Partner-Vertragspaket

Vertraulichkeit, Informationssicherheit und verantwortliche Zusammenarbeit

SC-PARTNER-1.0 | Stand 18. August 2026

Dieses versionierte Dokument ist die bei der elektronischen Partnerregistrierung verlinkte Vertragsfassung. Jede enthaltene Erklärung wird im Portal einzeln, aktiv und nicht vorausgewählt bestätigt.

Vertragspartner

SecuConCept Torsten Bentlage, Adolf-Grimme-Allee 3, 50829 Koeln, und das im Registrierungsformular eindeutig bezeichnete Partnerunternehmen. Die einreichende Person erklaert, fuer das Partnerunternehmen zur Abgabe der jeweiligen Erklaerungen berechtigt zu sein.

Inhalt

Rechtlicher Status: SecuConCept stellt diese Fassung als verbindliche Portalversion bereit. Eine externe fachanwaltliche Freigabe wurde zum Ausgabestand nicht bestaetigt. Zwingendes Recht, individuelle Vereinbarungen und die auftragsbezogene Pruefung von Haftung, Datenschutzrollen und Sicherheitsanforderungen bleiben vorrangig.

SC-NDA-PARTNER | Version 1.0 | gueltig ab 18.08.2026

Teil A - Gegenseitige Vertraulichkeitsvereinbarung

Die Parteien wollen eine moegliche Zusammenarbeit bei Sicherheits-, Bewachungs- und ergaenzenden Dienstleistungen pruefen, anbahnen und gegebenenfalls durchfuehren. Hierbei koennen sie einander vertrauliche Informationen offenlegen.

1. Zweck

Vertrauliche Informationen duerfen ausschliesslich zur Bewertung, Vorbereitung, Kalkulation und - nach gesonderter Beauftragung - Durchfuehrung der moeglichen Zusammenarbeit verwendet werden. Diese Vereinbarung verpflichtet keine Partei zur Aufnahme, Vergabe oder Annahme eines Auftrags.

2. Vertrauliche Informationen

Vertraulich sind alle nicht allgemein bekannten kaufmaennischen, technischen, organisatorischen, rechtlichen, personenbezogenen, kunden-, objekt- oder sicherheitsbezogenen Informationen, wenn sie als vertraulich gekennzeichnet sind oder ihre Schutzbeduerftigkeit aus Art, Inhalt oder Umstaenden erkennbar ist.

- Kalkulationen, Preise, Angebote, Vertragsentwuerfe und Geschaeftsplanungen
- Kunden-, Lieferanten-, Partner-, Standort- und Ansprechpartnerinformationen
- Objekt-, Einsatz-, Schicht-, Alarmierungs-, Schliess- und Sicherheitsinformationen
- System-, Zugangs-, Risiko-, Prozess- und technische Informationen
- Erlaubnis-, Versicherungs-, Zertifizierungs- und Referenzunterlagen
- Auswertungen, Notizen, Kopien und Zusammenfassungen aus diesen Informationen

3. Ausnahmen

Nicht vertraulich sind Informationen, soweit der Empfaenger nachweist, dass sie ihm bereits rechtmaessig und ohne Geheimhaltungspflicht bekannt waren, ohne Pflichtverletzung allgemein bekannt werden, rechtmaessig von einem berechtigten Dritten stammen, unabhaengig entwickelt oder vorab in Textform freigegeben wurden. Eine nicht allgemein bekannte Zusammenstellung oeffentlicher Einzelinformationen kann weiterhin vertraulich sein.

4. Schutzpflichten

- Nutzung nur fuer den vereinbarten Zweck und Schutz mindestens mit angemessener Sorgfalt.
- Zugriff nur nach Need-to-know fuer verpflichtete Beschaeftigte, Organe, Berater und zugelassene Unterauftragnehmer.
- Kopien, Downloads, lokale Ablagen und Weitergaben auf das Erforderliche begrenzen.
- Angemessene technische und organisatorische Schutzmassnahmen umsetzen.
- Kein Reverse Engineering ueberlassener Software, Muster oder Geraete, soweit eine solche Beschraenkung gesetzlich vereinbart werden darf.
- Tatsaechliche oder vermutete Verluste, Fehluebermittlungen oder unbefugte Zugriffe unverzueglich melden.

