Auftragsverarbeitungsvertrag (AVV)

Stand: 30. April 2026

zwischen

dem Kunden, der diesen Auftragsverarbeitungsvertrag im Onboarding-Prozess der Plattform „Vinolin Suite" elektronisch akzeptiert oder ihn als unterzeichnetes Dokument zurücksendet (im Folgenden „**Auftraggeber**"),

und

Vinolin UG (haftungsbeschränkt), einer Unternehmergesellschaft (haftungsbeschränkt) mit Sitz in Heilbronn, Deutschland, eingetragen im Handelsregister des Amtsgerichts Stuttgart unter HRB 803539, Geschäftsanschrift: Bildungscampus 11, 74076 Heilbronn, vertreten durch den Geschäftsführer David Blank,

(im Folgenden „**Auftragnehmer**")

— Auftraggeber und Auftragnehmer jeweils eine „**Partei**" und, zusammen, die „**Parteien**" —

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen gemäß den B2B-Nutzungsbedingungen für die Plattform „Vinolin Suite" und der Anlage 1 dieses Vertrags. Dabei wird auch eine Verarbeitung personenbezogener Daten erfolgen. Zur Wahrung der geltenden datenschutzrechtlichen Anforderungen schließen die Parteien den nachfolgenden Vertrag.

Dies vorausgeschickt, vereinbaren die Parteien, was folgt:

§ 1 Gegenstand/Umfang der Beauftragung

(1) Die Zusammenarbeit der Parteien hat zur Folge, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend, „Auftraggeberdaten") erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO verarbeitet.

(2) Die Verarbeitung der Auftraggeberdaten erfolgt gemäß Anlage 1 dieses Vertrags.

(3) Der Auftragnehmer ist berechtigt, einen Teil der Auftraggeberdaten zur Verbesserung der Leistungsfähigkeit der Plattform und der angebotenen Dienste zu verarbeiten, insbesondere zur Verbesserung der KI-gestützten Funktionen, zur Plattform-Optimierung und zur Erstellung anonymisierter oder aggregierter Statistiken. Für den Fall, dass eine Verarbeitung zu eigenen Zwecken stattfindet, gewährleistet der Auftragnehmer, dass die Verarbeitung stets auf Grundlage von Art. 6 DSGVO erfolgt und auch die weiteren Anforderungen der DSGVO eingehalten werden.

(4) Soweit andere Vereinbarungen zwischen Auftraggeber und Auftragnehmer abweichende Regelungen zum Schutz personenbezogener Daten enthalten, gilt vorrangig dieser Vertrag zur Auftragsverarbeitung, sofern die Parteien nicht ausdrücklich etwas anderes vereinbaren.

§ 2 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer trifft in seinem Verantwortungsbereich gemäß Anlage 2 dieses Vertrags alle erforderlichen technisch-organisatorischen Maßnahmen entsprechend Art. 32 DSGVO zum Schutz der personenbezogenen Daten.

(2) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Dem Auftragnehmer ist es daher gestattet, künftig alternative, gleichwertige

Maßnahmen umzusetzen, sofern das festgelegte Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

§ 3 Betroffenenrechte

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich durch geeignete technisch-organisatorische Maßnahmen bei der Bearbeitung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die im Auftrag verarbeiteten Daten nur auf Grundlage einer dokumentierten Weisung des Auftraggebers beauskunften, übertragen, berichtigen, löschen oder deren Verarbeitung einschränken. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter.

(2) Soweit im Leistungsumfang enthalten, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 4 Sonstige Pflichten des Auftragnehmers

Der Auftragnehmer stellt insbesondere die Einhaltung der folgenden Vorgaben sicher:

(1) Die Gewährleistung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, Art. 29 und Art. 32 Abs. 4 DSGVO. Der Auftragnehmer setzt für die Durchführung des Auftrags nur Beschäftigte ein, die zur Vertraulichkeit verpflichtet wurden und zuvor über die für sie relevanten Datenschutzbestimmungen informiert wurden.

(2) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese ausschließlich gemäß den Weisungen des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, eine gesetzliche Verpflichtung zur Verarbeitung liegt vor.

(3) Der Auftraggeber und der Auftragnehmer kooperieren auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit diese den vorliegenden Vertrag betreffen. Dies gilt ebenso für Ermittlungen einer zuständigen Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens, die die Verarbeitung personenbezogener Daten im Zusammenhang mit der Auftragsverarbeitung durch den Auftragnehmer betreffen.

