

Beschaffungsassistent

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 DSGVO mit Unterauftragsverarbeiterverzeichnis und technischen sowie organisatorischen Maßnahmen

Vertragspartner / Angaben zum Auftraggeber

Feld	Angabe
Auftraggeber / Organisation	
Adresse Auftraggeber	
Vertretungsberechtigte Person	
Datenschutzkontakt Auftraggeber	
Hauptvertrag / Bestellbezug	
Geltungsbeginn der AVV	
Zuständige Aufsichtsbehörde	
Besondere Weisungen oder Abweichungen	

Auftragnehmer / Auftragsverarbeiter

PPI Public Procurement Intelligence GmbH, Am alten Sportplatz 11, 52499 Baesweiler, Deutschland

Handelsregister: Amtsgericht Aachen, HRB 30043 | Vertreten durch: Lucas Spänhoff, Geschäftsführer

E-Mail: info@beschaffungsassistent.de | Dienst: Beschaffungsassistent / beschaffungsassistent.de

Präambel

Der Auftraggeber nutzt den Beschaffungsassistenten als webbasierte Software-as-a-Service-Lösung zur Unterstützung von Beschaffungs-, Vergabe- und Vertragsmanagementprozessen. Soweit die PPI Public

Procurement Intelligence GmbH im Rahmen des Dienstes personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, regeln die Parteien mit dieser Vereinbarung die Anforderungen des Art. 28 DSGVO.

Der Auftraggeber bleibt Verantwortlicher im Sinne des Datenschutzrechts. Die PPI Public Procurement Intelligence GmbH handelt als Auftragsverarbeiter, soweit keine abweichende Verantwortlichkeit ausdrücklich vereinbart ist.

DSGVO-konforme Nutzung

Der Dienst stellt technische, organisatorische und vertragliche Grundlagen für eine datenschutzkonforme Nutzung bereit. Die konkrete Rechtmäßigkeit einzelner Verarbeitungsvorgänge, Rollenvergaben, Informationspflichten und Weisungen liegt im Verantwortungsbereich des Auftraggebers.

§ 1 Gegenstand und Dauer der Verarbeitung

Gegenstand der Verarbeitung ist die Bereitstellung, der Betrieb, die Wartung und der Support des Beschaffungsassistenten einschließlich Registrierung, Authentifizierung, Organisations- und Rollenverwaltung, Projekt-, Beschaffungs-, Vergabe-, Anbieter-, Dokumenten- und Vertragsmanagement, KI-gestützter Analyse und Generierung einschließlich serverseitiger Modellsteuerung, Fallback- und Backup-Logik, optionaler Meeting-, Community-, Export- und Integrationsfunktionen sowie transaktionaler Kommunikation.

Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags zuzüglich erforderlicher Nachlauf-, Export-, Backup-, Nachweis- und Löschfristen gemäß dieser Vereinbarung. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung umfasst je nach Nutzung insbesondere Erheben, Erfassen, Organisieren, Strukturieren, Speichern, Auslesen, Abfragen, Verwenden, Übermitteln, Bereitstellen, Abgleichen, Einschränken, Löschen, Exportieren und Anonymisieren personenbezogener Daten.

Zweck ist ausschließlich die Erbringung des Beschaffungsassistenten und der damit verbundenen vertraglichen Leistungen, einschließlich Sicherheit, Fehlerdiagnose, Support, Dokumentation, Systembenachrichtigung, Missbrauchsabwehr und vertraglich vereinbarter Lösch- und Exportprozesse.

§ 3 Weisungen

Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, sofern keine gesetzliche Verpflichtung zu einer abweichenden Verarbeitung besteht. Als Weisungen gelten der Hauptvertrag, diese Vereinbarung, die Konfiguration und Nutzung des Dienstes durch berechtigte Nutzer sowie weitere Weisungen in Textform.

Der Auftragnehmer informiert den Auftraggeber, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Die Umsetzung offensichtlich rechtswidriger Weisungen kann bis zur Klärung ausgesetzt werden.

§ 4 Kategorien personenbezogener Daten und nicht bestimmungsgemäße Inhalte

Die Kategorien personenbezogener Daten und betroffener Personen ergeben sich aus Anlage 1.

