PROCEVIA

PROZESSMODELLIERUNG · MADE IN GERMANY

VERTRAULICH · VERTRAGSDOKUMENT

Auftrags-verarbeitungs-vertrag

gemäß Art. 28 DSGVO

Version	**1.5**
Stand	**Juli 2026**
Geltungsbereich	**Procevia SaaS-Plattform**
Vertragsabschluss	**Elektronisch (Art. 28 Abs. 9 DSGVO), eigenhändige Unterschrift nicht erforderlich**

Procevia GmbH
Geschäftsführer: Iordanis Kleinöder Stafidis
Linder Weg 115, 51147 Köln, Deutschland
HRB 128157 · AG Köln

legal@procevia.de
procevia.de

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

dem Kunden (nachfolgend „**Verantwortlicher**"), dessen Angaben (Firma, Anschrift, vertretungsberechtigte Person) sich aus den bei der Registrierung angegebenen und im Nutzerkonto hinterlegten Stammdaten ergeben,

FIRMA / ORGANISATION DES VERANTWORTLICHEN

Vollständige Angaben zum Verantwortlichen siehe „Angaben der Vertragsparteien„ am Ende dieses Vertrags.

und

Procevia GmbH
Geschäftsführer: Iordanis Kleinöder Stafidis
Linder Weg 115, 51147 Köln, Deutschland
Eingetragen im Handelsregister beim Amtsgericht Köln, HRB 128157
E-Mail: legal@procevia.de

(nachfolgend „**Auftragsverarbeiter**").

Stand: Juli 2026

Präambel

1. Der Verantwortliche nutzt die von Procevia bereitgestellte SaaS-Plattform „Procevia" gemäß den Allgemeinen Geschäftsbedingungen (nachfolgend „**Haupt-AGB**"). Im Rahmen dieser Nutzung verarbeitet der Auftragsverarbeiter personenbezogene Daten, für die der Verantwortliche datenschutzrechtlich verantwortlich ist (Art. 4 Nr. 7 DSGVO).
2. Dieser Auftragsverarbeitungsvertrag (nachfolgend „**AVV**") konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien gemäß Art. 28 DSGVO. Er gilt für sämtliche Tätigkeiten des Auftragsverarbeiters im Zusammenhang mit der Haupt-AGB, bei denen Beschäftigte, Hilfspersonen oder Subunternehmer des Auftragsverarbeiters mit personenbezogenen Daten des Verantwortlichen in Berührung kommen.
3. Dieser AVV wird bei Vertragsschluss zwischen Verantwortlichem und Auftragsverarbeiter nach den Haupt-AGB automatisch Bestandteil des Vertrages, ohne dass es einer gesonderten Unterzeichnung bedarf.

---

§ 1 Gegenstand und Dauer des Auftrags

1. **Gegenstand** des Auftrags ist die Erbringung der in den Haupt-AGB beschriebenen SaaS-Leistungen der Procevia-Plattform, insbesondere die KI-gestützte Erstellung, Bearbeitung, Speicherung und Bereitstellung von BPMN-Prozessdiagrammen und damit verbundenen Prozessdokumentationen.
2. Die **Dauer** des Auftrags entspricht der Laufzeit des Hauptvertrages gemäß § 4 der Haupt-AGB. Dieser AVV endet automatisch mit Beendigung des Hauptvertrages.

---

§ 2 Art und Zweck der Verarbeitung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Verantwortlichen zu folgenden Zwecken:

a. Bereitstellung und Betrieb der Procevia-Plattform und der darin enthaltenen Funktionen,

b. Übermittlung der vom Verantwortlichen über die Plattform eingegebenen Kundeninhalte (Texteingaben, hochgeladene Dokumente, Diagramm-Inhalte) an Subauftragsverarbeiter zum Zweck der KI-gestützten Generierung und Bearbeitung von BPMN-Prozessdiagrammen,
c. Speicherung von Nutzerinhalten und Kontodaten auf Servern innerhalb der EU,
d. Verwaltung von Workspaces, Team-Einladungen und Scout-Links für externe Interview-Teilnehmer,
e. Support und Fehlerbehebung im Rahmen der Haupt-AGB.