(5) Der Auftragnehmer überprüft regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die Verarbeitung im Verantwortungsbereich des Auftragnehmers den Anforderungen des geltenden Datenschutzrechts entspricht und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

(6) Der Auftragnehmer stellt sicher, dass die getroffenen technischen und organisatorischen Maßnahmen dem Auftraggeber auf Anfrage im Rahmen seiner Kontrollbefugnisse gemäß § 7 dieses Vertrags nachgewiesen werden können.

(7) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber, damit dieser seinen gesetzlichen Pflichten, insbesondere nach Art. 33 und Art. 34 DSGVO, nachkommen kann. Der Auftragnehmer erstellt eine vollständige Dokumentation des Vorfalls und stellt diese dem Auftraggeber zur Verfügung, um weitere Maßnahmen zu ermöglichen.

(8) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich bei der Erfüllung der Informationspflichten gegenüber Aufsichtsbehörden und betroffenen Personen, indem er ihm unverzüglich sämtliche relevanten Informationen zur Verfügung stellt.

(9) Sollte der Auftraggeber verpflichtet sein, eine Datenschutz-Folgenabschätzung durchzuführen, unterstützt der Auftragnehmer ihn entsprechend der Art der Verarbeitung und den ihm vorliegenden Informationen. Dies gilt auch für etwaige Verpflichtungen zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

§ 5 Unterauftragsverhältnisse

(1) Unterauftragsverhältnisse im Sinne dieser Regelung beziehen sich auf Dienstleistungen, die sich direkt auf die Erbringung der Hauptleistung beziehen. Nicht umfasst sind 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 verfügt über eine allgemeine Genehmigung des Auftraggebers für die Beauftragung von Unterauftragsverarbeitern. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt. Der Auftragnehmer ist verpflichtet, den Auftraggeber über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern mit einer angemessenen Vorlauffrist von mindestens dreißig (30) Tagen in Textform zu informieren und dem Auftraggeber damit ausreichend Zeit einzuräumen, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Die jeweils aktuelle Liste der Unterauftragsverarbeiter wird dem Auftraggeber im Vinolin-Dashboard bzw. unter einer dort verlinkten URL zur Verfügung gestellt.

(3) Wenn der Auftragnehmer einen Unterauftragsverarbeiter für die Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Auftraggebers einsetzt, ist dies durch einen entsprechenden Unterauftragsverarbeitungsvertrag abzubilden. Dabei ist sicherzustellen, dass der Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten erfüllt wie der Auftragnehmer. Der Auftragnehmer stellt sicher, dass der Unterauftragsverarbeiter alle Datenschutzanforderungen einhält, die auch für den Auftragnehmer nach diesen Klauseln und den geltenden Datenschutzgesetzen gelten.

(4) Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer sicher, dass die datenschutzrechtlichen Anforderungen durch geeignete Maßnahmen erfüllt werden, insbesondere durch den Abschluss von EU-Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO oder durch andere geeignete Garantien gemäß Kapitel V DSGVO (z. B. Selbstzertifizierung des Unterauftragsverarbeiters unter dem EU-US Data Privacy Framework, soweit anwendbar).

§ 6 Internationale Datenübermittlungen

(1) Jegliche Übermittlung von personenbezogenen Daten durch den Auftragnehmer an ein Drittland oder an eine internationale Organisation erfolgt ausschließlich auf Basis dokumentierter Weisungen des Auftraggebers oder zur Erfüllung einer spezifischen Vorschrift des Unionsrechts oder des Rechts eines Mitgliedstaats, dem der Auftragnehmer unterliegt. Diese Übermittlungen müssen den Anforderungen von Kapitel V der DSGVO entsprechen.

(2) Der Auftraggeber stimmt zu, dass der Auftragnehmer im Rahmen des Einsatzes von Unterauftragsverarbeitern gemäß § 5 dieses Vertrags, insoweit Kapitel V der DSGVO gilt, dessen Anforderungen unter anderem durch den Einsatz von Standardvertragsklauseln einhalten kann.

§ 7 Kontrollrechte

(1) Der Auftraggeber ist berechtigt, nach Abstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

(2) Der Auftragnehmer stellt sicher, dass der Auftraggeber sich von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann.

