# VERTRAG ÜBER DIE AUFTRAGSVERARBEITUNG (AVV)

gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO) unter besonderer Berücksichtigung von Geschäfts- und Kalkulationsgeheimnissen (§§ 2, 4, 23 GeschGehG) sowie Vertraulichkeit im Vergabeverfahren (§ 5 VgV)

**1. AUFTRAGGEBER (VERANTWORTLICHER)**

Unternehmen

_____

Anschrift

_____

_____

Vertreten durch / Kontakt

_____

E-Mail & Telefon

_____

**2. AUFTRAGNEHMER (AUFTRAGSVERARBEITER)**

Anbieter

**be.smart · Inhaber Sebastian Hammer**

Anschrift

Traminerweg 5, 68309 Mannheim, Deutschland

Kontakt & USt-IdNr.

E-Mail: info@be-smart-business.de

Tel.: +49 175 836 8824 · USt-IdNr.: DE313900155

Plattform & Datum

Tendermeister (tendermeister.com) · Stand: 17.11.2026

## Präambel

Dieser Vertrag über die Auftragsverarbeitung (nachfolgend „AVV") konkretisiert die datenschutz- und geheimnisschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Nutzung der webbasierten Vergabe- und Angebotsplattform „Tendermeister" auf Grundlage des zwischen den Parteien geschlossenen Hauptvertrags (AGB oder individuelles Unternehmensangebot) ergeben.

Im Rahmen der Vergaberecherche, der Analyse von Ausschreibungsunterlagen, der Kalkulation von Leistungsverzeichnissen (GAEB, PDF, Excel/CSV) sowie der Vorbereitung von Angebotsunterlagen verarbeitet der Auftragnehmer als Auftragsverarbeiter im Auftrag des Auftraggebers (Verantwortlicher) personenbezogene Daten gemäß Art. 4 Nr. 2 DSGVO sowie hochvertrauliche Angebots-, Preis- und Kalkulationsinformationen (§ 2 Nr. 1 GeschGehG, § 5 VgV). Die Parteien schließen hierzu nachfolgenden AVV gemäß Art. 28 Abs. 3 DSGVO.

## § 1 Gegenstand, Geltungsbereich und Dauer der Verarbeitung

(1) Gegenstand: Der Auftragsverarbeiter stellt dem Verantwortlichen die webbasierte SaaS-Plattform „Tendermeister" zur Verfügung. Die Auftragsverarbeitung umfasst insbesondere das mandantenisolierte Hosting von Ausschreibungsunterlagen, Leistungsverzeichnissen (GAEB, PDF, Excel/CSV), Referenzkatalogen und Unternehmensnachweisen, deren Strukturierung und KI-gestützte Auswertung (u. a. KO-Kriterien-, Risiko- und Vorbemerkungsanalyse, LV-Positionsextraktion, unternehmensinterne Preiskalkulationshilfe) sowie die Erstellung von Angebotsentwürfen und Exportdateien (X84/D84/.xlsx) gemäß Hauptvertrag.

(2) Geltungsbereich: Dieser AVV findet Anwendung auf sämtliche Verarbeitungen personenbezogener Daten, die der Auftragsverarbeiter im Auftrag und nach Weisung des Verantwortlichen im Zusammenhang mit der Nutzung von Tendermeister durchführt.

(3) Dauer: Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrags. Eine wirksame Beendigung oder Kündigung des Hauptvertrags beendet zugleich diesen AVV, unbeschadet fortgeltender Lösch-, Rückgabe- und Geheimhaltungspflichten sowie des Rechts zur außerordentlichen Kündigung aus wichtigem Grund.

## § 2 Art und Zweck der Verarbeitung, Kategorien betroffener Personen und Arten personenbezogener Daten

(1) Art und Zweck der Verarbeitung: Erheben, Erfassen, Organisation, Ordnen, persistente Speicherung im mandantenisolierten Workspace, Auslesen, Strukturierung, KI-gestützte Analyse und Textgenerierung, Export sowie Löschung von Daten mittels automatisierter Cloud-Verfahren zum Zweck der effizienten Bearbeitung öffentlicher und privater Ausschreibungen durch das Unternehmen des Verantwortlichen.