2. Art der Verarbeitung: Erheben, Erfassen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleichen oder Verknüpfen, Einschränken, Löschen oder Vernichten, jeweils gemäß Art. 4 Nr. 2 DSGVO.
3. **Datenminimierung bei externen KI-Diensten.** Bei der Übermittlung von Kundeninhalten an Subauftragsverarbeiter für KI-gestützte Funktionen gemäß Abs. 1 lit. b übermittelt der Auftragsverarbeiter ausschließlich die vom Verantwortlichen über die Plattform eingegebenen Inhalte. Eine Anreicherung der Kundeninhalte mit Stammdaten, Nutzungsdaten oder sonstigen personenbezogenen Daten aus dem Bestand des Auftragsverarbeiters vor der Übermittlung erfolgt nicht.

---

§ 3 Art der personenbezogenen Daten

Vom Auftrag umfasst sind insbesondere folgende Kategorien personenbezogener Daten:

a. **Stammdaten** (Name, E-Mail-Adresse, ggf. Firmenname, Rolle im Workspace),
b. **Kommunikationsdaten** (Chat-Nachrichten, Support-Anfragen),
c. **Inhaltsdaten** (vom Verantwortlichen eingegebene Prozessbeschreibungen, hochgeladene Dokumente, erzeugte BPMN-Diagramme; soweit diese Inhalte personenbezogene Daten Dritter enthalten, stammen diese ausschließlich aus den Eingaben des Verantwortlichen),
d. **Nutzungs- und Verbindungsdaten** (IP-Adressen, Browser-Informationen, Zugriffszeiten, Interaktionslogs),
e. **Zahlungsdaten** (nur zahlungsbezogene Referenzdaten; die eigentliche Zahlungsabwicklung erfolgt über Stripe als separaten Verantwortlichen, nicht als Subauftragsverarbeiter).

---

§ 4 Kategorien betroffener Personen

1. Vom Auftrag umfasst sind insbesondere:

a. Beschäftigte und autorisierte Nutzer des Verantwortlichen (Workspace-Mitglieder),
b. externe Interview-Teilnehmer, die vom Verantwortlichen über einen Scout-Link zur Teilnahme eingeladen werden,
c. in den Nutzerinhalten des Verantwortlichen genannte oder beschriebene Dritte (z. B. in Prozessbeschreibungen genannte Personen).

2. **Scout-Link-Teilnehmer und Verantwortlichkeit.** Externe Interview-Teilnehmer gemäß Abs. 1 lit. b werden ausschließlich vom Verantwortlichen über die Plattform-Funktion „Scout-Link" zur Teilnahme eingeladen. Der Auftragsverarbeiter spricht keine Einladungen aus eigener Initiative aus und steht in keinem unmittelbaren Vertragsverhältnis zu den externen Teilnehmern. Die datenschutzrechtliche Verantwortlichkeit gemäß Art. 4 Nr. 7 DSGVO für die Beziehung zwischen dem Verantwortlichen und den externen Teilnehmern verbleibt beim Verantwortlichen.
3. **Information externer Teilnehmer.** Vor Beginn der Eingabe von Antworten erhalten externe Teilnehmer über die Plattform Zugang zu den Allgemeinen Geschäftsbedingungen sowie zur Datenschutzerklärung des Auftragsverarbeiters und bestätigen deren Kenntnisnahme. Der Auftragsverarbeiter dokumentiert die Bestätigung mit Zeitstempel und Versionsstand der jeweiligen Dokumente. Die Bestätigung der Teilnehmer bezieht sich auf die Nutzung der Plattform des Auftragsverarbeiters; die datenschutzrechtliche Information der Teilnehmer über Zwecke und Um-

stände der Prozessaufnahme selbst obliegt dem Verantwortlichen gemäß Abs. 2, etwa im Rahmen der Einladung.

