Meistify

Auftragsverarbeitungsvertrag (AVV)

Anlage zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO

Basierend auf der Bitkom-Mustervertragsanlage Version 1.3 (2025)

Stand: August 2026 — Version 2.1

Zwischen

dem Auftraggeber (Nutzer der Meistify-Plattform)
– nachfolgend „Auftraggeber“ –

und

Meistify GmbH
Billy-Wilder-Promenade 47, 14167 Berlin
– nachfolgend „Auftragnehmer“ –

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Nutzung der SaaS-Plattform Meistify (nachfolgend „Plattform“) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

Sie findet Anwendung auf alle Tätigkeiten, die mit dem Nutzungsvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten („Daten“) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Gegenstand der Auftragsverarbeitung ist die Bereitstellung der SaaS-Plattform Meistify für Handwerksbetriebe. Die Plattform umfasst folgende Funktionsbereiche: Kundenverwaltung, Baustellenverwaltung, Auftragsverwaltung, Kostenvoranschläge, Rechnungsstellung, Zeiterfassung, Mitarbeiterverwaltung, Kalender & Disposition, digitale Abnahmeprotokolle sowie Dokumentenmanagement.

(2) Im Einzelnen sind folgende Daten Bestandteil der Datenverarbeitung:

Art der Daten	Art und Zweck der Datenverarbeitung	Kategorien betroffener Personen
Vor- und Nachname, Adressdaten, E-Mail-Adressen, Telefonnummern	Verwaltung von Kundenstammdaten, Angebots- und Rechnungserstellung, Kommunikation	Kunden des Auftraggebers, Ansprechpartner bei Geschäftspartnern
Vor- und Nachname, E-Mail-Adresse, Telefonnummer, Arbeitszeiten, Stundensätze	Mitarbeiterverwaltung, Zeiterfassung, Auftragsplanung, Lohn-/Kostenberechnung	Mitarbeiter des Auftraggebers
Bankverbindungsdaten (IBAN/BIC), Steuerliche Identifikationsnummern (USt-IdNr., Steuernummer)	Rechnungsstellung, DATEV-Export, ZUGFeRD/XRechnung E-Invoicing	Auftraggeber (Unternehmensdaten)
Digitale Unterschriften, Fotos, Standortdaten	Digitale Abnahmeprotokolle, Baustellendokumentation	Kunden und Mitarbeiter des Auftraggebers
Login-Daten (E-Mail, Passwort-Hash), IP-Adressen, Session-Daten	Authentifizierung, Zugriffskontrolle, Sicherheitsprotokollierung	Alle Nutzer der Plattform
Audio-/Sprachdaten, Transkriptionen, KI-Input und KI-Output (sofern KI-Funktionen genutzt werden)	Spracherkennung, Sprachbefehle, Erstellung automatisierter Inhalte, Auswertung durch KI-gestützte Funktionen	Nutzer der Plattform, Endkunden des Auftraggebers

Bei aktiver Nutzung von KI-Funktionen liegt es in der Verantwortung des Auftraggebers sicherzustellen, dass keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) sowie keine Geschäfts- oder Betriebsgeheimnisse Dritter über die KI-Eingabefelder verarbeitet werden.

(3) Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Nutzungsvertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben. Eine isolierte Beendigung dieser Anlage ist ausgeschlossen.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Nutzungsvertrag und in der Leistungsbeschreibung konkretisiert sind. 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 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Nutzungsvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die in diesem Vertrag dokumentierten Weisungen sind grundsätzlich abschließend. Ergänzende Einzelweisungen, die über den Inhalt dieses Vertrages hinausgehen oder zusätzliche Anforderungen stellen, bedürfen der Zustimmung des Auftragnehmers; sie werden als Antrag auf Leistungsänderung behandelt. Die hierdurch entstehenden angemessenen Mehrkosten beim Auftragnehmer gehen zu Lasten des Auftraggebers. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. 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.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die aktuellen technischen und organisatorischen Maßnahmen sind in Anlage 1 zu diesem Vertrag dargelegt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

Mobile Arbeit / Homeoffice: Eine Verarbeitung personenbezogener Daten durch Beschäftigte des Auftragnehmers im Rahmen mobiler Arbeit, von Telearbeitsplätzen oder im