Der Dienst ist nicht auf die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO, Patientendaten, Gesundheitsdaten, Sozialdaten, Daten über strafrechtliche Verurteilungen und Straftaten oder Berufsgeheimnisse ausgerichtet. Solche Daten dürfen nur verarbeitet werden, wenn dies vorab ausdrücklich vereinbart wurde, eine geeignete Rechtsgrundlage besteht und die hierfür erforderlichen zusätzlichen technischen, organisatorischen und vertraglichen Maßnahmen festgelegt wurden.

Der Auftraggeber nutzt Freitextfelder, Uploads, Meetingfunktionen, KI-Prompts und Supportkanäle datenminimiert. Werden nicht bestimmungsgemäße sensible Inhalte unbeabsichtigt eingebracht, unterstützen sich die Parteien angemessen bei Sperrung, Löschung, Export oder sonstiger Risikominimierung.

§ 5 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet die mit der Verarbeitung betrauten Personen auf Vertraulichkeit oder stellt sicher, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftragnehmer trifft technische und organisatorische Maßnahmen nach Art. 32 DSGVO gemäß Anlage 3 und passt diese unter Berücksichtigung von Risiko, Stand der Technik und Dienstentwicklung angemessen an.

Der Auftragnehmer unterstützt den Auftraggeber in angemessenem Umfang bei Betroffenenrechten, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen, aufsichtsbehördlichen Anfragen und Nachweisen, soweit sich diese auf die Auftragsverarbeitung im Beschaffungsassistenten beziehen.

Der Auftragnehmer verarbeitet produktive Kundendaten nicht für eigene Trainingszwecke. Eine optionale Trainings- oder Verbesserungsnutzung final freigegebener Inhalte erfolgt nur nach ausdrücklichem Opt-In und nur in anonymisierter Form.

§ 6 Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Rechtsgrundlagen, Informationspflichten, die Wahrung der Betroffenenrechte und die Richtigkeit seiner Weisungen verantwortlich.

Der Auftraggeber verwaltet Nutzer, Rollen und Berechtigungen in eigener Verantwortung und stellt sicher, dass nur berechnete Personen Zugriff erhalten.

Bei Meeting-Aufzeichnungen informiert der Auftraggeber bzw. der aufzeichnende Nutzer alle Teilnehmenden vor Beginn der Aufzeichnung transparent und holt erforderliche Einwilligungen ein.

Der Auftraggeber exportiert vor Vertragsende rechtzeitig Daten, die er nach Vertragsende benötigt.

§ 7 Unterauftragsverarbeiter

Der Auftraggeber erteilt eine allgemeine Genehmigung zum Einsatz der in Anlage 2 benannten Unterauftragsverarbeiter. Der Auftragnehmer setzt Unterauftragsverarbeiter nur ein, soweit dies zur Erbringung, Sicherheit, Wartung, Skalierung, Zustellung oder Unterstützung des Dienstes erforderlich ist.

Der Auftragnehmer stellt sicher, dass mit Unterauftragsverarbeitern datenschutzrechtliche Vereinbarungen bestehen, die im Wesentlichen ein angemessenes Schutzniveau für die betroffenen Daten vorsehen. Der Auftragnehmer bleibt für die Leistung seiner Unterauftragsverarbeiter nach Maßgabe des Art. 28 DSGVO verantwortlich.

Wesentliche Änderungen der Unterauftragsverarbeiterliste werden grundsätzlich mindestens 30 Tage vor Wirksamwerden angekündigt, soweit eine vorherige Information möglich und zumutbar ist. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

§ 8 Drittlandübermittlungen

Die produktive Kernverarbeitung ist auf EU-/EWR-Regionen ausgerichtet. Der Einsatz globaler Endpunkte, Partner-/KI-Modelle, Support-, Sicherheits- oder Betriebsprozesse kann je nach Funktion zu Drittlandbezügen führen. Drittlandübermittlungen erfolgen nur, soweit hierfür eine zulässige Grundlage besteht, insbesondere Standardvertragsklauseln, ergänzende Schutzmaßnahmen, vertragliche Unter-Unterauftragsverarbeiterpflichten oder andere Transfermechanismen nach Kapitel V DSGVO.