§ 5 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen, soweit er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist.
2. Der Auftragsverarbeiter stellt sicher, dass alle Personen, die zur Verarbeitung befugt sind, zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
3. Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (siehe § 11 und Anlage 1 zu diesem AVV).
4. Der Auftragsverarbeiter unterstützt den Verantwortlichen soweit möglich bei der Erfüllung seiner Pflichten gemäß Art. 32 bis 36 DSGVO, insbesondere hinsichtlich Datensicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und Konsultation der Aufsichtsbehörde.
5. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung von Anträgen Betroffener gemäß Kapitel III DSGVO (Art. 12 bis 22 DSGVO) durch geeignete technische und organisatorische Maßnahmen. Auf Unterstützungsersuchen des Verantwortlichen im Zusammenhang mit Anträgen Betroffener reagiert der Auftragsverarbeiter unverzüglich, spätestens innerhalb von fünf Arbeitstagen. Soweit der Verantwortliche Betroffenenanfragen selbst über die Plattform-Funktionen (Export, Löschung) erfüllen kann, obliegt ihm die Erfüllung primär selbst.
6. Der Auftragsverarbeiter übergibt dem Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen alle ihm überlassenen personenbezogenen Daten auf Wunsch oder löscht sie, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht (§ 9 dieses AVV).
7. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt.
8. Die Informationspflicht nach Abs. 7 begründet keine Verpflichtung des Auftragsverarbeiters zur Rechtsberatung. Die Prüfung der datenschutzrechtlichen Zulässigkeit einer Weisung obliegt weiterhin dem Verantwortlichen.
9. Ansprechpartner des Auftragsverarbeiters für Datenschutzangelegenheiten ist für den Verantwortlichen erreichbar unter legal@procevia.de. Anträge betroffener Personen auf Ausübung ihrer Rechte nach Kapitel III DSGVO richten sich an den Verantwortlichen, dem ihre Erfüllung obliegt (§ 5 Abs. 5); dies gilt auch für die vom Verantwortlichen eingeladenen Nutzer (Workspace-Mitglieder), die der Verantwortliche selbst verwaltet. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an den Verantwortlichen weiter und beantwortet ihn nur nach Rücksprache mit dem Verantwortlichen.

§ 6 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die datenschutzrechtliche Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen allein verantwortlich.
2. Der Verantwortliche stellt sicher, dass die Mitwirkungspflichten gemäß § 6 Haupt-AGB (insbesondere Verbot der Eingabe besonderer Kategorien personenbezogener Daten, Berufsgeheimnisse, Geschäftsgeheimnisse Dritter ohne Einwilligung) eingehalten werden.
3. Der Verantwortliche erteilt dem Auftragsverarbeiter die notwendigen Weisungen zur Erbringung der Verarbeitungsleistung. Die Erteilung der Weisungen erfolgt grundsätzlich durch die Nutzung

der Plattform-Funktionen und die in den Haupt-AGB vereinbarten Prozesse. Ergänzende Weisungen können in Textform erteilt werden.

§ 7 Weisungsrechte

1. Weisungen werden primär durch den Verantwortlichen oder von ihm autorisierte Personen über die Plattform-Funktionen erteilt (z. B. Upload, Generierung, Löschung von Inhalten).
2. Ergänzende Weisungen sind in Textform an legal@procevia.de zu richten.

