunkt des Wirksamwerdens der Änderung zu kündigen, wenn eine einvernehmliche Lösung (z. B. Verzicht auf den betreffenden Subunternehmer) nicht möglich oder dem Auftragnehmer nicht zumutbar ist.

**(4)** Nicht als Subunternehmer im Sinne dieser Vereinbarung gelten Dienstleister, deren Leistungen der Auftraggeber selbst und in eigener Verantwortung anbindet. Dies betrifft insbesondere die vom Auftraggeber angebundene Drittplattform (derzeit Meta Platforms Ireland Ltd. / Instagram): Die Übermittlung freigegebener Inhalte an das eigene Konto des Auftraggebers bei der Drittplattform erfolgt auf dessen Weisung (Freigabe) im Rahmen der Auftragsverarbeitung; die anschließende Verarbeitung durch den Drittplattform-Betreiber erfolgt jedoch auf Grundlage des eigenen Vertrags- und Nutzungsverhältnisses zwischen dem Auftraggeber und dem Drittplattform-Betreiber, in dem dieser als eigenständiger Verantwortlicher handelt. Der Auftragnehmer ist für die Datenverarbeitung durch den Drittplattform-Betreiber nicht verantwortlich.

---

## § 11 Haftung

**(1)** Für die Haftung der Parteien im Innen- und Außenverhältnis gilt Art. 82 DSGVO. Im Innenverhältnis haftet jede Partei nur für den Teil des Schadens, der auf ihren eigenen Verantwortungsbeitrag entfällt.

**(2)** Der Auftraggeber stellt den Auftragnehmer im Innenverhältnis von Ansprüchen betroffener Personen und von Bußgeldern frei, soweit diese darauf beruhen, dass der Auftraggeber personenbezogene Daten ohne tragfähige Rechtsgrundlage in die Plattform eingegeben oder seine Pflichten als Verantwortlicher verletzt hat, und soweit der Auftraggeber dies zu vertreten hat.

**(3)** Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.

---

## § 12 Löschung und Rückgabe, Laufzeit, Schlussbestimmungen

**(1)** Nach Beendigung des Hauptvertrags löscht der Auftragnehmer sämtliche im Auftrag verarbeiteten personenbezogenen Daten, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung besteht (z. B. handels- und steuerrechtliche Aufbewahrungspflichten für Abrechnungsdaten). Vor der Löschung kann der Auftraggeber seine Daten nach Maßgabe des Hauptvertrags exportieren.

**(2)** Der Auftraggeber kann die Löschung jederzeit selbst über die hierfür vorgesehene Funktion im Kundenkonto veranlassen (vollständige Kontolöschung); die Löschung erfolgt in diesem Fall unmittelbar, vorbehaltlich gesetzlicher Aufbewahrungspflichten. Alternativ kann der Auftraggeber die Löschung in Textform (kontakt@vafe.io) verlangen; sie wird in diesem Fall innerhalb von 30 Tagen umgesetzt.

**(3)** Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, darf der Auftragnehmer über das Vertragsende hinaus entsprechend den jeweiligen gesetzlichen Fristen aufbewahren.

**(4)** Diese Vereinbarung tritt mit Abschluss des Hauptvertrags in Kraft und endet mit dessen Beendigung, unbeschadet fortgeltender Pflichten (insbesondere Vertraulichkeit und Löschung).

**(5)** Im Fall von Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen hinsichtlich der Verarbeitung personenbezogener Daten die Regelungen dieser Vereinbarung vor.

**(6)** Es gilt das Recht der Bundesrepublik Deutschland. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.

**(7)** Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine wirksame Regelung, die dem Zweck der unwirksamen Bestimmung am nächsten kommt.

## Anhang 1 — Subunternehmer (weitere Auftragsverarbeiter)

| Subunternehmer                 | Sitz                    | Leistung                                                       | Serverstandort / Datenverarbeitung                    | Drittlandtransfer & Garantien                                                                                                                           |
|--------------------------------|-------------------------|----------------------------------------------------------------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supabase Inc.                  | USA                     | Datenbank, Authentifizierung, verschlüsselte Token-Speicherung | AWS-Region eu-west-1 (Irland)                         | Mögliche Support-Zugriffe aus den USA; EU-Standardvertragsklauseln (Art. 46 DSGVO) als Bestandteil des AVV                                              |
| OpenAI Ireland Ltd.            | Irland                  | KI-gestützte Textgenerierung                                   | EU/USA                                                | Zertifizierung der US-Konzerngesellschaft unter dem EU-US Data Privacy Framework (Art. 45 DSGVO); ergänzend EU-Standardvertragsklauseln (Art. 46 DSGVO) |
| Nifty Software GmbH („Placid“) | Österreich              | Bildrendering (grafische Aufbereitung der Inhalte)             | EU                                                    | Kein Drittlandtransfer                                                                                                                                  |
| IONOS SE                       | Deutschland (Montabaur) | Serverhosting der Workflow-Automatisierung (n8n)               | Deutschland/EU                                        | Kein Drittlandtransfer                                                                                                                                  |
| Vercel Inc.                    | USA                     | Hosting der Web-Anwendung (vafe.io)                            | EU (Region Frankfurt); Edge-/CDN-Infrastruktur global | Zertifizierung unter dem EU-US Data Privacy Framework (Art. 45 DSGVO)                                                                                   |