5. Gesetzlich erforderliche oder geschuetzte Offenlegung

Eine zwingend gesetzliche, gerichtliche oder behoerdliche Offenlegung bleibt zulaessig. Soweit rechtlich erlaubt, wird die offenlegende Partei vorher informiert und die Offenlegung auf das notwendige Mass beschraenkt. Rechtmaessige Hinweise nach dem Hinweisgeberschutzgesetz, gesetzliche Beteiligungsrechte, Behoerdenkontakte sowie Offenlegungen zur Aufdeckung rechtswidriger Handlungen werden nicht behindert.

6. Personenbezogene Daten

Personenbezogene Daten unterliegen zusaetzlich dem Datenschutzrecht. Diese NDA schafft allein keine Rechtsgrundlage und ersetzt weder eine Rollenpruefung noch eine erforderliche Vereinbarung nach Art. 28 DSGVO.

7. Sicherheitsvorfaelle

Ein Vorfall wird unverzueglich an einkauf@secuconcept.de und bei Datenschutzbezug an datenschutz@secuconcept.de gemeldet. Die Erstmeldung darf nicht bis zur vollstaendigen Aufklaerung verzoegert werden und enthaelt soweit bekannt Zeitpunkt, Art, betroffene Informationen/Systeme, Folgen, Gegenmassnahmen und Kontaktperson.

8. Rueckgabe und Loeschung

Auf Verlangen, bei Ablehnung oder nach Wegfall des Zwecks werden vertrauliche Informationen grundsaetzlich innerhalb von 30 Kalendertagen zurueckgegeben oder sicher geloescht. Ausgenommen bleiben konkret gesetzlich erforderliche Aufbewahrung, technisch nicht einzeln entfernbare regulaere Sicherungskopien bis zur Ueberschreibung und eine zwingend erforderliche Belegkopie zur Rechtsverteidigung. Restbestaende bleiben gesperrt und geschuetzt.

9. Rechte und Laufzeit

Alle Rechte verbleiben beim jeweiligen Rechteinhaber; Lizenzen oder Eigentumsrechte werden nicht uebertragen. Die Pflichten gelten ab dokumentierter Annahme, waehrend der Zusammenarbeit und fuer gewoehnliche vertrauliche Informationen fuenf Jahre nach der letzten Offenlegung. Fuer Geschaeftsgeheimnisse gelten sie, solange die gesetzlichen Schutzvoraussetzungen bestehen.

10. Elektronische Wirksamkeit

SecuConCept stellt diese NDA im Portal als verbindliches Angebot bereit. Sie wird wirksam, wenn eine fuer das Partnerunternehmen berechtigte Person die Dokumentfassung SC-NDA-PARTNER Version 1.0 nach moeglichem Download aktiv bestaetigt und die Registrierung absendet. Dokument-ID, Version, Dokument-Pruefwert, Unternehmen, erklaerende Person, Zeitpunkt und Transaktionsnummer werden protokolliert. Individuelle Vereinbarungen und zwingendes Recht bleiben vorrangig. Fuer besonders sensible Objekt- oder Kundendaten kann vor Offenlegung eine zusaetzliche Gegenzeichnung verlangt werden.

SC-TOM-PARTNER | Version 1.0 | gueltig ab 18.08.2026

Teil B - Technische und organisatorische Mindestmassnahmen

Der Partner schuetzt alle im Zusammenhang mit der Partnerpruefung oder Zusammenarbeit erhaltenen Daten, Dokumente, Systeme und Zugaenge risikogerecht und nach dem Stand der Technik. Die Massnahmen sind Mindestanforderungen und ersetzen keine projektspezifische AVV.