§ 8 Subauftragsverarbeiter

1. **Begriff.** Subauftragsverarbeiter im Sinne dieses AVV sind ausschließlich Stellen, die im Auftrag des Auftragsverarbeiters personenbezogene Daten des Verantwortlichen verarbeiten (Art. 4 Nr. 8 DSGVO). Dienstleister, deren Tätigkeit keine Verarbeitung personenbezogener Daten des Verantwortlichen umfasst (z. B. Code-Hosting, Build- und Entwicklungs-Werkzeuge, anonymisierte Telemetrie, interne Office-Software), sind keine Subauftragsverarbeiter und unterliegen nicht den Pflichten dieses § 8.
2. Der Auftragsverarbeiter ist berechtigt, Subauftragsverarbeiter einzusetzen. Der Verantwortliche erteilt mit Abschluss dieses AVV eine allgemeine Genehmigung zur Hinzuziehung der in Anlage 2 zu diesem AVV aufgeführten Subauftragsverarbeiter.
3. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung anderer Subauftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Die Mitteilung erfolgt per E-Mail an die im Account hinterlegte administrative Kontakt-E-Mail-Adresse, spätestens vier Wochen vor Wirksamwerden der Änderung.
4. **Notfallklausel.** In dringenden Fällen, insbesondere wenn der Wechsel oder die Hinzuziehung eines Subauftragsverarbeiters aus Sicherheits-, Verfügbarkeits- oder rechtlichen Gründen sofort erforderlich ist (z. B. Ausfall eines bestehenden Subauftragsverarbeiters, behördliche Anordnung, akute Sicherheitslücke), kann die Frist nach Abs. 3 auf das technisch und rechtlich erforderliche Mindestmaß verkürzt werden. Der Auftragsverarbeiter informiert den Verantwortlichen in einem solchen Fall unverzüglich nachträglich unter Angabe der Gründe für die Fristverkürzung.
5. Erhebt der Verantwortliche innerhalb der Frist nach Abs. 3 berechtigten Einspruch, ist der Auftragsverarbeiter berechtigt, den betroffenen Teilvertrag außerordentlich zu kündigen, wenn der Einsatz des Subauftragsverarbeiters für die Erbringung der Leistung wesentlich ist.
6. Der Auftragsverarbeiter verpflichtet jeden Subauftragsverarbeiter in einem schriftlichen Vertrag zu denselben Datenschutzpflichten, die ihm selbst durch diesen AVV auferlegt werden.
7. Die in Abs. 3 und 5 geregelten Informations-, Einspruchs- und Kündigungsrechte gelten nicht für Subauftragsverarbeiter, die ausschließlich im Zusammenhang mit optionalen Funktionen oder Features der Plattform eingesetzt werden, deren Nutzung dem Verantwortlichen freisteht. Aktiviert der Verantwortliche eine solche optionale Funktion, gilt dies als Zustimmung zur Hinzuziehung der damit verbundenen Subauftragsverarbeiter gemäß Anlage 2. Solche ausschließlich für optionale Funktionen eingesetzten Subauftragsverarbeiter werden in Anlage 2 gesondert als optional gekennzeichnet; derzeit fällt kein Subauftragsverarbeiter unter diese Regelung.

§ 9 Löschung und Übergabe

1. Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Ausgenommen sind Sicherheitskopien (Backups), soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2. Nach Abschluss der vertraglichen Arbeiten (insbesondere nach Beendigung des Hauptvertrages) hat der Auftragsverarbeiter die ihm überlassenen oder für den Verantwortlichen erzeugten Daten nach Wahl des Verantwortlichen entweder zu übergeben oder datenschutzkonform zu löschen. Die Übergabe erfolgt nach Maßgabe von § 5a Haupt-AGB (EU Data Act).
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

---

§ 10 Meldepflichten

1. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 36 Stunden nach Kenntnisnahme einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 33 DSGVO. Weitere relevante Erkenntnisse werden fortlaufend und unaufgefordert nachgemeldet.
2. Die Benachrichtigung enthält, soweit verfügbar:

a. eine Beschreibung der Art der Verletzung (Art der Daten, Kategorie und Anzahl der Betroffenen, Kategorie und Anzahl betroffener Datensätze),
b. Name und Kontaktdaten des beim Auftragsverarbeiter zuständigen Ansprechpartners,
c. wahrscheinliche Folgen der Verletzung,
d. die getroffenen oder vorgeschlagenen Maßnahmen zur Eindämmung der Folgen.

---

§ 11 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, die in **Anlage 1** zu diesem AVV konkretisiert sind. Der Auftragsverarbeiter überprüft die TOMs regelmäßig und passt sie an den Stand der Technik an.

---

§ 12 Kontrollrechte des Verantwortlichen

1. **Nachweis durch Compliance-Dokumentation.** Der Auftragsverarbeiter weist die Einhaltung seiner Pflichten aus diesem AVV nach durch Vorlage geeigneter Compliance-Dokumentation (nachfolgend „**Compliance-Dokumentation**"). Dazu zählen insbesondere:

a. Zertifikate und Testate unabhängiger Dritter (beispielsweise ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, C5) seiner Subauftragsverarbeiter,
b. interne Dokumentationen wie das Verzeichnis von Verarbeitungstätigkeiten, die technischen und organisatorischen Maßnahmen gemäß Anlage 1 sowie das Löschkonzept.

Die Compliance-Dokumentation wird dem Verantwortlichen auf angemessene Anfrage bereitgestellt und gilt regelmäßig als ausreichender Nachweis für die Einhaltung der Pflichten des Auftragsverarbeiters.