Die einbezogenen Plattform-, Infrastruktur- und KI-Anbieter sehen in ihren jeweiligen DPAs, Servicebedingungen und Subprozessorregelungen für Unterauftragsverarbeiter, Support-, Sicherheits-, Betriebs- und Partner-Model-Prozesse geeignete Garantien vor. Soweit hieraus eine Verarbeitung außerhalb der EU/des EWR entsteht, erfolgt diese nur nach Maßgabe der dort geregelten Transfermechanismen und Schutzpflichten.

§ 9 Sicherheit und TOM

Die in Anlage 3 beschriebenen TOM konkretisieren das Schutzniveau des Dienstes. Der Auftragnehmer kann gleichwertige oder bessere Maßnahmen einsetzen, sofern das Schutzniveau nicht wesentlich abgesenkt wird.

Der Auftraggeber ist für sicherheitsrelevante Einstellungen in seinem Organisationsaccount, insbesondere Nutzerverwaltung, Rollen, Passwörter, MFA-Nutzung, lokale Endgeräte und exportierte Daten, verantwortlich.

§ 10 Datenschutzverletzungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, soweit im Auftrag verarbeitete personenbezogene Daten betroffen sind. Die Mitteilung enthält, soweit verfügbar, Art des Vorfalls, betroffene Datenkategorien, wahrscheinliche Auswirkungen und eingeleitete oder empfohlene Gegenmaßnahmen.

Die Parteien unterstützen sich im erforderlichen Umfang bei der Aufklärung und bei gesetzlichen Melde- oder Benachrichtigungspflichten.

§ 11 Betroffenenrechte und Unterstützung

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung angemessen bei Auskunft, Berichtigung, Löschung, Einschränkung, Herausgabe, Datenübertragbarkeit, Widerspruch und sonstigen Betroffenenrechten, soweit dies die vom Auftragnehmer verarbeiteten Daten und Systeme betrifft.

Erhält der Auftragnehmer eine Betroffenenanfrage, die dem Auftraggeber zuzuordnen ist, leitet er diese grundsätzlich an den Auftraggeber weiter, sofern keine gesetzliche Pflicht zu einer eigenen Reaktion besteht.

§ 12 Nachweise und Audits

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage angemessene Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieser Vereinbarung nachzuweisen. Vorrangig können geeignete Nachweise wie TOM-Beschreibungen, DPA-Auszüge, Zertifikate, Auditberichte, Subprozessorlisten, Richtlinien, Remote-Auskünfte oder das Nachweis-/DPA-Verzeichnis nach Anlage 5 bereitgestellt werden.

Vor-Ort-Audits sind ausgeschlossen, soweit der Prüfzweck durch geeignete Nachweise, Zertifikate, Dokumentation, Remote-Auskünfte oder sonstige angemessene Prüfhandlungen erreicht werden kann. Zwingende gesetzliche Prüf- oder Inspektionsrechte bleiben unberührt; in diesem Fall sind Prüfungen angemessen vorher anzukündigen, vertraulich durchzuführen und so zu begrenzen, dass Betrieb, Sicherheit und Rechte anderer Kunden nicht beeinträchtigt werden.

§ 13 Rückgabe, Export und Löschung

Der Auftraggeber kann während der Vertragslaufzeit verfügbare Exportfunktionen nutzen. Nach Vertragsende werden produktive Kundendaten grundsätzlich für einen begrenzten Nachlaufzeitraum zur Rückgabe vorgehalten, soweit keine sofortige Löschung geschuldet ist oder gesetzliche Aufbewahrungspflichten entgegenstehen.

Produktive Daten werden nach Ablauf des Nachlaufzeitraums gelöscht oder anonymisiert. Für die produktive Supabase-Pro-Datenbank werden täglich automatisierte Datensicherungen erstellt. Im Standardbetrieb stehen die Sicherungen der letzten sieben Tage zur Wiederherstellung zur Verfügung. Die Datenbanksicherungen enthalten keine Dateiobjekte aus Supabase Storage. Residuale Sicherungs-, Recovery- oder Löschrufen einzelner Infrastruktur- oder Plattformanbieter können sich zusätzlich nach deren DPA und Dienstbedingungen richten und werden nicht für produktive Zwecke genutzt.

Support-Tickets, Sicherheits- und Betriebsnachweise dürfen für Vertragserfüllung, Nachweisführung, Sicherheit und Compliance bis zu 24 Monate aufbewahrt werden, soweit kein kürzerer Löschanpruch oder eine längere gesetzliche Pflicht besteht.