(3) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen. Solche Nachweise können insbesondere erfolgen durch:

• die Vorlage aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren);

• die Vorlage einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001);

• schriftliche Auskünfte zu den eingesetzten technischen und organisatorischen Maßnahmen.

§ 8 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Grundlage dokumentierter Weisungen des Auftraggebers, es sei denn, er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform). Die Festlegung der initialen Weisungen des Auftraggebers erfolgt im Rahmen dieses Vertrags und der zugrundeliegenden B2B-Nutzungsbedingungen.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen geltendes Datenschutzrecht. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange zu unterbrechen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 9 Löschung und Rückgabe personenbezogener Daten

(1) Es erfolgt keine Erstellung von Kopien oder Duplikaten der Daten ohne Wissen des Auftraggebers. Hiervon ausgenommen sind zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderliche Sicherheitskopien sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Verarbeitungstätigkeiten oder zu einem früheren Zeitpunkt nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der zugrundeliegenden B2B-Nutzungsbedingungen – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

§ 10 Weitere Vertragsparteien

Verantwortliche oder Auftragsverarbeiter, die nicht Partei dieses Vertrags sind, können, mit Zustimmung der Vertragsparteien, diesem Vertrag jederzeit beitreten, indem sie die Anlagen dieses Vertrages ausfüllen und entsprechend bestätigen.

§ 11 Vertragsschluss und Schriftform

(1) Dieser Vertrag wird durch Unterzeichnung beider Parteien oder durch elektronische Akzeptanz seitens des Auftraggebers im Vinolin-Dashboard im Rahmen des Onboarding-Prozesses vor der Live-Schaltung des Shops geschlossen. Sowohl die schriftliche Unterzeichnung als auch die elektronische Akzeptanz erfüllen die Schriftformerfordernisse gemäß Art. 28 Abs. 9 DSGVO.

(2) Der Auftraggeber erhält nach erfolgter Akzeptanz eine Kopie des unterzeichneten Vertrags inklusive aller Anlagen per E-Mail bzw. zum Download im Dashboard.

(3) Der Auftragnehmer ist berechtigt, diesen AVV bei wesentlichen Änderungen der Rechtslage, der Sub-Dienstleister-Konstellation oder der angebotenen Dienste anzupassen. Wesentliche Änderungen werden dem Auftraggeber mit einer Vorlauffrist von mindestens dreißig (30) Tagen in Textform mitgeteilt. Widerspricht der Auftraggeber den Änderungen nicht innerhalb dieser Frist, gelten die Änderungen als angenommen. Der Auftragnehmer wird den Auftraggeber bei der Mitteilung auf diese Folge hinweisen.

Unterschriften

Die Parteien bestätigen mit ihrer Unterschrift, diesen Auftragsverarbeitungs-vertrag einschließlich der Anlagen 1 bis 4 zur Kenntnis genommen und akzeptiert zu haben.

Für den Auftraggeber	**Für den Auftragnehmer**
(Kunde)	Vinolin UG (haftungsbeschränkt)
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift	David Blank, Geschäftsführer
_____	
Name in Druckbuchstaben / Funktion	

Anlage 1: Beschreibung der Verarbeitung

Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung der Software-as-a-Service-Plattform „Vinolin Suite" durch den Auftragnehmer, die es dem Auftraggeber ermöglicht, einen Online-Shop für den Direktvertrieb von Wein und weinbezogenen Produkten zu betreiben. Die Plattform umfasst insbesondere die Einrichtung und Verwaltung des Online-Shops, die Bearbeitung und Abwicklung von Bestellungen, die Konfiguration von Versand- und Zahlungsoptionen, die Verwaltung von Endkundendaten und Bestellhistorie, einen KI-gestützten Sommelier sowie einen Newsletter-Autopiloten.

Dauer der Verarbeitung

Die Dauer dieser Verarbeitung entspricht der Laufzeit der zugrundeliegenden B2B-Nutzungsbedingungen zwischen den Parteien. Die Verarbeitung erfolgt für unbestimmte Zeit und endet mit der Beendigung des Nutzungsvertrags zwischen den Parteien.