(2) Kategorien betroffener Personen:

- Beschäftigte, Projektleiter, Kalkulatoren, Einkäufer und gesetzliche Vertreter des Verantwortlichen
- Ansprechpartner, Sachbearbeiter und Vergabestellen-Mitarbeitende aufseiten öffentlicher und privater Auftraggeber
- Ansprechpartner, Bauleiter und Fachkräfte von Nachunternehmern, Bietergemeinschaftspartnern und Lieferanten, soweit vom Verantwortlichen in Unterlagen oder Referenzen erfasst

(3) Arten personenbezogener Daten:
• Account-, Stammdaten und Kontaktdaten (Name, geschäftliche E-Mail-Adresse, Telefonnummer, Firmenanschrift, Funktion)
• Projekt-, Ausschreibungs- und Vertragsdaten (Vergabestellen-Kontakte, Referenzprojekte, Eignungs- und Qualifikationsnachweise, Lebensläufe bzw. Personalqualifikationen soweit in Bieterunterlagen enthalten)
• Angebots-, Kalkulations- und Ergebnisdaten (Einheitspreise, Referenzkataloge, Submissionsrang, Bieterabstände, Notizen)
• Technische Authentifizierungs-, Sicherheits- und Protokolldaten (Firebase User-ID, Zeitstempel, Änderungsprotokolle)

## § 3 Rechte, Pflichten und Weisungsbefugnis des Verantwortlichen

(1) Rechtmäßigkeit und Weisungen: Der Verantwortliche ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Übermittlung der personenbezogenen Daten an den Auftragsverarbeiter sowie für die Wahrung der Betroffenenrechte verantwortlich. Weisungen werden über die Konfiguration der Plattform oder in Textform (z. B. per E-Mail an info@be-smart-business.de) erteilt; mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(2) Prüf- und Hinweispflicht (Art. 28 Abs. 3 UAbs. 2 DSGVO): Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung des Verantwortlichen gegen die DSGVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist berechtigt, die Ausführung der betreffenden Weisung auszusetzen, bis sie vom Verantwortlichen bestätigt oder geändert wird.

(3) Mitwirkung des Verantwortlichen: Der Verantwortliche teilt dem Auftragsverarbeiter unverzüglich mit, wenn er bei der Prüfung von Verarbeitungsergebnissen Fehler oder Unregelmäßigkeiten feststellt.

(4) RDG- und Kalkulations-Klarstellung: KI-gestützte Risiko- und Vergabehinweise (z. B. zu Vorbemerkungen, ZVB/BVB, KO-Kriterien oder Rügefristen) sowie Preisvorschläge aus dem eigenen historischen Referenzkatalog des Verantwortlichen sind rein technische Hilfsmittel. Sie ersetzen weder eine Rechtsberatung nach dem Rechtsdienstleistungsgesetz (RDG) noch die eigenverantwortliche technische, vergaberechtliche und kaufmännische Prüfung vor Angebotsabgabe durch den Verantwortlichen.

## § 4 Pflichten des Auftragnehmers, Schutz von Kalkulationsgeheimnissen (§ 2 GeschGehG) & Ausschluss von KI-Training

(1) Weisungsgebundenheit: Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf die Übermittlung in ein Drittland, sofern er nicht durch Unionsrecht oder das Recht eines Mitgliedstaats hierzu verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO).

(2) Vertraulichkeit, Datengeheimnis & Schutz von Geschäfts- und Kalkulationsgeheimnissen (§ 53 BDSG, §§ 2, 4, 23 GeschGehG, § 5 VgV): Der Auftragsverarbeiter verpflichtet sich, sämtliche vom Verantwortlichen hochgeladenen Ausschreibungsunterlagen, Leistungsverzeichnisse, Einheitspreise, Margen, Nachunternehmerkonditionen und Angebotsentwürfe als vertrauliche Geschäftsgeheimnisse (§ 2 Nr. 1 GeschGehG) im Sinne der vergaberechtlichen Vertraulichkeit (§ 5 VgV) zu behandeln. Alle mit der Datenverarbeitung betrauten Mitarbeitenden und Erfüllungsgehilfen werden vor Aufnahme ihrer Tätigkeit schriftlich auf die Vertraulichkeit, das Datengeheimnis (§ 53 BDSG, Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO) und den Schutz von Geschäftsgeheimnissen (§§ 2, 4, 23 GeschGehG) nach dem Need-to-know-Prinzip verpflichtet (Muster in Anlage 3). Diese Verpflichtung gilt über das Ende des Vertrags- und Beschäftigungsverhältnisses hinaus fort.

(3) Verbindliche Zero-Training- & Zero-Cross-Tenant-Garantie: Weder der Auftragsverarbeiter (be.smart) noch Google Cloud Vertex AI nutzen Kundendaten, Ausschreibungsunterlagen, Leistungsverzeichnisse, Einheitspreise oder Kalkulationen des Verantwortlichen zum Training, zum Fine-Tuning oder zur Weiterentwicklung von KI-Modellen — auch nicht in anonymisierter, pseudonymisierter oder aggregierter Form. Historische Einheitspreise und Referenzkataloge des Verantwortlichen werden strikt mandantenisoliert je Kunden-Workspace (companyId samt der durch den Auftraggeber ausdrücklich autorisierten Team-Mitglieder über company_members und den workspaceCompanyId-Token-Claim) verarbeitet und fließen niemals in Preisvorschläge, Benchmarks oder Auswertungen fremder Kunden-Tenants ein.