§ 14 Schlussbestimmungen

Diese Vereinbarung ergänzt den Hauptvertrag. Im Fall von Widersprüchen gehen individualvertragliche Regelungen und zwingende gesetzliche Anforderungen vor; im Übrigen gilt die für den Hauptvertrag vereinbarte Rangfolge.

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform, soweit nicht zwingende gesetzliche Anforderungen eine andere Form erfordern.

Anlage 1 - Gegenstand, Datenkategorien und betroffene Personen

Kategorie	Beschreibung
Gegenstand	Bereitstellung, Betrieb, Wartung, Support und Weiterentwicklung des Beschaffungsassistenten als SaaS-Plattform.
Dauer	Laufzeit des Hauptvertrags zuzüglich Nachlauf-, Export-, Backup-, Nachweis- und Löschrufen.
Art und Zweck	Speicherung, Bearbeitung, Strukturierung, Analyse, Generierung, Kommunikation, Export und Löschung von Daten zur Unterstützung von Beschaffungs-, Vergabe- und Vertragsmanagementprozessen.

Datenkategorien

Datenkategorie	Beispiele
Account- und Organisationsdaten	Name, dienstliche E-Mail-Adresse, Organisation, Rolle, Lizenzstatus, Kontaktdaten, Login- und Rolleninformationen.
Projekt-, Vergabe- und Vertragsdaten	Vergabeunterlagen, Vertragsakten, Fristen, Projektnotizen, Dokumente, Chat-Inhalte, Freitexte, Exportdaten, KI-generierte Entwürfe und Zusammenfassungen.
Anbieter-, Angebots- und Portaldaten	Kontaktpersonen, Unternehmensangaben, Uploads, Einreichungen, Angebotsdateien, Termin- und Rückfragedaten.
Kommunikations- und Supportdaten	Supportanfragen, E-Mails, Systembenachrichtigungen, Ticketdaten, Statusmeldungen.
Meetingdaten	Audioaufzeichnungen, Transkripte, Zusammenfassungen, Termin- und Einladungsdaten, Teilnehmerbezug.
Communitydaten	Beiträge, Kommentare, Zeitstempel, sichtbare Profilinformationen.
Protokoll- und Sicherheitsdaten	IP-Adressen, Geräte-/Browserinformationen, Login-Zeitpunkte, API-Requests, Fehlermeldungen, Sicherheitsereignisse, Rechteänderungs-, Angebots- und Vergabeereignisse sowie technische Nutzungs-, KI-, Modellrouting- und Fallback-Metadaten.

Betroffene Personen

Betroffene Personen	Beispiele
Nutzer des Auftraggebers	Beschäftigte, Administratoren, fachliche Bearbeiter, Freigabeberechtigte.
Externe Beteiligte	Anbieter, Bieter, Lieferanten, Kontaktpersonen, Meetingteilnehmende, Supportkontakte.
Dritte in Unterlagen	Personen, die in hochgeladenen oder erzeugten Dokumenten, Freitexten, Kommunikations- oder

Betroffene Personen	Beispiele
	Meetingdaten genannt werden.

Nicht bestimmungsgemäße sensible Inhalte

Besondere Kategorien personenbezogener Daten, Gesundheits- und Patientendaten, Sozialdaten, Daten über strafrechtliche Verurteilungen und Straftaten sowie Berufsgeheimnisse sind nicht Gegenstand der Standardnutzung. Eine abweichende Verarbeitung bedarf einer gesonderten Vereinbarung und zusätzlicher Schutzmaßnahmen.

Anlage 2 - Unterauftragsverarbeiterverzeichnis

Der Auftraggeber genehmigt die nachfolgend benannten Unterauftragsverarbeiter. Unter-Unterauftragsverarbeiter ergeben sich aus den jeweils gültigen Subprozessorlisten und Datenschutzbedingungen der Anbieter.