1. Organisation

- Klare Verantwortlichkeiten fuer Informationssicherheit und Datenschutz.
- Dokumentierte Sicherheits-, Berechtigungs-, Loesch-, Backup- und Vorfallprozesse.
- Regelmaessige Risiko- und Schutzbedarfsbewertung sowie mindestens jaehrliche Wirksamkeitspruefung.

2. Personal und Vertraulichkeit

- Zuverlaessige Auswahl, nachweisbare Vertraulichkeitsverpflichtung und regelmaessige Schulung vor Zugriff.
- Geregelte Prozesse bei Eintritt, Aufgabenwechsel und Austritt; nicht mehr benoetigte Zugaenge unverzueglich sperren.

3. Identitaeten und Berechtigungen

- Individuelle Konten, Least Privilege, starke Authentisierung und sichere Kontowiederherstellung.
- Mehrfaktor-Authentisierung fuer administrative, privilegierte und externe Zugaenge sowie Systeme mit vertraulichen Partnerunterlagen, soweit technisch verfuegbar.
- Regelmaessige, dokumentierte Rechtepruefung und getrennte Administrationskonten.

4. Uebermittlung und Speicherung

- Transportverschluesselung nach dem Stand der Technik und risikogerechte Verschluesselung ruhender Daten.
- Keine privaten Messenger, privaten Cloudspeicher, offenen Dauerlinks oder ungeschuetzten E-Mail-Anhaenge fuer vertrauliche Unterlagen.
- Besonders sensible Objekt-, Alarm- oder Zugangsdaten nur ueber ausdruecklich freigegebene Kanaele.

5. Systeme und Anwendungen

- Unterstuetzte Systeme, zeitnahe Sicherheitsupdates, sichere Basiskonfiguration, Schwachstellen- und Malware-Schutz.
- Trennung von Test- und Produktivdaten sowie Segmentierung nach Schutzbedarf.
- Dateiuploads nur mit erlaubten Typen, Groessen, Speicherorten und serverseitiger Validierung.

6. Protokollierung

- Sicherheitsrelevante Anmeldungen, Rechteaenderungen, Dateiabrufe, Administrationshandlungen und Fehlversuche angemessen protokollieren.
- Protokolle vor Veraenderung schuetzen, zweckgebunden begrenzen und risikobasiert auswerten.

7. Verfuegbarkeit

- Regelmaessige, verschluesselte und logisch getrennte Sicherungen sowie dokumentierte Wiederherstellungs- und Notfallverfahren.
- Wiederherstellungstests und Schutz gegen unbeabsichtigte Loeschung, Schadsoftware und Systemausfall.

8. Loeschung

- Dokumentierter Aufbewahrungs- und Loeschplan, sichere Datentraegervernichtung und Loeschbestaetigung auf begruendete Anfrage.

9. Sicherheits- und Datenschutzvorfaelle

- Dokumentierter Prozess zur Erkennung, Eindammung, Untersuchung, Beweissicherung, Meldung und Nachbereitung.
- Vorfalle mit Bezug zu SecuConCept unverzueglich, als vertragliches Fruehwarnziel moeglichst binnen 24 Stunden nach Bekanntwerden, melden. Gesetzliche Fristen bleiben unberuehrt.

10. Unterauftragnehmer

- Vorherige Risiko-, Datenschutz- und Sicherheitspruefung, gleichwertige Verpflichtung und transparente Benennung.
- Bei Auftragsverarbeitung gelten zusaetzlich Art. 28 Abs. 2 und 4 DSGVO.

11. Nachweise und Pruefung

- Auf begruendete, risikobasierte Anfrage geeignete TOM, Frageboegen, Zertifikate, Audit-Zusammenfassungen, Schulungs-, Rechte- und Wiederherstellungsnachweise bereitstellen.
- Abweichungen offenlegen, mit Massnahmenplan versehen und innerhalb abgestimmter Frist beheben.