2. **Vor-Ort-Audit.** Ergänzend zum Nachweis durch Compliance-Dokumentation ist der Verantwortliche berechtigt, ein Vor-Ort-Audit (nachfolgend „**Audit**") durchzuführen:

a. einmal je Vertragsjahr nach schriftlicher Ankündigung mit einer Frist von mindestens vier Wochen, sowie
b. darüber hinaus anlassbezogen und ohne Bindung an Häufigkeit und Frist nach lit. a, wenn dokumentierte Anhaltspunkte einen begründeten Verdacht auf einen erheblichen Verstoß gegen diesen AVV begründen, beim Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 33 DSGVO eingetreten ist oder eine Prüfung von der zuständigen Aufsichtsbehörde des Verantwortlichen verlangt wird.

3. **Bedingungen des Audits.**

a. Der Umfang des Audits ist strikt auf die Überprüfung der Einhaltung der konkret betroffenen Pflicht beschränkt.
b. Das Audit wird während der üblichen Geschäftszeiten durchgeführt; der Betrieb des Auftragsverarbeiters darf dabei nicht unverhältnismäßig beeinträchtigt werden. Im Fall des Abs. 2 lit. b kann die Ankündigungsfrist auf das erforderliche Maß verkürzt werden.
c. Das Audit wird durch den Verantwortlichen selbst (beispielsweise durch dessen Datenschutzbeauftragten) oder durch einen von ihm beauftragten Dritten durchgeführt. Prüfende Personen dürfen keine Wettbewerber des Auftragsverarbeiters sein und müssen einer angemessenen Geheimhaltungspflicht unterliegen.
d. Jede Partei trägt die ihr durch das Audit entstehenden eigenen Kosten. Bei Audits nach Abs. 2 lit. a erstattet der Verantwortliche dem Auftragsverarbeiter dessen angemessenen Unterstützungsaufwand. Ergibt ein Audit einen erheblichen Verstoß des Auftragsverarbeiters gegen diesen AVV, trägt der Auftragsverarbeiter den angemessenen Aufwand des Audits.

4. **Gesetzliche Kontrollrechte.** Die Regelungen dieses § 12 schränken gesetzliche Kontrollrechte der Aufsichtsbehörden nach Art. 58 DSGVO nicht ein.

---

§ 13 Drittlandtransfer

1. **Grundsatz der EU/EWR-Verarbeitung.** Der Auftragsverarbeiter verarbeitet personenbezogene Daten grundsätzlich innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) sowie in Staaten, für die die Europäische Kommission ein angemessenes Datenschutzniveau festgestellt hat (Angemessenheitsbeschluss gemäß Art. 45 DSGVO).
2. **Geeignete Garantien.** Eine Übermittlung personenbezogener Daten an Subauftragsverarbeiter in Drittländern ohne Angemessenheitsbeschluss erfolgt nur auf Grundlage geeigneter Garantien gemäß Kapitel V DSGVO, insbesondere

a. Standardvertragsklauseln der Europäischen Kommission (Art. 46 Abs. 2 lit. c DSGVO), gegebenenfalls ergänzt durch zusätzliche Schutzmaßnahmen nach Maßgabe eines Transfer Impact Assessments, oder
b. sonstiger Garantien nach Art. 46 DSGVO.

Die aktuell geltenden Garantien für die in Anlage 2 aufgeführten Subauftragsverarbeiter werden dem Verantwortlichen auf Anfrage benannt.

3. **Fortbestand der Schutzmaßnahmen.** Sollte eine der vorstehenden Schutzmaßnahmen nach Auffassung der Europäischen Kommission, des Europäischen Datenschutzausschusses oder eines zuständigen Gerichts nicht mehr ausreichen, um das angemessene Schutzniveau gemäß Kapitel V DSGVO zu gewährleisten, unternimmt der Auftragsverarbeiter wirtschaftlich vertretbare Anstrengungen, eine andere geeignete Schutzmaßnahme einzuführen oder stellt die betreffende Übermittlung ein.