Art und Zweck der Verarbeitung

Die Verarbeitung umfasst insbesondere folgende Tätigkeiten:

- Erfassung, Speicherung und Verarbeitung von Endkundendaten im Rahmen des Online-Shop-Betriebs;
- Abwicklung von Bestellungen, Zahlungen und Versand-Avisierungen;
- Bereitstellung KI-gestützter Wein-Empfehlungen für Endkunden auf Basis von Geschmackspräferenzen und Sortiment des Auftraggebers;
- Versand von Transaktions-E-Mails (z. B. Bestellbestätigungen, Versandbestätigungen);
- Versand von Newslettern auf Grundlage entsprechender Einwilligungen der Endkunden;
- Bereitstellung von Authentifizierungs- und Sitzungs-Mechanismen für Endkunden-Konten;
- Verarbeitung im Rahmen von Background-Jobs (z. B. asynchrone Bestellverarbeitung, periodische Aufgaben);
- Bereitstellung von Karten- und Standortfunktionen sowie Bot-Schutzmaßnahmen.

Zweck der Verarbeitung ist die ordnungsgemäße Erfüllung des zwischen Auftraggeber und seinen Endkunden geschlossenen Kaufvertrags sowie die damit zusammenhängenden Geschäftsprozesse des Auftraggebers.

Art der personenbezogenen Daten

Die Verarbeitung umfasst folgende Datenkategorien:

1. Stammdaten der Endkunden

- Name, Vorname, Nachname
- Geschlecht (optional)
- Profilbild (optional)
- Geburtsdatum (optional, im Rahmen der Altersangabe bei der Registrierung; eine Verifikation findet seitens des Auftragnehmers nicht statt)

2. Kontaktdaten

- E-Mail-Adresse (Pflicht)
- E-Mail-Verifikationsstatus
- Telefonnummer (optional)
- Kommunikationspräferenzen (E-Mail-Opt-In)

3. Adressdaten

- Lieferadresse, Rechnungsadresse (Straße, Hausnr., PLZ, Stadt, Land)
- Adress-Snapshot pro Bestellung (zur Erfüllung handelsrechtlicher Aufbewahrungspflichten)

4. Vertrags- und Bestelldaten

- Bestellnummer, Bestellpositionen, Mengen, Preise, Währung
- Bestellstatus, Versandstatus, ggf. Stornierungsgrund
- Sendungsverfolgungs-Identifikatoren
- Rechnungs-/Quittungs-URLs

5. Zahlungsabwicklungs-Identifikatoren

- Stripe Checkout Session ID, Payment Intent ID, Invoice ID
- Webhook-Event-Payloads
- (Hinweis: Vollständige Kartendaten oder IBANs werden nicht beim Auftragnehmer gespeichert, sondern ausschließlich beim Zahlungsdienstleister)

6. Authentifizierungs- und Sitzungsdaten

- Session-Token, OAuth-Tokens (Access / Refresh)
- Anonyme Session-IDs (Aufbewahrung 30 Tage)
- IP-Adresse, User-Agent (bei Login)

7. Marketing- und Einwilligungsdaten

- Newsletter-Status (Pending / Verified / Unsubscribed)
- Newsletter-Verifikationstoken, Unsubscribe-Token
- Account-Marketing-Opt-In

8. KI-Sommelier-Daten

- Chat-Verlauf
- Geschmacksprofil (Freitext)
- Wein-Empfehlungen (mit Anlass, Food-Pairing)
- Bewertungen einzelner KI-Antworten
- Anonyme Sessions mit ggf. nachträglicher Account-Verknüpfung

9. Sonstige Daten

- Zeitstempel (Erstellung, Update jeder Entität)
- Interne Notizen zur Bestellung (durch Auftraggeber verfasst, ggf. mit Bezug zum Endkunden)

Kategorien betroffener Personen

Die Verarbeitung betrifft folgende Kategorien von Personen:

- Endkunden des Auftraggebers (Käufer im Online-Shop)
- Interessenten des Auftraggebers (z. B. Newsletter-Abonnenten, Nutzer des KI-Sommeliers ohne Bestellung)
- Sonstige natürliche Personen, deren Daten im Rahmen der Bestellabwicklung verarbeitet werden (z. B. abweichende Lieferanschriften, Empfänger von Geschenkbestellungen)

Anlage 2: Technisch-organisatorische Maßnahmen (TOMs)

***Hinweis:** Dieser Abschnitt beschreibt die zum Zeitpunkt der Vertragsunterzeichnung vom Auftragnehmer eingesetzten technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Der Auftragnehmer ist berechtigt, diese Maßnahmen weiterzuentwickeln, sofern das festgelegte Sicherheitsniveau nicht unterschritten wird.*

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle (physisch)

Der Auftragnehmer betreibt keine eigenen Rechenzentren oder Serverräume. Sämtliche Server-Infrastruktur wird durch zertifizierte Sub-Dienstleister (siehe Anlage 3) bereitgestellt, die ihrerseits den Schutz vor unberechtigtem Zutritt zu ihren Rechenzentren durch geeignete Maßnahmen sicherstellen (insbesondere Vercel, Neon, Google, Amazon Web Services).