12. Aenderungen

- Massnahmen duerfen durch gleichwertige oder bessere ersetzt werden. Wesentliche Verringerungen des Schutzniveaus, neue Speicherlaender oder kritische Unterauftragnehmer werden vorab mitgeteilt.

SC-CODE-PARTNER | Version 1.0 | gueltig ab 18.08.2026

Teil C - Partner- und Lieferantenkodex

Dieser Kodex definiert die Mindestanforderungen an potenzielle und bestehende Partner, Nachunternehmer und Lieferanten von SecuConCept. Einzelauftraege koennen strengere Anforderungen vorsehen.

1. Gesetzestreue und Voraussetzungen

- Alle anwendbaren Gesetze, Behoerdenauflagen und Genehmigungen einhalten.
- Erforderliche Gewerbeerlaubnisse, Registrierungen, Versicherungen und Qualifikationen waehrend der Zusammenarbeit aktuell halten.
- Ablauf, Widerruf, Ruhen oder wesentliche Aenderungen unverzueglich mitteilen.
- Fuer Bewachungsleistungen insbesondere § 34a GewO und Bewachungsverordnung beachten.

2. Integritaet

- Keine Bestechung, Bestechlichkeit, unzulaessige Vorteilsgewaehrung, Erpressung oder wettbewerbswidrige Absprache.
- Keine Bargeldgeschenke; Einladungen und Aufmerksamkeiten nur transparent, angemessen und ohne Entscheidungsbezug.
- Interessenkonflikte und Nebenabreden offenlegen; nachvollziehbare Geschaeftsunterlagen fuehren.

3. Beschaeftigte

- Mindestlohn-, Arbeitszeit-, Sozialversicherungs-, Arbeitnehmerueberlassungs-, Entsende- und Arbeitsschutzregeln einhalten.
- Keine Schwarzarbeit, illegale Beschaeftigung, Diskriminierung, Belaestigung, Zwangs- oder Kinderarbeit und kein Menschenhandel.
- Nur geeignete, zuverlaessige, qualifizierte und ordnungsgemaess eingewiesene Personen einsetzen.

4. Menschenrechte und Umwelt

- Menschenrechtliche und umweltbezogene Risiken angemessen vermeiden, Abhilfe schaffen und relevante Unterauftragnehmer einbeziehen, ohne eine nicht bestehende gesetzliche LkSG-Anwendbarkeit zu behaupten.
- Ressourcen verantwortungsvoll einsetzen und sichere, wirtschaftlich vertretbare Umweltmassnahmen foerdern.

5. Datenschutz und Sicherheit

- Personenbezogene Daten nur rechtmaessig, zweckgebunden und minimiert verarbeiten.
- NDA und TOM einhalten, Vorfaelle unverzueglich melden und Drittlandofflegungen nur bei erfuellten Voraussetzungen vornehmen.
- Fotos, Referenznennungen und Veroeffentlichungen mit Kunden- oder Objektbezug nur nach Freigabe.

6. Unterauftragnehmer

- Einsatz nur entsprechend Hauptvertrag und Freigabeanforderungen; Eignung, Zuverlaessigkeit, Versicherung und Sicherheit pruefen.
- Massgebliche Pflichten weitergeben und fuer ordnungsgemaesse Leistung verantwortlich bleiben.

7. Hinweise, Abweichungen und Abhilfe

- Verstoesse, Verdachtsfaelle, Interessenkonflikte und Erlaubnisprobleme vertraulich an einkauf@secuconcept.de melden.
- Keine Benachteiligung rechtmaessiger Hinweise; NDA und Kodex verhindern keine geschuetzten Meldungen oder Behoerdenkontakte.
- Festgestellte Abweichungen offen kommunizieren und fristgerecht beheben. Schwere oder wiederholte Verstoesse koennen zur Ablehnung, Sperrung oder Beendigung fuehren; gesetzliche Rechte bleiben unberuehrt.