Dienstleister	Leistungsbereich	Ort / Region	AVV/DPA / Garantien
Supabase, Inc.	Datenbank, Authentifizierung, Storage, Plattformfunktionen, Edge Functions, Backups und betriebliche Kernfunktionen.	Frankfurt / EU	Abgeschlossenes Data Processing Addendum; SCCs und genehmigte Unter-Unterauftragsverarbeiter gemäß DPA; technische und organisatorische Maßnahmen, Sicherheits- und Compliance-Nachweise über Supabase.
Google Cloud	Hosting, Cloud Run, Infrastruktur, Storage, Logging, Verschlüsselungsdienste, Google Cloud / Gemini Enterprise Agent Platform (vormals Vertex AI), Speech-/Transkriptions- und weitere KI-Funktionen einschließlich serverseitigem Modellrouting, Fallback-	Frankfurt am Main, europäische Regionen oder die Google-Mehrregion EU. Speech-Transkriptionen ausschließlich über den europäischen Regionalendpunkt; weitere KI-Funktionen nur an europäischen Verarbeitungsorten.	Cloud Data Processing Addendum; anwendbare Google Cloud Service Terms und Partner-Model-Bedingungen; SCCs, Transfermechanismen, Subprozessorlisten und TOM von Google Cloud.

Dienstleister	Leistungsbereich	Ort / Region	AVV/DPA / Garantien
	und Backup-Logik. Vorgesehene KI-Backup-Logik: Claude Sonnet 4.6 über Google Cloud als alternative Anlaufstelle; Gemini 2.5 Flash über Google Cloud als zweite Backup-Anlaufstelle, jeweils soweit technisch verfügbar und für den Dienst aktiviert.		
Scaleway S.A.S.	Transaktionaler E-Mail-Versand für Registrierung, Einladungen, Passwort-Reset und Systemmails.	EU / Frankreich	Data Processing Agreement; Subprozessor- und SCC-Regelungen nach DPA; TOM von Scaleway.

Änderungen

Neue oder ersetzende Unterauftragsverarbeiter werden grundsätzlich mindestens 30 Tage vor Wirksamwerden mitgeteilt, soweit dies möglich und zumutbar ist. Ein Widerspruch ist aus wichtigem datenschutzrechtlichem Grund möglich. Wird keine angemessene Lösung gefunden, kann hinsichtlich der betroffenen Leistung ein Sonderkündigungsrecht bestehen.

Anlage 3 - Technische und organisatorische Maßnahmen (TOM)

Die Maßnahmen werden risikoorientiert umgesetzt und fortentwickelt. Gleichwertige oder bessere Maßnahmen können eingesetzt werden, sofern das Schutzniveau nicht wesentlich abgesenkt wird.

Schutzbereich	Konkrete Maßnahmen
Zutrittskontrolle und Rechenzentren	Produktive Systeme werden in professionell betriebenen Cloud- und Plattformumgebungen betrieben. Eigene öffentlich zugängliche Serverräume für Produktivdaten werden nicht betrieben. Für die physische Sicherheit werden die Rechenzentrums- und Standortkontrollen der Plattformanbieter genutzt: mehrschichtige Perimeter- und Gebäudesicherheit, Zugangsbeschränkungen, Authentifizierung des Zutritts, Besucherkontrolle, Video-/Umgebungsüberwachung, Brandschutz sowie

Schutzbereich	Konkrete Maßnahmen
	Wartungs- und Supportkontrollen nach den jeweiligen Anbieter-TOM.
Zugangskontrolle	Nutzerzugang erfolgt über Authentifizierungsprozesse des Dienstes. Betreiber- und Administrationszugänge werden vom normalen Nutzerzugang getrennt und nach dem Need-to-know-Prinzip vergeben. Für privilegierte Betriebszugänge wird MFA eingesetzt. Passwort-, Reauth- und Schutzmechanismen gegen kompromittierte Zugangsdaten werden in der Auth-Konfiguration nach dem Stand der verfügbaren Plattformfunktionen eingesetzt und überprüft.
Zugriffskontrolle und Rollen	Zugriffe werden über Organisations-, Projekt- und Rollenbezüge gesteuert. Nutzer sehen nur die für ihre Organisation, Rolle und Projekte freigegebenen Inhalte. Administrative Zugriffe werden organisatorisch begrenzt, nur anlassbezogen genutzt und nach Möglichkeit protokolliert. Service- und Betreiberrollen werden ausschließlich in geschützten serverseitigen Kontexten verwendet und nicht im Client offengelegt.
Mandantentrennung	Fachliche Anwendungstabellen und Storage-Metadaten werden datenbankseitig mit Row Level Security abgesichert. Die Zugriffskontrolle stützt sich auf RLS-Policies, Organisationsmitgliedschaften, Projektberechtigungen und geprüfte Berechtigungsfunktionen. Breitere technische Datenbankrollen werden dadurch nicht als alleinige Zugriffsbeschränkung verwendet; der fachliche Zugriff wird zusätzlich durch Policies und serverseitige Prüfungen eingeschränkt.
Dateiablage und Storage-Zugriffe	Vertraulichkeitsnahe Dateiablagen für Chat-, Nachrichten-, Meeting-, Projekt- und Vorlagendateien werden nicht über dauerhaft öffentliche URLs bereitgestellt. Der Zugriff erfolgt über projekt- oder organisationsbezogene Berechtigungen und kurzlebige Signed URLs. Öffentliche Ablagebereiche sind auf bewusst öffentliche Inhalte, insbesondere Logos oder öffentlich freizugebende Ressourcen, zu beschränken.