1.2 Zugangskontrolle (logisch)

- Authentifizierung von Mitarbeitern des Auftragnehmers an allen relevanten Systemen über persönliche Benutzerkonten;
- Zwei-Faktor-Authentifizierung (2FA) bei allen externen Diensten, soweit vom jeweiligen Anbieter unterstützt (insbesondere Vercel, Neon, Google);
- Authentifizierung am Vinolin-Dashboard über das Authentifizierungs-Framework Better Auth mit PostgreSQL-basierter Sitzungsverwaltung;
- Zugriffe auf die Produktions-Datenbank sind ausschließlich auf einen begrenzten Personenkreis beschränkt (Geschäftsführung sowie eine für die Softwareentwicklung verantwortliche Person);
- Endkunden-Authentifizierung über Session-Tokens, OAuth (Sign in with Apple, Google), mit verschlüsselter Token-Speicherung.

1.3 Zugriffskontrolle

- Rollenbasiertes Berechtigungskonzept: Mitarbeiter haben jeweils nur Zugriff auf die für ihre Tätigkeit erforderlichen Systeme und Daten (Need-to-know-Prinzip);
- Trennung zwischen Produktions-, Test- und Entwicklungs-Umgebungen;
- Zugriffe auf personenbezogene Daten erfolgen ausschließlich über die Anwendungslogik der Plattform, die durch Berechtigungsprüfungen geschützt ist.

1.4 Trennungskontrolle

- Mandantentrennung auf Datenbank-Ebene: Daten verschiedener Auftraggeber (Winzer-Shops) werden logisch durch Tenant-Identifier getrennt und sind durch entsprechende Anwendungslogik gegen unbefugten Cross-Tenant-Zugriff geschützt;
- Trennung zwischen Produktions- und Testdaten.

1.5 Pseudonymisierung und Verschlüsselung

- Verschlüsselung der Datenübertragung: Sämtliche Datenübertragungen über das Internet erfolgen ausschließlich über verschlüsselte Verbindungen (TLS 1.2 oder höher);
- Verschlüsselung im Ruhezustand (Encryption at Rest): Datenbanken und Datei-Speicher werden mit den vom jeweiligen Sub-Dienstleister bereitgestellten Standard-Verschlüsselungsmechanismen geschützt (insbesondere Neon-Datenbank-Verschlüsselung im Standard-Konfigurationsumfang, Vercel Blob Storage Standard-Verschlüsselung);
- Sensitive Tokens (z. B. OAuth-Refresh-Tokens) werden verschlüsselt gespeichert.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Eingabekontrolle

- Server-Logs durch Vercel mit Erfassung von IP-Adressen und Zeitstempeln zur Nachvollziehbarkeit von Zugriffen auf die Plattform.

2.2 Weitergabekontrolle

- Datenübertragungen an Sub-Dienstleister erfolgen ausschließlich über verschlüsselte API-Verbindungen (HTTPS/TLS);
- Mit allen eingesetzten Sub-Dienstleistern bestehen Auftragsverarbeitungsverträge bzw. gleichwertige vertragliche Garantien;
- Bei Drittlandtransfers werden EU-Standardvertragsklauseln (SCCs) und/oder die Selbstzertifizierung unter dem EU-US Data Privacy Framework eingesetzt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

- Hosting der Plattform über Vercel mit redundanter, weltweit verteilter Infrastruktur;
- Datenbank-Hosting über Neon mit automatischen Backup-Mechanismen im Standard-Konfigurationsumfang;
- Background-Job-Verarbeitung über Inngest mit Retry-Mechanismen.

3.2 Wiederherstellbarkeit

- Tägliche automatische Datenbank-Backups durch den Datenbank-Sub-Dienstleister Neon im Standard-Konfigurationsumfang.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Auftragskontrolle: Sub-Dienstleister werden vor Beauftragung auf datenschutzrechtliche Eignung geprüft (insbesondere Vorhandensein eines AVV bzw. SCCs, Verarbeitungsorte, Zertifizierungen);
- Verpflichtung der Mitarbeiter auf Vertraulichkeit und Datenschutz in schriftlicher oder elektronischer Form;
- Sensibilisierung der Mitarbeiter für Datenschutzthemen.