(4) Speicher- und Privacy-Architektur (Code-Wahrheit): Tendermeister speichert Ausschreibungen, Leistungsverzeichnisse und Referenzkataloge persistent im mandantenisolierten Workspace des Verantwortlichen (TLS 1.3 in transit, AES-256 at rest, serverseitige Bearer-Token- und Firestore-Rules-Isolation) bis zur aktiven Löschung durch den Verantwortlichen. Im Tarif „Tendermeister Ultra“ steht dem Verantwortlichen zusätzlich ein optionales clientseitiges Schwärzungsmodul (BidSecretPreviewModal) zur Verfügung, mit dem sensible Bieterangaben (z. B. Firmennamen, IBAN, USt-IdNr., E-Mail, Telefonnummern und Margen) vor einer KI-Analyse lokal im Browser durch Platzhalter ersetzt werden können.

## § 5 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

(1) Der Auftragsverarbeiter gewährleistet ein dem Risiko angemessenes Schutzniveau nach Art. 32 DSGVO durch Umsetzung der in Anlage 1 im Einzelnen festgelegten technischen und organisatorischen Maßnahmen (TOMs).

(2) Weiterentwicklungsklausel: Die in Anlage 1 beschriebenen Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter ist berechtigt, alternative adäquate Maßnahmen umzusetzen, sofern das vertraglich vereinbarte Sicherheitsniveau dadurch nicht unterschritten wird. Wesentliche Änderungen, die das Sicherheitsniveau betreffen könnten, werden dem Verantwortlichen vorab in Textform mitgeteilt.

## § 6 Unterauftragsverhältnisse (Art. 28 Abs. 2 & 4 DSGVO) & Europäische Datenresidenz

(1) Allgemeine Genehmigung: Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine schriftliche Genehmigung zur Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter. Keine Unterauftragsverhältnisse im Sinne dieses AVV sind Nebenleistungen wie Telekommunikations-, Post-/Transport- oder Gebäudereinigungsdienste sowie die in Anlage 2 ausdrücklich abgegrenzten eigenständigen Verantwortlichen.

(2) Europäische Datenresidenz & verifizierte EU-Regionen: Die produktive Cloud-Infrastruktur (Cloud Functions, Firestore, Cloud Storage und Firebase Authentication) wird in der Google Cloud Region europe-west1 (St. Ghislain, Belgien / EU) betrieben. Die KI-Inferenz und LV-Extraktion über Google Cloud Vertex AI (primär gemini-4-hydrogen, im Tarif Ultra optional gemini-4-carbon sowie technischer Kapazitäts-Overflow-Fallback gemini-3.8-flash innerhalb von Vertex AI EU) erfolgt ausschließlich im EU Multi-Region-Standort eu (Europäische Union) unter Google Cloud DPA und Enterprise Zero-Training-Garantie. Ein rein interner, aggregierter KPI-Tagesexport (ohne personenbezogene Ausschreibungsinhalte oder Angebotskalkulationen) läuft in europe-west3 (Frankfurt am Main, Deutschland).

(3) Weitergegebene Pflichten & Haftung: Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen schriftlichen Vertrag gemäß Art. 28 Abs. 4 DSGVO, der mindestens gleichwertige Datenschutz-, Sicherheits- und Geheimhaltungspflichten auferlegt. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Einhaltung der Pflichten durch seine Unterauftragsverarbeiter gemäß Art. 28 Abs. 4 Satz 2 DSGVO.

(4) Änderungsverfahren & Drittlandgarantien (Kapitel V DSGVO): Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage im Voraus per E-Mail oder In-App-Mitteilung über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters. Der Verantwortliche kann innerhalb von 14 Tagen nach Zugang der Mitteilung aus wichtigem datenschutzrechtlichem Grund in Textform Einspruch erheben. Lässt sich der Einspruch nicht einvernehmlich auflösen, steht dem Verantwortlichen ein außerordentliches Sonderkündigungsrecht hinsichtlich der betroffenen Leistungen zu. Soweit im Einzelfall (z. B. beim Edge-Routing über Cloudflare oder beim EU-Ingest von Sentry) eine Zugriffsmöglichkeit verbundener US-Einheiten nicht vollständig ausgeschlossen werden kann, erfolgt diese ausschließlich auf Basis eines Angemessenheitsbeschlusses nach Art. 45 DSGVO (EU-US Data Privacy Framework) sowie der EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914 nach Art. 46 Abs. 2 lit. c DSGVO) samt ergänzender technischer Schutzmaßnahmen.