Schutzbereich	Konkrete Maßnahmen
	Upload-Pfade werden organisations-, projekt- oder nutzerbezogen strukturiert.
Privilegierte Datenbankfunktionen	Privilegierte RPC- und Datenbankfunktionen werden nur für kontrollierte fachliche Operationen eingesetzt. Administrations- und Berechtigungsprüfungen werden serverseitig hergeleitet; clientseitig veränderbare Benutzer-Metadaten werden nicht als alleinige Grundlage für Administrationsrechte verwendet. Direkte Ausführungsrechte für sensible Hilfsfunktionen werden auf erforderliche Rollen beschränkt.
Übertragungssicherheit	Die Kommunikation zwischen Nutzer, Plattform und unterstützenden Diensten erfolgt über TLS-basierte Transportverschlüsselung oder gleichwertige Verfahren. Browserseitige Sicherheitsheader und angemessene CORS-/Origin-Regeln unterstützen den Schutz gegen unbefugte Einbindung, Clickjacking und unsichere Übertragung.
Speichersicherheit und Verschlüsselung	Gespeicherte Daten werden im Rahmen der eingesetzten Plattform- und Infrastrukturleistungen verschlüsselt oder durch gleichwertige Verschlüsselungs- und Zugriffsschutzmechanismen geschützt. Supabase dokumentiert AES-256-basierte Verschlüsselung für Datenträger und Backups; Google Cloud und Scaleway stellen infrastruktureitige Schutz- und Verschlüsselungsmechanismen bereit. Secrets und Service-Schlüssel werden getrennt von Anwendungscode geführt.
Protokollierung und Nachvollziehbarkeit	Sicherheits- und betriebsrelevante Vorgänge werden protokolliert. Dazu gehören insbesondere Authentifizierungsereignisse, Rechteänderungen, Angebots- und Vergabeereignisse, technische Fehler, API-/Integrationsereignisse und ausgewählte KI-/Nutzungsmetadaten. Zugriff auf Logs erfolgt nach Need-to-know; Inhalte werden nach Möglichkeit datensparsam gestaltet.
Verfügbarkeit und Wiederherstellung	Die Plattform nutzt verwaltete Cloud-Dienste, Backup-

Schutzbereich	Konkrete Maßnahmen
	Mechanismen, Wiederherstellungsprozesse und Incident-Management. Datenbanksicherungen und Anbieter-Backups werden verschlüsselt verarbeitet, soweit vom Anbieter vorgesehen. Wiederherstellungsverfahren werden dokumentiert und risikoorientiert getestet; konkrete RTO-/RPO-Zusagen gelten nur, soweit sie im Hauptvertrag oder SLA ausdrücklich vereinbart sind.
Änderungsmanagement	Änderungen an Anwendung, Datenbankschema, Storage-Policies, Cloud-Konfigurationen und sicherheitsrelevanten Einstellungen werden versioniert, nachvollziehbar dokumentiert und kontrolliert ausgerollt. Sicherheitsrelevante Migrationen, Berechtigungsänderungen und Infrastrukturänderungen werden gesondert geprüft.
Schwachstellen und Patches	Relevante Komponenten, Abhängigkeiten und Plattformhinweise werden regelmäßig überprüft. Bekannte Schwachstellen werden nach Risiko priorisiert bearbeitet. Für Code und Abhängigkeiten werden automatisierte Prüfungen, Dependency-Monitoring und manuelle Reviews eingesetzt, soweit für die jeweilige Komponente einschlägig.
Entwicklungs-, Test- und Produktivtrennung	Entwicklungs-, Test- und Produktivumgebungen werden logisch getrennt und mit getrennten Projekt-, Rollen- und Secret-Konfigurationen betrieben. Umgebungen mit produktionsnahen oder personenbezogenen Daten werden ebenfalls als schutzbedürftig behandelt. Produktive Kundendaten werden nicht in Umgebungen mit niedrigerem Schutzniveau kopiert.
Datenschutz durch Technikgestaltung	Funktionen werden datenminimiert gestaltet. KI- und E-Mail-Prozesse sollen nur erforderliche Inhalte erhalten. Produktive Kundendaten werden nicht für eigene Trainingszwecke genutzt; eine optionale Verbesserungsnutzung erfolgt nur nach Opt-In und Anonymisierung. Nutzer werden angehalten, keine unnötigen personenbezogenen oder sensiblen Inhalte