|                                      |     |                                                  |                     |                                                                          |
|--------------------------------------|-----|--------------------------------------------------|---------------------|--------------------------------------------------------------------------|
| Functional Software, Inc. („Sentry“) | USA | Fehler- und Stabilitätsüberwachung der Anwendung | EU-Datenspeicherung | Data Processing Addendum mit EU-Standardvertragsklauseln (Art. 46 DSGVO) |
|--------------------------------------|-----|--------------------------------------------------|---------------------|--------------------------------------------------------------------------|

**Hinweis zur Drittplattform:** Der Betreiber der vom Auftraggeber angebundenen Drittplattform (derzeit Meta Platforms Ireland Ltd. / Instagram) ist **kein Subunternehmer** des Auftragnehmers, sondern verarbeitet Daten als eigenständiger Verantwortlicher auf Grundlage des eigenen Nutzungsverhältnisses mit dem Auftraggeber (vgl. § 10 Abs. 4 dieser Vereinbarung).

**Hinweis zum Zahlungsdienstleister:** Der für die Abwicklung der Vergütung eingesetzte Zahlungsdienstleister (Stripe) verarbeitet Zahlungsdaten des Auftraggebers selbst; diese Verarbeitung ist nicht Gegenstand der Auftragsverarbeitung nach dieser Vereinbarung und in der Datenschutzerklärung des Auftragnehmers beschrieben.

## Anhang 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

### 1. Vertraulichkeit

#### Zugangskontrolle (Systeme):

- Zugriff auf alle Verwaltungs- und Infrastruktursysteme (Datenbank, Hosting, Quellcodeverwaltung, Zahlungsdienstleister) ausschließlich durch den Auftragnehmer, jeweils gesichert durch individuelle Zugangsdaten und Zwei-Faktor-Authentifizierung (2FA)
- Kundenzugänge zur Plattform ausschließlich über individuelle Konten mit Passwort-Authentifizierung; Passwörter werden ausschließlich als kryptografische Hashes gespeichert

#### Zugriffskontrolle (Daten):

- Mandantenfähige Datenbankarchitektur mit strikter Zugriffstrennung auf Datenbankebene (Row Level Security): Jeder Kunde kann ausschließlich auf die Daten seines eigenen Mandanten zugreifen
- Verschlüsselte Speicherung sensibler Zugangsdaten (insbesondere Instagram-Access-Token) in einem dedizierten Secrets-Speicher (Supabase Vault)
- Privilegierte Datenbankzugriffe der Anwendung erfolgen ausschließlich serverseitig mit expliziter Mandantenfilterung

#### Trennungskontrolle:

- Logische Mandantentrennung sämtlicher Kundendaten auf Datenbankebene (Row Level Security)
- Trennung von Produktions- und Testumgebungen bzw. Test-Mandanten

### 2. Integrität

#### Übertragungskontrolle:

- Sämtliche Datenübertragungen zwischen Endgerät, Anwendung, Datenbank und eingebundenen Diensten erfolgen ausschließlich transportverschlüsselt (TLS/HTTPS)



- Übermittlungen an Subunternehmer nur im für die jeweilige Leistung erforderlichen Umfang

**Eingabekontrolle:**

- Statusänderungen an Verarbeitungsvorgängen werden systemseitig protokolliert (Zeitstempel)
- Fehlerereignisse werden über ein Monitoring-System (Sentry, EU-Datenspeicherung) erfasst

**3. Verfügbarkeit und Belastbarkeit**

- Speicherung der Daten in der Infrastruktur eines zertifizierten Cloud-Anbieters (AWS-Region eu-west-1 über Supabase) mit automatisierten Sicherungskopien
- Verschlüsselung der gespeicherten Daten (Encryption at Rest) durch die eingesetzte Cloud-Infrastruktur
- Überwachung der Verfügbarkeit kritischer Hintergrundprozesse durch automatisierte Prüfmechanismen (Uptime-/Healthcheck-Monitoring)
- Schutz öffentlich erreichbarer Formulare vor automatisiertem Missbrauch (Bot-Schutz)

**4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

- Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen im Rahmen der Weiterentwicklung der Plattform
- Auswertung von Fehler- und Sicherheitsereignissen über das Monitoring-System
- Auswahl von Subunternehmern unter Berücksichtigung von deren Datenschutz- und Sicherheitsniveau; Abschluss von Auftragsverarbeitungsverträgen mit sämtlichen Subunternehmern
- Umgehende Prüfung und Dokumentation bei Hinweisen auf Sicherheitsvorfälle