**Verifizierte EU-Cloud- & KI-Datenresidenz (Tendermeister Produktivbetrieb)**

**Unterauftragsverarbeiter:** Google Cloud EMEA Limited / Google Ireland Limited (Gordon House, Barrow Street, Dublin 4, Irland)

**Leistung / Zweck:** Cloud-Infrastruktur, Authentifizierung, Datenbank, Dateispeicher & Enterprise KI-Verarbeitung (Google Cloud Platform)

- **Cloud Functions, Firestore, Cloud Storage & Firebase Auth:** europe-west1 (St. Ghislain, Belgien / Europäische Union)
- **Google Cloud Vertex AI (KI-Inferenz & LV-Extraktion):** Multi-Region eu (Europäische Union) — primär gemini-4-hydrogen, Ultra optional gemini-4-carbon, Kapazitäts-Overflow-Fallback gemini-3.8-flash innerhalb Vertex AI EU
- **Interner täglicher KPI-Export (aggregierte Betriebsmetriken):** europe-west3 (Frankfurt am Main, Deutschland) — ohne personenbezogene Ausschreibungs- oder Kalkulationsinhalte

Vertraglich abgesichert über Google Cloud Data Processing Addendum (DPA) inkl. Enterprise Zero-Training-Garantie (kein Training öffentlicher oder kundenspezifischer Basismodelle mit Eingaben oder Ausgaben).

## § 7 Rechte der betroffenen Personen und Unterstützungspflichten (Kapitel III & Art. 32–36 DSGVO)

(1) Unterstützung bei Betroffenenrechten: Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Kräften mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie Widerspruch (Art. 15–22 DSGVO).

(2) Weiterleitung direkter Anfragen: Richtet eine betroffene Person einen Antrag nach Kapitel III DSGVO unmittelbar an den Auftragsverarbeiter, leitet dieser das Ersuchen unverzüglich an den Verantwortlichen weiter und antwortet nicht eigenmächtig ohne dessen Weisung.

(3) Unterstützung bei Art. 32–36 DSGVO: Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus den Artikeln 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörde).

## § 8 Mitteilungspflichten bei Datenschutzverletzungen (Art. 33 & 34 DSGVO)

(1) Unverzügliche Meldepflicht (binnen 24 Stunden): Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten sowie schwerwiegende Störungen der Vertraulichkeit oder Integrität unverzüglich, spätestens jedoch binnen 24 Stunden nach Bekanntwerden, in Textform.

(2) Pflichtinhalte der Meldung (Art. 33 Abs. 3 DSGVO): Die Meldung umfasst mindestens folgende Angaben (soweit bereits verfügbar, andernfalls unverzüglich schrittweise nachgereicht):
1. Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, einschließlich der Kategorien und ungefähren Zahl der betroffenen Personen sowie der betroffenen Datensätze;
2. Name und Kontaktdaten einer Anlaufstelle für weitere Informationen (info@be-smart-business.de);
3. Beschreibung der wahrscheinlichen Folgen der Verletzung;
4. Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Mitwirkung: Der Auftragsverarbeiter ergreift unverzüglich angemessene Sicherungsmaßnahmen zur Eindämmung des Vorfalls und unterstützt den Verantwortlichen bei der Erfüllung etwaiger Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

## § 9 Speicherdauer, Selbstbedienungs-Export sowie Löschung und Rückgabe von Daten (Art. 17 & Art. 28 Abs. 3 lit. g DSGVO)

(1) Selbstbedienungs-Export & jederzeitige Löschung: Während der Vertragslaufzeit kann der Verantwortliche strukturierte Ergebnisse und Leistungsverzeichnisse jederzeit in den angebotenen Exportformaten (GAEB X84/D84, Excel .xlsx, Konzept-Texte) herunterladen sowie einzelne Ausschreibungen oder sein gesamtes Konto jederzeit selbstständig über die Anwendungsoberfläche löschen.

(2) Vollständige Löschung nach Vertragsende bzw. Löschanforderung: Nach Beendigung der Erbringung der Verarbeitungsleistungen oder bei Ausübung einer Kontolöschung nach Art. 17 DSGVO löscht der Auftragsverarbeiter sämtliche personenbezogenen Daten und Projektinhalte in Cloud Firestore (sämtliche mandantenbezogenen Collections und Subcollections), Google Cloud Storage (Dateipfad companies/{uid}/... sowie zugehörige Dokumentenpfade) und Firebase Authentication vollständig sowie einschließlich Replikationen und Backups innerhalb von maximal 30 Tagen. Auf Verlangen des Verantwortlichen stellt der Auftragsverarbeiter eine schriftliche Löschbestätigung aus.