Schutzbereich	Konkrete Maßnahmen
	einzubringen.
KI-spezifische Maßnahmen	KI-Funktionen sind assistive Funktionen und ersetzen keine rechtliche, vergaberechtliche oder fachliche Entscheidung des Auftraggebers. Die Verarbeitung erfolgt serverseitig über vertraglich eingebundene Anbieter und nach den regionalen Konfigurationen des Dienstes. KI-Anfragen können über eine Modellsteuerung verarbeitet werden; Fallback-/Backup-Modelle werden nur bei Verfügbarkeit, Fehlern, Latenz, Quoten, Qualitätssicherung oder Konfigurationsvorgaben genutzt. Derzeit vorgesehene Backup-Logik: Claude Sonnet 4.6 als alternative Anlaufstelle und Gemini 2.5 Flash als zweite Backup-Anlaufstelle, jeweils über Google Cloud / Gemini Enterprise Agent Platform (vormals Vertex AI), soweit aktiviert. Prompts, Outputs, Audio, Transkripte und KI-/Routing-Metadaten werden datensparsam und zweckgebunden verarbeitet; produktive Kundendaten werden durch den Auftragnehmer nicht für eigene Trainingszwecke genutzt.
E-Mail-spezifische Maßnahmen	Transaktionale E-Mails enthalten nur erforderliche Systeminformationen wie Registrierung, Einladung, Passwort-Reset, Status- oder Systemhinweise. Projekt-, Angebots-, Dokument-, Gesundheits- oder Berufsgeheimnisinhalte sollen nicht per transaktionaler E-Mail versendet werden. Domain-Authentifizierung, Bounce-/Fehlerbehandlung und Versandprotokolle werden technisch und organisatorisch berücksichtigt.
EU-Regionen und Unterauftragsverarbeiter	Die produktive Kernverarbeitung ist auf EU-/EWR-Regionen ausgerichtet. Supabase, Google Cloud und Scaleway werden vertraglich eingebunden. Drittlandbezüge, Supportprozesse, globale Endpunkte, Partner-/KI-Modelle und Unter-Unterauftragsverarbeiter richten sich nach den jeweiligen DPAs, Servicebedingungen, Subprozessorlisten und Transfermechanismen.

Schutzbereich	Konkrete Maßnahmen
Incident Response	Für Betriebs-, Sicherheits- und Datenschutzvorfälle bestehen interne Eskalations- und Bearbeitungsprozesse. Vorfälle werden bewertet, eingedämmt, dokumentiert und, soweit auftragsverarbeitete Daten betroffen sind, dem Auftraggeber mit den verfügbaren Informationen gemeldet.
Dienstleistersteuerung	Unterauftragsverarbeiter werden nach Leistungsbereich, Datenarten, Region, DPA-Status und Sicherheitsnachweisen bewertet. Änderungen werden nach Maßgabe dieser Vereinbarung angekündigt. Die Nachweisakte wird fortlaufend gepflegt.
Löschung und Retention	Produktive Kundendaten werden nach Vertragsende oder dokumentierter Weisung gelöscht oder anonymisiert, soweit keine Aufbewahrungspflichten entgegenstehen. Backup-Nachläufe, Support-, Sicherheits- und Betriebsnachweise werden zweckgebunden und zeitlich begrenzt aufbewahrt. Private Dateiablagen werden bei Account-, Projekt- oder Vorlagenlöschungen in die Löschprozesse einbezogen.