Homeoffice ist zulässig, sofern der Auftragnehmer durch geeignete technische und organisatorische Maßnahmen sicherstellt, dass das in Anlage 1 vereinbarte Schutzniveau auch an diesen Arbeitsplätzen eingehalten wird (insbesondere durch verschlüsselte Verbindungen, Bildschirmsperre, Verbot der lokalen Datenspeicherung sowie schriftliche Verpflichtung der Beschäftigten auf die Vertraulichkeit). Eine separate Zustimmung des Auftraggebers ist hierfür nicht erforderlich.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Die Meldung erfolgt unverzüglich nach Kenntniserlangung, in der Regel innerhalb von 48 Stunden, an die vom Auftraggeber hinterlegte E-Mail-Adresse. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Datenschutzbeauftragter und Ansprechpartner: Beim Auftragnehmer ist derzeit kein Datenschutzbeauftragter im Sinne der Art. 37 ff. DSGVO bestellt, da die gesetzlichen Voraussetzungen für eine Bestellpflicht nicht vorliegen. Ansprechpartner für sämtliche im Rahmen dieses Vertrages anfallenden Datenschutzfragen ist erreichbar unter datenschutz@meistify.com. Sollte zu einem späteren Zeitpunkt ein Datenschutzbeauftragter bestellt werden, wird der Auftragnehmer den Auftraggeber hierüber unverzüglich informieren.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Die Löschung erfolgt automatisch innerhalb von 30 Tagen nach Vertragsende, sofern der Auftraggeber nicht vorher eine Herausgabe verlangt. Macht der Auftraggeber nicht rechtzeitig vor Vertragsende von seinem Wahlrecht Gebrauch, ist der Auftragnehmer berechtigt, nach Ablauf von 30 Tagen die Auftraggeberdaten zu löschen. Steuerrelevante Daten (insbesondere finalisierte Rechnungen) werden gemäß § 147 AO / § 257 HGB für die gesetzliche Aufbewahrungsfrist von 10 Jahren in anonymisierter Form aufbewahrt.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(11) Aufsichtsbehördliche Maßnahmen: Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen, Maßnahmen oder Anfragen einer

Datenschutzaufsichtsbehörde oder einer sonstigen hoheitlichen Aufsichtsbehörde, soweit diese die für den Auftraggeber verarbeiteten Daten betreffen — es sei denn, eine solche Information ist dem Auftragnehmer gesetzlich oder behördlich untersagt.

(12) Anonymisierung: Der Auftragnehmer ist berechtigt, im Rahmen der Auftragsverarbeitung erlangte Daten in vollständig anonymisierter und/oder aggregierter Form — bei der eine Re-Identifikation einzelner natürlicher Personen oder einzelner Auftraggeber-Unternehmen ausgeschlossen ist — zu eigenen Zwecken zu nutzen, insbesondere zur Fehleranalyse, zur Weiterentwicklung der Plattform sowie zur Erstellung von Branchen-Benchmarks. Die Anonymisierung selbst ist eine Verarbeitungstätigkeit im Auftrag; das Ergebnis der Anonymisierung unterliegt nicht mehr der DSGVO und damit auch nicht mehr diesem Vertrag.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(2) Der Auftragnehmer stellt dem Auftraggeber folgende Funktionen zur eigenständigen Wahrnehmung der Betroffenenrechte innerhalb der Plattform zur Verfügung: Datenexport (Art. 15 DSGVO) als ZIP-Datei mit allen personenbezogenen Daten, Kunden-Anonymisierung (Art. 17 DSGVO) mit Smart-Delete-Logik, Mitarbeiter-Anonymisierung (Art. 17 DSGVO) mit automatischer Referenzprüfung, Account-Löschung (Art. 17 DSGVO) mit 30-Tage-Frist und automatischer Durchführung.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmer dem Auftraggeber folgende Informationen vorlegen: Durchführung eines Selbstaudits, Audit-Logs der Plattform (GoBD-konform, append-only), Dokumentation der technischen und organisatorischen Maßnahmen.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von mindestens 14 Kalendertagen durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt. Über die jährliche Regelinspektion hinausgehende Kontrollen sind nach vorheriger Absprache mit dem Auftragnehmer durchzuführen und unterliegen der Erstattung der damit verbundenen angemessenen Kosten durch den Auftraggeber.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Unterauftragsverarbeiter (weitere Auftragsverarbeiter)