(3) Gesetzliche Aufbewahrungspflichten: Von der Löschung ausgenommen bleiben ausschließlich Daten, zu deren Aufbewahrung der Auftragsverarbeiter nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland verpflichtet ist (z. B. handels- und steuerrechtliche Abrechnungsbelege gemäß § 147 AO und § 257 HGB) sowie eine minimale Sperr-/Opt-out-Dokumentation zur Durchsetzung bestehender Werbewidersprüche.

## § 10 Kontrollrechte, Haftung und Schlussbestimmungen

(1) Kontrollrechte & Zertifikatsnachweis: Der Verantwortliche ist berechtigt, die Einhaltung dieses AVV zu überprüfen. Hinsichtlich der zugrundeliegenden Cloud-Rechenzentren von Google Cloud EMEA Limited sind physische Vor-Ort-Begehungen durch den Verantwortlichen ausgeschlossen; der Nachweis erfolgt durch Vorlage aktueller unabhängiger Testate und Zertifikate (insbesondere ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II und BSI C5). Vor-Ort-Kontrollen oder Audits in den Geschäftsräumen des Auftragnehmers sind nach schriftlicher Anmeldung mit mindestens 14 Werktagen Vorlauf während der üblichen Geschäftszeiten zulässig, sofern der Betriebsablauf nicht unverhältnismäßig gestört wird.

(2) Haftung: Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO; im Innenverhältnis haften die Parteien entsprechend ihrem jeweiligen Verursachungsbeitrag nach den gesetzlichen Bestimmungen und etwaigen Haftungsbegrenzungen des Hauptvertrags, soweit gesetzlich zulässig.

(3) Formvorschrift (Art. 28 Abs. 9 DSGVO): Dieser AVV kann schriftlich oder in einem elektronischen Format gemäß Art. 28 Abs. 9 DSGVO abgeschlossen werden. Änderungen und Ergänzungen dieses AVV bedürfen mindestens der Textform (§ 126b BGB).

(4) Rangfolge & Salvatorische Klausel: Bei Widersprüchen zwischen diesem AVV und den AGB oder sonstigen Vereinbarungen zwischen den Parteien gehen die Regelungen dieses AVV in Bezug auf den Datenschutz vor. Sollte eine Bestimmung dieses AVV unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(5) Anwendbares Recht und Gerichtsstand: Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG). Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist Mannheim, sofern der Verantwortliche Kaufmann im Sinne des Handelsgesetzbuchs (HGB), juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist (§ 38 Abs. 1 ZPO).

---

Elektronische Ausfertigung gem. Art. 28 Abs. 9 DSGVO (oder schriftliche Gegenzeichnung).

**FÜR DEN AUFTRAGGEBER (VERANTWORTLICHER)**

_____

Vertretungsberechtigte Person

Ort, Datum (17.11.2026) · Unterschrift

**FÜR DEN AUFTRAGNEHMER (AUFTRAGSVERARBEITER)**

**be.smart · Inhaber Sebastian Hammer**

Traminerweg 5, 68309 Mannheim, Deutschland

Mannheim, 17.11.2026 · Elektronische Ausfertigung gem. Art. 28 Abs. 9 DSGVO

ANLAGE 1 ZUM AVV

# Technische und organisatorische Maßnahmen (TOMs gem. Art. 32 DSGVO)

Plattform Tendermeister (be.smart) · Auftraggeber: Verantwortlicher

## 1. Zutrittskontrolle

Art. 32 Abs. 1 lit. b DSGVO · ISO/IEC 27001 / BSI C5

- Hosting der produktiven Anwendung und Datenbanken ausschließlich in zertifizierten Rechenzentren von Google Cloud EMEA Limited in europe-west1 (St. Ghislain, Belgien).
- Mehrstufige physische Zutrittssicherung im Rechenzentrum durch biometrische Zugangsschleusen, elektronische Ausweiskontrolle, lückenlose Videoüberwachung und 24/7-Sicherheitsdienst.
- Keine Speicherung produktiver Kundendaten auf lokalen Servern in den Geschäftsräumen des Auftragnehmers; Zugangskontrolle zu den Geschäftsräumen in Mannheim über gesicherte Schließsysteme.