Anlage 4 - Verantwortlichkeiten des Auftraggebers

Die folgende Übersicht dient der praktischen Umsetzung und Dokumentation beim Auftraggeber.

- Rechtsgrundlage für die eigene Verarbeitung bestimmen und dokumentieren, z. B. öffentliche Aufgabe, Vertragserfüllung oder Einwilligung.
- Nutzer, Rollen und Projektzugriffe regelmäßig prüfen; ausgeschiedene Nutzer entfernen.
- Freitextfelder, Uploads, KI-Prompts und Meetingfunktionen datenminimiert nutzen.
- Keine nicht bestimmungsgemäßen sensiblen Inhalte einstellen, sofern hierfür keine gesonderte Vereinbarung besteht.
- Meetingteilnehmende vor Aufzeichnungen informieren und erforderliche Einwilligungen einholen.
- Vergabe-, haushalts-, handels- und steuerrechtliche Aufbewahrungspflichten eigenverantwortlich beachten; erforderliche Daten vor Löschung exportieren.
- Datenschutz-Folgenabschätzung prüfen, soweit Art, Umfang oder Kontext der Verarbeitung ein hohes Risiko nahelegen.

- Interne Datenschutz- und IT-Sicherheitsdokumentation, Berechtigungskonzepte und Betroffeneninformationen aktualisieren.

Zusätzliche Angaben des Auftraggebers

Thema	Angabe / Weisung
Abweichende Weisungen / Einschränkungen	
Besondere interne Lösch-/Exportanforderungen	
Besondere Rollen-/Berechtigungsvorgaben	
Besondere Vertraulichkeitsanforderungen	

Anlage 5 - Nachweis- und DPA-Anlagen

Die folgenden Unterlagen dienen der Nachweisführung gegenüber Auftraggebern. Vollständige DPAs von Unterauftragsverarbeitern sollten nicht automatisch Bestandteil jeder Kunden-AVV werden; sie können nach berechtigter Anfrage als Auszug, Link, Zertifikat, Subprozessorliste oder redigierte Nachweiskopie bereitgestellt werden, soweit keine Vertraulichkeits-, Sicherheits- oder Datenschutzgründe entgegenstehen.

Nachweis / Unterlage	Status / Ablage	Hinweis für Kundenbereitstellung
Supabase Data Processing Addendum	abgeschlossen; Nachweisakte	Als Nachweis für Datenbank-, Auth-, Storage-, Edge-Functions- und Backup-Leistungen. Vollständige signierte Fassung eher nicht standardmäßig beifügen; bei Bedarf redigierte Kopie oder Auszug bereitstellen.
Google Cloud Data Processing Addendum und anwendbare Google Cloud Service-/Partner-Model-Bedingungen	Nachweis in der Google-Cloud-Nachweisakte dokumentieren/ergänzen	Relevant für Google Cloud Platform / Gemini Enterprise Agent Platform (vormals Vertex AI), einschließlich Gemini 2.5 Flash und Claude Sonnet 4.6 als über Google Cloud bereitgestelltes Partner-/MaaS-Modell, soweit aktiviert.
Scaleway Data Processing Agreement	Nachweisakte	Relevant für transaktionalen E-Mail-Versand, Registrierung, Einladungen, Passwort-Reset und Systembenachrichtigungen.
Subprozessorlisten, TOM-Auszüge, Zertifikate, Audit-/Compliance-Nachweise	laufend aktuell halten	Vorrangige Nachweisform gegenüber vollständigen Drittanbieter-DPAs; Aktualität vor Kundenausgabe prüfen.

Unterschriften / Annahme

Diese Vereinbarung kann in Textform, elektronisch oder durch beiderseitige Unterzeichnung angenommen werden, soweit der Hauptvertrag keine strengere Form vorsieht.

Für den Auftraggeber	Für den Auftragnehmer
Ort, Datum	Ort, Datum
Name / Funktion	Name / Funktion PPI Public Procurement Intelligence GmbH vertreten durch Lucas Spänhoff, Geschäftsführer
Unterschrift / elektronische Signatur	Unterschrift / elektronische Signatur