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung folgender Unterauftragsverarbeiter durchgeführt. Der Auftraggeber stimmt dem Einsatz der nachfolgend genannten Unterauftragsverarbeiter zu:

Unterauftragsverarbeiter	Sitz / Serverstandort	Beschreibung der Teilleistungen
Vercel Inc.	USA / EU-Region fra1 (Frankfurt)	Hosting, CDN und Auslieferung der Webanwendung. Alle Datenverarbeitung in der EU-Region Frankfurt (fra1). Zertifiziert nach EU-US Data Privacy Framework.
Supabase Inc.	USA / EU-Region (Frankfurt)	Datenbank (PostgreSQL), Authentifizierung (Auth), Dateispeicher (Storage). Alle Daten werden in der EU-Region gespeichert und verarbeitet.
Brevo (Sendinblue SAS)	Frankreich / EU	Transaktionale E-Mails (Kontobestätigung, Passwort-Reset, Systembenachrichtigungen). Server ausschließlich in der EU.

(2) Der Auftraggeber stimmt zu, dass der Auftragnehmer weitere Unterauftragsverarbeiter hinzuziehen kann. Vor Hinzuziehung oder Ersetzung der Unterauftragsverarbeiter informiert der Auftragnehmer den Auftraggeber mindestens 14 Kalendertage im Voraus. Der Auftraggeber kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichen Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist,

gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(3) Der Auftragnehmer stellt dem Auftraggeber eine aktuelle Liste aller eingesetzten Unterauftragsverarbeiter über die Plattform unter Einstellungen > Rechtliches zur Verfügung.

(4) Erteilt der Auftragnehmer Aufträge an Unterauftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Unterauftragsverarbeiter zu übertragen.

(5) Keine Unterauftragsverarbeitung bei Nebenleistungen: Ein Unterauftragsverhältnis im Sinne dieses Vertrages liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Hierzu gehören insbesondere Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zur vertragsgegenständlichen Leistung, Bewachungsdienste sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der Hard- und Software ohne konkreten Datenbezug. Der Auftragnehmer wird auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

§ 8 Übermittlung in Drittstaaten

(1) Eine Verarbeitung personenbezogener Daten in einem Drittland außerhalb der EU/des EWR erfolgt nur unter Beachtung der Voraussetzungen der Art. 44 ff. DS-GVO und auf dokumentierte Weisung des Auftraggebers.

(2) Soweit der Auftragnehmer Unterauftragsverarbeiter mit Sitz in den USA einsetzt (Vercel Inc., Supabase Inc.), gilt Folgendes: Die Datenverarbeitung erfolgt ausschließlich in EU-Rechenzentren (Frankfurt, fra1). Die US-Unternehmen sind nach dem EU-US Data Privacy Framework (DPF) zertifiziert. Zusätzlich bestehen Standarddatenschutzklauseln (SCC) gemäß Art. 46 Abs. 2 lit. c DS-GVO. Ein Transfer Impact Assessment (TIA) wurde durchgeführt und wird dem Auftraggeber auf Anfrage zur Verfügung gestellt.

(3) Eine Drittlandsverarbeitung durch den Auftragnehmer oder dessen Unterauftragsverarbeiter ist nur mit vorheriger Zustimmung des Auftraggebers zulässig, sofern nichts anderes vereinbart wurde.

§ 9 Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

(2) Im Verhältnis der Vertragsparteien zueinander gelten für die Haftung des Auftragnehmers nach diesem AVV ergänzend die im Nutzungsvertrag (AGB) vereinbarten Haftungsausschlüsse und -beschränkungen, insbesondere die dortigen Regelungen zu Haftungs-Cap, Kardinalpflichten und Datenverlust.