## 2. Zugangskontrolle (Systemzugang)

Art. 32 Abs. 1 lit. b DSGVO

- Authentifizierung aller Nutzer ausschließlich über Firebase Authentication (Google OAuth 2.0 oder E-Mail/Passwort-Verfahren) mit kryptografisch signierten Session-Tokens.
- Jeder geschützte Backend-API-Aufruf erzwingt die serverseitige Validierung des Firebase Bearer ID Tokens (verifyAuth) vor Verarbeitung oder Cache-Zugriff.
- Administrativer Zugang zur Google Cloud Platform / Firebase Console ausschließlich über Hardware-/App-basierte Multi-Faktor-Authentifizierung (MFA) nach dem Least-Privilege-Prinzip.

## 3. Zugriffskontrolle (Datenzugriff)

Art. 32 Abs. 1 lit. b DSGVO · § 2 GeschGehG

- Strikte mandantenspezifische Zugriffsisolation auf Datenbankebene über Firestore Security Rules je Kunden-Workspace (isActiveWorkspaceMember(companyId): Eigentümer request.auth.uid == companyId sowie vom Auftraggeber ausdrücklich autorisierte aktive Team-Mitglieder über company_members und den serverseitig gesetzten workspaceCompanyId-Token-Claim) sowie unveränderliche Mandantenzuordnung bei Dokumenten-Updates.
- Serverseitige Eigentumsprüfung (assertTenderOwnership / tender.companyId === uid) bei sämtlichen Sub-Endpunkten vor Lese-, Cache- und Schreibvorgängen.
- Minimale Zugriffsrechte innerhalb von Cloud Storage auf mandantenbezogene Speicherpfade (companies/{uid}/...); Cron- und Wartungsendpunkte sind zusätzlich durch timing-sichere Secret-Prüfung (CRON_SECRET) abgesichert.

## 4. Weitergabekontrolle & Verschlüsselung

Art. 32 Abs. 1 lit. a & b DSGVO

- Ausnahmslose Transportverschlüsselung sämtlicher Web-, API- und Datenbankverbindungen über TLS 1.3 / HTTPS.
- Durchgängige Ruhedatenverschlüsselung (Encryption at Rest) aller Firestore-Datenbanken, Cloud-Storage-Objekte und Backups mittels AES-256.
- Im Tarif Tendermeister Ultra steht zusätzlich das optionale clientseitige Schwärzungsmodul (BidSecretPreviewModal) bereit, um Firmennamen, IBAN, USt-IdNr., Kontaktdaten und Margen vor dem Versand an KI-Endpunkte lokal im Browser zu tokenisieren.

## 5. Eingabekontrolle

Art. 32 Abs. 1 lit. b DSGVO

- Protokollierung von Dokumentenuploads, Analyse-Status, LV-Preisänderungen und Submission-Outcomes mit serverseitigen Zeitstempeln und eindeutigen Benutzer-/Mandantenkennungen.
- Input-Validierung und serverseitige Bereinigung sicherheitskritischer Felder (z. B. Stripe-IDs, companyId-Unveränderlichkeit) an sämtlichen Cloud-Function-Schnittstellen.
- Datensparsames Client-/Server-Fehlertracking (Sentry EU, de.sentry.io) ohne Übertragung von Klarnamen, Passwörtern, User-Agents oder vertraulichen Ausschreibungs- und Kalkulationsinhalten.

## 6. Auftragskontrolle & KI-Datenresidenz

Art. 28 Abs. 3, Art. 32 Abs. 1 lit. b DSGVO

- Verarbeitung ausschließlich auf Basis dieses AVV nach Art. 28 DSGVO sowie dokumentierter Kundenweisungen; verbindliche Vertraulichkeits- und GeschGehG-Verpflichtung aller Mitarbeitenden (Anlage 3).
- KI-Inferenz ausschließlich über Google Cloud Vertex AI im EU Multi-Region-Standort eu unter B2B Enterprise Privacy Terms (Zero-Training-Garantie: kein Modelltraining mit Kundendaten).
- Abschluss von Art.-28-DSGVO-Vereinbarungen (DPAs) mit sämtlichen in Anlage 2 genannten Unterauftragsverarbeitern.

### 7. Verfügbarkeitskontrolle & Belastbarkeit

Art. 32 Abs. 1 lit. b & c DSGVO

- Hochverfügbare Serverless-Architektur auf Google Cloud Run / Firebase Cloud Functions v2 (europe-west1) mit automatischer Skalierung und Lastverteilung.
- Automatisierte Datensicherungen in Firestore und Cloud Storage innerhalb der EU sowie Edge-DDoS-Schutz und WAF-Filterung über Cloudflare.
- Definierte Timeouts, Ratenbegrenzungen und Ausfallsicherung (Overflow-Fallback innerhalb Vertex AI EU) zur Gewährleistung der Systemstabilität bei großen Ausschreibungspaketen.