SC-AVV-ROLECHECK | Version 1.0 | gueltig ab 18.08.2026

Teil D - Rollenpruefung und Auftragsverarbeitung

NDA, TOM und Kodex ersetzen niemals eine erforderliche Vereinbarung zur Auftragsverarbeitung. Datenschutzrollen werden pro Einzelauftrag vor dem ersten produktiven Zugriff bestimmt.

1. Entscheidungsschema

- Keine personenbezogenen Daten fuer SecuConCept: regelmaessig keine AVV.
- Ausschliessliche Verarbeitung nach dokumentierten Weisungen von SecuConCept: regelmaessig Auftragsverarbeitung; AVV vor Zugriff.
- Eigene Zwecke oder wesentliche Mittel aufgrund eigener Verantwortung: regelmaessig eigenstaendige Verantwortlichkeit; Rechtsgrundlage und Transparenz pruefen.
- Gemeinsame Bestimmung von Zwecken und wesentlichen Mitteln: moegliche gemeinsame Verantwortlichkeit nach Art. 26 DSGVO.
- Unklare Rolle: keine Datenfreigabe bis zur dokumentierten Datenschutzpruefung.

2. Mindestprozess

- Rollen, Zwecke und Weisungsrahmen bestimmen.
- Datenarten, betroffene Personen, Systeme, Empfaenger, Loeschfristen und Drittlandbezuege dokumentieren.
- Konkrete TOM und Unterauftragnehmer risikobasiert pruefen.
- Soweit Art. 28 DSGVO greift, vor Leistungsbeginn eine AVV mit allen Pflichtinhalten abschliessen.

3. Verbindliche Erklaerung

Der Partner beginnt keine Verarbeitung personenbezogener Daten im Auftrag von SecuConCept, bevor die Rollenpruefung abgeschlossen und - falls erforderlich - eine wirksame AVV einschliesslich konkreter Weisungen, TOM, Unterauftragnehmerregelung, Unterstuetzungs-, Pruef-, Rueckgabe- und Loeschpflichten abgeschlossen ist. Die Registrierung erteilt keine Weisung und ersetzt keinen Einzelauftrag.

SC-REGISTRATION-TERMS | Version 1.0 | gueltig ab 18.08.2026

Teil E - Registrierungs- und Portalbedingungen

Diese Bedingungen regeln die unverbindliche Einreichung und Pruefung einer moeglichen B2B-Partnerschaft sowie die Nutzung des geschuetzten Partnerportals. Sie ersetzen keine Einzelauftragsbedingungen.

1. Betreiber und B2B-Ausrichtung

Betreiber ist SecuConCept Torsten Bentlage, Adolf-Grimme-Allee 3, 50829 Koeln. Das Portal richtet sich ausschliesslich an Unternehmen und deren vertretungs- oder einreichungsberechtigte Personen.

2. Zweck

Die Registrierung ermoeglicht die strukturierte Eignungspruefung. Sie ist kein Auftrag, keine Zusage, keine Ausschreibung und kein Abschluss eines Partner- oder Einzelvertrags.

3. Berechtigung und Richtigkeit

Die einreichende Person bestaetigt ihre Berechtigung. Angaben und Unterlagen muessen aktuell, vollstaendig und sachlich richtig sein. Wesentliche Aenderungen sind unverzueglich mitzuteilen; ein Nachweis der Berechtigung kann angefordert werden.

4. Unterlagen

Es duerfen nur erforderliche, rechtmaessig verfuegbare Unternehmensunterlagen hochgeladen werden. Nicht erforderliche Personendaten sind zu schwaerzen; Rechte Dritter, Geschaeftsgeheimnisse und Upload-Hinweise sind zu beachten.

5. Pruefung

SecuConCept darf Angaben und Nachweise auf Plausibilitaet, Gueltigkeit und Eignung pruefen, Rueckfragen stellen und weitere erforderliche Nachweise anfordern. Entscheidungen erfolgen nicht ausschliesslich automatisiert.