(3) Freistellung: Sollten Dritte gegen den Auftragnehmer Ansprüche geltend machen, die darauf beruhen, dass der Auftraggeber schuldhaft gegen diesen AVV oder eine ihn als Verantwortlichen treffende datenschutzrechtliche Verpflichtung verstoßen hat, stellt der

Auftraggeber den Auftragnehmer auf erstes Anfordern von diesen Ansprüchen frei. Der Auftraggeber verpflichtet sich darüber hinaus, den Auftragnehmer auf erstes Anfordern von solchen Geldbußen freizustellen, die gegen den Auftragnehmer verhängt werden, soweit diese dem Anteil des Auftraggebers an dem mit der Geldbuße sanktionierten Verstoß entsprechen.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Nutzungsvertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DS-GVO)

Der Auftragnehmer hat folgende technische und organisatorische Maßnahmen getroffen, die dem aktuellen Stand der Technik entsprechen und ein dem Risiko angemessenes Schutzniveau gewährleisten:

1. Vertraulichkeit

Zutrittskontrolle: Hosting in professionellen Rechenzentren von Vercel und Supabase (Frankfurt, EU) mit physischer Zutrittskontrolle, Videoüberwachung und Zugangsprotokollierung.

Zugangskontrolle: Authentifizierung über Supabase Auth mit gehashten Passwörtern (bcrypt). Erzwungene Passwortkomplexität. Session-basierte Zugriffskontrolle.

Zugriffskontrolle: Row Level Security (RLS) auf Datenbankebene. Mandantentrennung über organization_id auf allen Tabellen. Rollenbasiertes Berechtigungssystem (Admin, Meister, Office, Geselle) mit unterschiedlichen Zugriffsrechten.

Trennungskontrolle: Logische Trennung aller Mandantendaten über organization_id. Kein mandantenübergreifender Datenzugriff möglich. Trennung von Produktiv- und Testsystem.

Pseudonymisierung: Anonymisierungsfunktionen für Kunden- und Mitarbeiterdaten (Smart Delete). Personenbezogene Daten werden bei Löschungsanfragen durch Platzhalter ersetzt, während steuerrelevante Daten erhalten bleiben.

2. Integrität

Weitergabekontrolle: Verschlüsselung aller Datenübertragungen mit TLS 1.3. HTTPS erzwungen auf allen Endpunkten. Keine unverschlüsselte Datenübertragung.

Eingabekontrolle: Lückenlose Protokollierung aller schreibenden Zugriffe über Audit-Log (GoBD-konform, append-only). Nachvollziehbarkeit aller Datenänderungen mit Zeitstempel, Akteur und betroffener Ressource.

3. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Hosting auf Vercel Edge Network mit automatischer Skalierung und Geo-Redundanz in der EU-Region. Supabase PostgreSQL mit automatischen Backups und Point-in-Time Recovery.

Belastbarkeit: Automatische Skalierung der Anwendungsinfrastruktur bei Lastspitzen. Serverless Architecture ohne Single Points of Failure.

Wiederherstellbarkeit: Automatische tägliche Backups der Datenbank durch Supabase. Recovery Point Objective (RPO) < 24 Stunden. Recovery Time Objective (RTO) < 8 Stunden bei kritischen Ausfällen. Point-in-Time-Recovery für die letzten 7 Tage.

4. Verfahren zur regelmäßigen Überprüfung

Datenschutz-Management: Integrierter AVV mit Versionierung und elektronischer Akzeptierung. DSGVO-konforme Datenexport-Funktion (Art. 15). Automatische Account-Löschung nach 30-Tage-Frist (Art. 17).

Incident-Management: Automatische Benachrichtigung bei Datenschutzvorfällen. Definierter Meldeprozess an Auftraggeber innerhalb von 48 Stunden.

Auftrags- und Weisungskontrolle: Schriftliche Dokumentation aller Weisungen. Audit-Log für alle administrativen Aktionen.

Mitarbeiterschulung und -verpflichtung: Schriftliche Verpflichtung aller Mitarbeiter und Auftragnehmer auf Vertraulichkeit und das Datengeheimnis vor Aufnahme der Tätigkeit. Regelmäßige Schulungen zu Datenschutz und Informationssicherheit (mindestens jährlich oder anlassbezogen).

Regelmäßige TOM-Überprüfung: Die hier dokumentierten technischen und organisatorischen Maßnahmen werden mindestens einmal jährlich sowie anlassbezogen auf Wirksamkeit überprüft, evaluiert und bei Bedarf angepasst (Art. 32 Abs. 1 lit. d DSGVO).