5. Hinweise zum aktuellen Stand der Maßnahmen

Der Auftragnehmer arbeitet an der kontinuierlichen Weiterentwicklung der technisch-organisatorischen Maßnahmen. Insbesondere sind folgende Maßnahmen geplant oder befinden sich in Umsetzung:

- Einführung einer Zwei-Faktor-Authentifizierung für das Vinolin-Dashboard;
- Erweiterung des Loggings auf Anwendungsebene zur Nachvollziehbarkeit von Zugriffen auf personenbezogene Daten;
- Erstellung eines dokumentierten Sicherheits- und Notfallkonzepts;
- Durchführung regelmäßiger Penetrationstests durch externe Anbieter.

Bei wesentlichen Änderungen der eingesetzten technisch-organisatorischen Maßnahmen wird der Auftragnehmer den Auftraggeber gemäß § 2 Abs. 2 dieses Vertrags informieren.

Anlage 3: Genehmigte Unterauftragsverhältnisse

#	Firma	Anschrift	Leistung, Zweck	Verarbeitungsort	Garantien bei Drittlandtransfer
1	Vercel Inc.	340 S Lemon Ave #4133, Walnut, CA 91789, USA	Web-Hosting, Content Delivery Network (CDN), Blob Storage, Analytics, AI Gateway	USA (mit globaler CDN-Verteilung)	EU-Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO; Selbstzertifizierung unter dem EU-US Data Privacy Framework
2	Neon Inc.	209 Avenida Del Mar, Suite C #2275, San Clemente, CA 92672, USA	Datenbank-Hosting (PostgreSQL)	Frankfurt am Main, Deutschland (Datenverarbeitungsort)	EU-Standardvertragsklauseln (SCCs); Selbstzertifizierung unter dem EU-US Data Privacy Framework
3	Google Ireland Ltd.	Gordon House, Barrow Street, Dublin 4, D04 E5W5, Irland	KI-Funktionen (Vertex AI), Maps, OAuth (Sign in with Google), Bot-Schutz (reCAPTCHA)	Frankfurt am Main, Deutschland (für Vertex AI) bzw. innerhalb der EU; Subprozessoren ggf. in Drittländern	EU-Verarbeitung durch Hauptdienstleister; bei Subprozessoren in Drittländern EU-Standardvertragsklauseln
4	Stripe Payments Europe Ltd.	1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland	Zahlungsabwicklung (Kreditkarte, SEPA, etc.)	EU (Irland)	EU-Verarbeitung
5	PayPal (Europe) S.à r.l. et Cie, S.C.A.	22-24 Boulevard Royal, L-2449 Luxembourg, Luxemburg	Zahlungsabwicklung (PayPal)	EU (Luxemburg)	EU-Verarbeitung
6	Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg, Luxemburg	Versand von Transaktions-E-Mails (Amazon SES)	Frankfurt am Main, Deutschland	EU-Verarbeitung
7	Inngest, Inc.	2261 Market Street #4257, San Francisco, CA 94114, USA	Background-Job-Verarbeitung (asynchrone Tasks, Cron-Jobs)	USA	EU-Standardvertragsklauseln (SCCs); Selbstzertifizierung unter dem EU-US Data Privacy Framework
8	Apple Distribution International Ltd.	Hollyhill Industrial Estate, Hollyhill, Cork, Irland	Authentifizierung (Sign in with Apple)	EU (Irland)	EU-Verarbeitung

Anlage 4: Beitrittserklärung

Diese Anlage findet Anwendung, sofern Verantwortliche oder Auftragsverarbeiter, die nicht ursprünglich Partei dieses Vertrags sind, dem Vertrag gemäß § 10 beitreten möchten.

Firma bzw. Geschäftsbezeichnung der Partei:	
Anschrift:	
Registerdaten:	
Ort und Datum:	
Name des/der Unterzeichner(s):	
Unterschrift(en) bzw. elektronische Bestätigung:	

Die beitretende Partei erklärt ihren Beitritt in folgender Rolle:

Verantwortlicher:	☐
Auftragnehmer (Unterauftragnehmer):	☐

Stand: 30. April 2026