6. Kein Anspruch

Es besteht kein Anspruch auf Aufnahme, Rueckmeldung binnen bestimmter Frist, Exklusivitaet, Mindestvolumen oder Auftrag. Leistungsumfang und Verguetung werden spaeter gesondert vereinbart.

7. Geschuetzter Zugang

Der Zugang wird dem bei der Registrierung verwendeten Geschaeftskonto zugeordnet. Sitzungen und Konten sind zu schuetzen; erkennbarer Missbrauch ist unverzueglich mitzuteilen.

8. Auftragsanfragen

Portal-Anfragen sind vertraulich und nur fuer den zugeordneten Partner bestimmt. Angaben zu Einsatzorten, Zeiten, Kunden und Anforderungen duerfen nicht unbefugt verwendet oder weitergegeben werden.

9. Angebote

Angebote muessen Preis, Verfuegbarkeit, Personalansatz und Konzept richtig wiedergeben. Einreichen begruendet keine Beauftragung; Annahme und Auftrag werden gesondert bestaetigt.

10. Vertragspaket

NDA, TOM, Kodex, AVV-Rollenhinweis und diese Bedingungen werden einzeln bestaetigt. Dokument-ID, Version, Dokument-Pruefwert, Unternehmen, erklaerende Person, Zeitpunkt und Transaktionsnummer werden gespeichert.

11. Datenschutz

Es gelten die zum Zeitpunkt der Registrierung bereitgestellten Datenschutzhinweise. Die Kenntnisnahme ist keine pauschale Einwilligung. Eine optionale Partnerpool-Einwilligung bleibt freiwillig und widerrufbar.

12. Kuenftige Aenderungen

Aenderungen gelten nicht rueckwirkend. Wesentliche neue Pflichten erfordern eine neue aktive Bestaetigung. Individuelle Vereinbarungen und zwingendes Recht bleiben vorrangig.

Nachweis und Quellen

Elektronischer Annahmenachweis

Das Portal speichert zu jeder Pflichtbestaetigung Unternehmen, Rechtsform, einreichende Person, Funktion, Geschaefts-E-Mail, Dokument-ID, Version, Dokument-Pruefwert, exakten Bestaetigungszeitpunkt, Vorgangsnummer und einen kryptografischen Ereignis-Pruefwert. Die Dokumentfassung wird vor Abgabe zum Download bereitgestellt. Die Kenntnisnahme der Datenschutzhinweise wird getrennt von Vertragserklaerungen erfasst.

Wesentliche offizielle Grundlagen

- DSGVO: https://eur-lex.europa.eu/eli/reg/2016/679/oj/?locale=de
- EU-Standardvertragsklauseln nach Art. 28: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0915
- Geschaeftsgeheimnisgesetz: https://www.gesetze-im-internet.de/geschgehg/
- Hinweisgeberschutzgesetz: https://www.gesetze-im-internet.de/hinschg/
- BGB zu Form, AGB und Verjaehrung: https://www.gesetze-im-internet.de/bgb/
- Gewerbeordnung § 34a: https://www.gesetze-im-internet.de/gewo/__34a.html
- Bewachungsverordnung: https://www.gesetze-im-internet.de/bewachv_2019/
- BSI IT-Grundschutz: https://www.bsi.bund.de/grundschutz

Betriebshinweis: SecuConCept dokumentiert und ueberprueft Identitaet und Vertretung, elektronische Abschlusslogik, bestaendige Vertragskopie, Datenschutzinformation, eingesetzte Auftragsverarbeiter, Malware-Pruefung, Rollen und Berechtigungen, Loeschtests sowie den konkreten AVV-Prozess. Festgestellte Abweichungen werden vor der betroffenen Verarbeitung behoben.

Dokumentpaket SC-PARTNER-1.0 | Stand 18. August 2026