

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO · Version 1.1

1. Vertragsparteien

Verantwortlicher („Auftraggeber“): der Kunde, der einen Tarif von nootiz nutzt.

Auftragsverarbeiter („Auftragnehmer“): hantha GmbH, Dick 48/B, 39058 Sarntal / Sarnthein, Südtirol – Italien, UID IT03231400213, E-Mail info@nootiz.com, Betreiber der Software nootiz (app.nootiz.com).

Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus dem Hauptvertrag (AGB/Nutzungsvertrag nootiz). Er wird in elektronischer Form gemäß Art. 28 Abs. 9 DSGVO geschlossen und gilt mit Registrierung bzw. Abschluss eines Tarifs als vereinbart. Einer Unterschrift bedarf es nicht.

2. Gegenstand, Dauer, Art und Zweck

Gegenstand ist die Bereitstellung der SaaS-Lösung nootiz zur Erfassung, Verwaltung und Bearbeitung von visuellem Website-Feedback. Die Dauer entspricht der Laufzeit des Hauptvertrags.

Art der Daten: Kontakt- und Kontodaten (Name, E-Mail, Rolle), Feedback-Inhalte (Kommentare, Screenshots, Anhänge, URL, Browser- und Geräteinformationen), Projekt- und Nutzungsdaten, Protokolldaten.

Betroffene Personen: Nutzer:innen des Auftraggebers, deren Kund:innen, Projektbeteiligte und eingeladene Gäste; ggf. Personen, die auf Screenshots erkennbar sind.

Zweck: ausschließlich die Erbringung der vertraglich vereinbarten Leistungen.

3. Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf Übermittlungen in Drittländer, sofern er nicht durch Unionsrecht oder das Recht eines Mitgliedstaats dazu verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO). Die Weisungen ergeben sich aus diesem Vertrag, dem Hauptvertrag und den Einstellungen in der Software. Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich.

4. Vertraulichkeit

Alle zur Verarbeitung befugten Personen sind zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO).

5. Sicherheit der Verarbeitung

Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Er darf sie an den technischen Fortschritt anpassen, sofern das Schutzniveau nicht unterschritten wird.

6. Unterauftragsverarbeiter

Der Auftraggeber genehmigt allgemein den Einsatz der in Anlage 2 genannten Unterauftragsverarbeiter. Der Auftragnehmer informiert den Auftraggeber vorab per E-Mail oder in der Software über beabsichtigte Änderungen. Der Auftraggeber kann innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt keine Einigung, kann er den Hauptvertrag außerordentlich kündigen.

Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf (Art. 28 Abs. 4 DSGVO).

7. Übermittlung in Drittländer

Erfolgt eine Verarbeitung außerhalb des EWR, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das geschieht insbesondere über einen Angemessenheitsbeschluss (EU-US Data Privacy Framework für zertifizierte Anbieter) oder über die EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914), ggf. mit ergänzenden Maßnahmen.

8. Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Maßnahmen bei der Erfüllung der Betroffenenrechte (Art. 12–23 DSGVO) sowie bei den Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung, Datenschutz–Folgenabschätzung, vorherige Konsultation). Anfragen Betroffener, die direkt beim Auftragnehmer eingehen, leitet er unverzüglich weiter.

9. Meldung von Datenschutzverletzungen

Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis. Die Meldung enthält die Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar.

10. Löschung und Rückgabe

Projektende: Projekte können vom Auftraggeber archiviert, aber nicht gelöscht werden. Archivierte Projekte bleiben bis zum Vertragsende gespeichert. Auf Anforderung per E-Mail an info@nootiz.com löscht der Auftragnehmer einzelne Projekte (Feedback, Screenshots, Anhänge, Kommentare) innerhalb von 30 Tagen endgültig.

Kündigung oder Vertragsende: Der Auftraggeber kann seine Daten noch 30 Tage nach Vertragsende exportieren. Danach löscht der Auftragnehmer alle personenbezogenen Daten des Kontos endgültig, sofern keine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g DSGVO). Auf Wunsch gibt er die Daten vorher zurück.

Sicherungskopien: Gelöschte Daten werden spätestens 30 Tage nach der Löschung automatisch aus den Backups entfernt. Bis dahin sind sie gegen Zugriff geschützt und werden nicht weiterverarbeitet.

Ausnahme: Rechnungs- und Abrechnungsdaten werden für die Dauer gesetzlicher Aufbewahrungspflichten (z. B. 10 Jahre steuerrechtlich) aufbewahrt.

Auf Wunsch bestätigt der Auftragnehmer die Löschung schriftlich per E-Mail.

11. Nachweise und Kontrollen

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung dieser Pflichten zur Verfügung. Er ermöglicht Überprüfungen und Inspektionen nach angemessener Vorankündigung zu den üblichen Geschäftszeiten und trägt dazu bei (Art. 28 Abs. 3 lit. h DSGVO). Vorrangig erfolgt der Nachweis durch Selbstauskunft, Dokumentation oder Zertifikate der Unterauftragsverarbeiter.

12. Haftung und Schlussbestimmungen

Die Haftung richtet sich nach Art. 82 DSGVO und im Übrigen nach dem Hauptvertrag. Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in datenschutzrechtlichen Fragen vor. Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. Es gilt das Recht des Sitzstaats des Auftragnehmers unter Vorrang der DSGVO.

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Vertraulichkeit: Verschlüsselte Übertragung (TLS/HTTPS) für alle Verbindungen. Verschlüsselung gespeicherter Daten (at rest) bei den Hosting- und Datenbankanbietern. Rollen- und rechtebasierter Zugriff, Zugriff nur für befugtes Personal nach dem Need-to-know-Prinzip. Passwörter werden ausschließlich gehasht gespeichert. Mandantentrennung auf Projekt- und Kontoebene.

Integrität: Protokollierung administrativer Zugriffe. Eingabevalidierung. Änderungen am Code nur über versionierte, nachvollziehbare Deployments.

Verfügbarkeit und Belastbarkeit: Betrieb in professionellen Rechenzentren mit redundanter Infrastruktur. Regelmäßige automatische Datensicherungen. Überwachung der Verfügbarkeit.

Wiederherstellbarkeit: Wiederherstellung aus Sicherungen ist dokumentiert und wird getestet.

Überprüfung und Bewertung: Regelmäßige Überprüfung der Maßnahmen, Sicherheitsupdates von Abhängigkeiten, sorgfältige Auswahl und Kontrolle der Unterauftragsverarbeiter.

Anlage 2 – Unterauftragsverarbeiter

Anbieter	Leistung	Ort / Garantie
Vercel Inc., San Francisco, USA	Hosting der Anwendung app.nootiz.com	EU-Region nach Konfiguration; EU-US Data Privacy Framework, EU-Standardvertragsklauseln
MongoDB, Inc. (Atlas), New York, USA	Datenbank-Hosting	EU-Region nach Konfiguration; EU-US Data Privacy Framework, EU-Standardvertragsklauseln
Resend (Plus Five Five, Inc.), USA	Versand von System-E-Mails	EU-US Data Privacy Framework, EU-Standardvertragsklauseln

Hinweis: Die Zahlungsabwicklung erfolgt über Stripe (Stripe Payments Europe, Ltd., Dublin, Irland). Stripe verarbeitet Zahlungsdaten als eigenständiger Verantwortlicher und ist daher kein Unterauftragsverarbeiter im Sinne dieses Vertrags.

Fragen zu diesem Vertrag: info@nootiz.com