### 8. Trennungskontrolle

Art. 32 Abs. 1 lit. b DSGVO · § 5 VgV

- Vollständige logische und kryptografische Mandantentrennung je Kunden-Workspace (companyId inklusive ausdrücklich autorisierter Team-Mitglieder über company_members / workspaceCompanyId-Claim; strikt getrennt von fremden Kunden-Tenants) in allen Datenbank-Collections, Cloud Storage und KI-Kontexten.
- Strikte Trennung von Unternehmenspreis-Katalogen (tender_lv/ref_{companyId}_{docId}): Historische Einheitspreise eines Kunden stehen technisch niemals anderen Mandanten zur Verfügung.
- Getrennte Produktiv-, Entwicklungs- und Testumgebungen sowie getrennte Verarbeitung aggregierter interner KPI-Metriken (europe-west3) ohne Personen- oder Angebotsbezug.

### 9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Art. 32 Abs. 1 lit. d DSGVO

- Regelmäßige Überprüfung der Firestore Security Rules, API-Authentifizierungspfade und IAM-Berechtigungen sowie automatisierte Typ-, Build- und Sicherheitstests vor Produktiv-Releases.
- Laufendes Monitoring der Funktionsverfügbarkeit und Fehlerquoten sowie regelmäßige Prüfung der Compliance-Zertifizierungen der Unterauftragsverarbeiter (ISO 27001, SOC 2 Type II, BSI C5).
- Dokumentierter Incident-Response-Prozess zur Erfüllung der 24-Stunden-Meldepflicht nach § 8 dieses AVV sowie regelmäßige Aktualisierung der TOMs bei technischen Weiterentwicklungen.

ANLAGE 2 ZUM AVV

# Genehmigte Unterauftragsverarbeiter & Abgrenzung

| Unterauftragsverarbeiter | Leistung / Zweck | Standort & Garantien |
|---|---|---|
| **Google Cloud EMEA Limited / Google Ireland Limited**<br>Gordon House, Barrow Street, Dublin 4, Irland | Cloud-Infrastruktur, Authentifizierung (Firebase Auth), Datenbank (Cloud Firestore), Dateispeicher (Cloud Storage), Backend-Funktionen (Cloud Functions) & Enterprise KI-Verarbeitung (Vertex AI) | **EU: europe-west1 (St. Ghislain, Belgien); Vertex AI Multi-Region eu (EU); interner aggregierter KPI-Export europe-west3 (Frankfurt am Main, DE)**<br>Google Cloud DPA (Art. 28 DSGVO), Enterprise Zero-Training SLA, ISO/IEC 27001 / 27017 / 27018, SOC 2 Type II, BSI C5 |
| **Cloudflare, Inc. / Cloudflare Germany GmbH**<br>Rosental 7, 80331 München, Deutschland / 101 Townsend St, San Francisco, CA 94107, USA | DNS-Auflösung, TLS-Terminierung, Edge-Routing, Web Application Firewall & DDoS-Schutz | **EU / Global Edge Network (Data Localization / EU Edge)**<br>Cloudflare DPA (Art. 28 DSGVO), EU-US Data Privacy Framework (Art. 45 DSGVO), EU-Standardvertragsklauseln (2021/914) |
| **Functional Software, Inc. (Sentry EU)**<br>45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA · EU-Ingest: de.sentry.io | Technisches Fehler- und Stabilitäts-Monitoring ohne Übertragung von Klarnamen oder vertraulichen Ausschreibungs-/Kalkulationsinhalten | **Europäische Union (Ingest-Endpunkt de.sentry.io)**<br>Sentry DPA (Art. 28 DSGVO), EU-US Data Privacy Framework (Art. 45 DSGVO), EU-Standardvertragsklauseln (2021/914) |
| **Resend, Inc. / Brevo (Sendinblue SAS)**<br>Brevo: 106 boulevard Haussmann, 75008 Paris, Frankreich / Resend: 2261 Market Street, San Francisco, CA 94114, USA | Zustellung transaktionaler System-, Frist-, Benachrichtigungs- und Onboarding-E-Mails (ausschließlich Empfängeradresse & Benachrichtigungsinhalt) | **EU (Brevo, Paris, FR) bzw. EU/US mit DPF & EU-SCC (Resend)**<br>Jeweiliger Auftragsverarbeitungsvertrag (DPA Art. 28 DSGVO), EU-US Data Privacy Framework / EU-Standardvertragsklauseln |

**Ausdrückliche Abgrenzung (keine Unterauftragsverarbeitung im Sinne dieses AVV):**

- **Stripe Payments Europe, Limited / Stripe, Inc. (Eigenständiger Verantwortlicher (Art. 4 Nr. 7 DSGVO)):** Abwicklung von Abonnement-Zahlungen, Kreditkarten-, SEPA-Lastschrift- und steuerkonformer Rechnungsstellung. Stripe verarbeitet Abrechnungs- und Zahlungsdaten in eigener datenschutzrechtlicher Verantwortung (https://stripe.com/privacy) und erhält keinen Zugriff auf Ausschreibungsunterlagen oder Kalkulationsdaten.
- **Google Analytics 4 (Mess-ID G-8RNM0LTVDS, Google Ireland Limited) (Striktes Opt-In ausschließlich auf öffentlichen Informationsseiten (Art. 6 Abs. 1 lit. a DSGVO)):** Google Analytics 4 ist standardmäßig deaktiviert und wird erst nach ausdrücklicher aktiver Einwilligung (Opt-In) im Cookie-Banner geladen. Dabei greifen automatische IP-Anonymisierung sowie die Maskierung vertraulicher Anwendungspfade (u. a. /workflow/ und /proposals/). Ein Widerruf ist jederzeit über „Cookie-Einstellungen“ möglich.

ANLAGE 3 ZUM AVV

# Anlage 3: Muster-Verpflichtungserklärung zur Vertraulichkeit, zum Datengeheimnis und zum Schutz von Geschäftsgeheimnissen

*gemäß Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO, § 53 BDSG sowie §§ 2, 4, 23 GeschGehG*

**Hintergrund:** Der Auftragsverarbeiter (be.smart) erbringt über die Plattform Tendermeister IT- und KI-Dienstleistungen für Unternehmen aus der Bau-, Dienstleistungs- und Lieferwirtschaft im Bereich öffentlicher und privater Vergabeverfahren. Hierbei können Mitarbeitende und Erfüllungsgehilfen Zugriff auf personenbezogene Daten sowie auf hochvertrauliche Angebots-, Preis- und Kalkulationsgeheimnisse (§ 2 Nr. 1 GeschGehG, § 5 VgV) erhalten.

### 1. Belehrung über das Datengeheimnis (Art. 29, 32 Abs. 4 DSGVO, § 53 BDSG)

Die verpflichtete Person wurde darüber belehrt, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten, Dritten zugänglich zu machen oder zu anderen als den jeweils zur rechtmäßigen Aufgabenerfüllung gehörenden Zwecken zu nutzen (Datengeheimnis). Die Pflicht zur Wahrung des Datengeheimnisses besteht auch nach Beendigung der Tätigkeit für be.smart fort.

### 2. Belehrung über den Schutz von Geschäfts- und Kalkulationsgeheimnissen (§§ 2, 4, 23 GeschGehG, § 5 VgV)

Die verpflichtete Person wurde ausdrücklich darüber belehrt, dass Kundenunterlagen — insbesondere Leistungsverzeichnisse, Einheitspreise, Kalkulationsansätze, Margen, Referenzkataloge, Subunternehmerangebote und Bieterstrategien — schützenswerte Geschäftsgeheimnisse im Sinne des § 2 Nr. 1 GeschGehG darstellen. Nach §§ 4, 23 GeschGehG ist das unbefugte Erlangen, Nutzen oder Offenlegen von Geschäftsgeheimnissen verboten und kann zivilrechtliche Schadensersatzansprüche sowie strafrechtliche Folgen (Freiheitsstrafe bis zu drei Jahren oder Geldstrafe) nach sich ziehen.

### 3. Need-to-know-Prinzip und Verbot der Weitergabe / Modellnutzung

Die verpflichtete Person darf Kundendaten ausschließlich im absolut erforderlichen Umfang zur Erfüllung dokumentierter Support-, Wartungs- oder Betriebsaufgaben einsehen (Need-to-know-Prinzip). Jede Weitergabe von Preis-, Bieter- oder Projektdaten an unbefugte Dritte oder andere Kunden sowie jede Verwendung zu Trainingszwecken ist strikt untersagt.

### 4. Verbindliche Verpflichtungserklärung

Die verpflichtete Person verpflichtet sich hiermit verbindlich, über sämtliche im Rahmen ihrer Tätigkeit bekannt werdenden personenbezogenen Daten sowie Geschäfts- und Kalkulationsgeheimnisse der Kunden von be.smart strengstes Stillschweigen zu bewahren, alle Sicherheitsvorgaben (TOMs, MFA, verschlüsselte Systeme) einzuhalten und diese Pflichten auch nach Beendigung des Beschäftigungs- oder Auftragsverhältnisses uneingeschränkt zu wahren.

**Verpflichtete Person**

Datum, Ort · Name, Unterschrift des Verpflichteten

**Auftragsverarbeiter (be.smart · Sebastian Hammer)**

Mannheim, 17.11.2026 · Unterschrift be.smart