---

§ 14 Haftung

Für die Haftung der Parteien gelten die Regelungen gemäß Art. 82 DSGVO sowie ergänzend § 18 der Haupt-AGB. Die Verteilung der Haftung untereinander richtet sich im Übrigen nach dem Verursachungsbeitrag der Parteien.

---

§ 15 Schlussbestimmungen

1. Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien ersetzen unwirksame Bestimmungen durch solche, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommen.
2. Änderungen dieses AVV bedürfen der Textform.

3. Bei Widersprüchen zwischen diesem AVV und der Haupt-AGB gehen die Regelungen dieses AVV im Bereich der Verarbeitung personenbezogener Daten vor.
4. Es gilt deutsches Recht.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Diese Anlage fasst die wesentlichen technischen und organisatorischen Maßnahmen zusammen und definiert den vertraglich zugesicherten Mindeststandard. Die jeweils aktuelle, konkretere Umsetzung ergibt sich aus dem TOM-Dokument des Auftragsverarbeiters, das als Compliance-Dokumentation gemäß § 12 bereitgestellt wird.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle Die Server des Auftragsverarbeiters werden in zertifizierten Rechenzentren innerhalb der EU betrieben (Amazon Web Services EMEA SARL; Primärregion Paris für sämtliche Kundendaten, Region Irland ausschließlich für den E-Mail-Eingang). Diese Rechenzentren sind nach ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3 sowie C5 (BSI) zertifiziert. Physischer Zutritt erfolgt ausschließlich durch autorisiertes Personal von AWS. Die Arbeitsplätze des Auftragsverarbeiters sind mit vollverschlüsselten, personengebundenen Endgeräten ausgestattet (Full-Disk-Encryption, automatische Bildschirmsperre). Personenbezogene Daten des Verantwortlichen werden nicht lokal auf Endgeräten vorgehalten; der Zugriff erfolgt ausschließlich über die gesicherten Cloud-Systeme. Eine papiergebundene Verarbeitung findet nicht statt.

1.2 Zugangskontrolle

- Zugriff auf die Plattform erfolgt ausschließlich authentifiziert, entweder passwortgeschützt oder per Single Sign-On über den Identitätsanbieter des Nutzers (dabei greift dessen Mehrfaktor-Richtlinie).
- Passwort-Mindestanforderungen gemäß BSI-Empfehlung (Länge, Komplexität).
- Administrative Zugänge des Auftragsverarbeiters sind mit Zwei-Faktor-Authentifizierung gesichert.
- Session-Timeout bei Inaktivität.

1.3 Zugriffskontrolle

- Rollen- und rechtebasierte Zugriffskontrolle (Admin, Editor, Viewer im Workspace).
- Mitarbeiter des Auftragsverarbeiters erhalten Zugriff nur im erforderlichen Umfang und nur nach expliziter Autorisierung („Need-to-know"-Prinzip).
- Protokollierung administrativer Zugriffe.

1.4 Trennungskontrolle

- Logische Trennung der Kundendaten im Multi-Tenant-System.
- Eindeutige Kennung pro Workspace und Account.
- Strikt getrennte AWS-Accounts beziehungsweise Ressourcen-Scopes für die einzelnen Stages (siehe Ziffer 1.6).

1.5 Pseudonymisierung Wo die Leistungserbringung es zulässt, arbeitet der Auftragsverarbeiter mit pseudonymen technischen Kennungen statt Klardaten, insbesondere mit internen Nutzer- und Mandanten-Kennungen sowie einem Fehler- und Performance-Monitoring ohne Klaridentitäten. Vom Verantwortlichen eingegebene Inhaltsdaten werden zur Leistungserbringung nicht pseudonymisiert, da ihre inhaltliche Gestalt vom Verantwortlichen bestimmt wird.

1.6 Entwicklungs- und Testumgebungen (Drei-Stage-Architektur)

- Procevia betreibt drei strikt voneinander getrennte Umgebungen: **Entwicklung (Dev)**, **Vorabnahme (Staging)** und **Produktion (Prod)**. Jede Stage hat eigene Infrastruktur (AWS-Konten beziehungsweise Ressourcen-Scopes), eigene Datenbankinstanzen, eigene Zugriffsrollen und ein eigenes Set an API-Schlüsseln.
- In den Umgebungen **Dev** und **Staging** werden *keine produktiven Kundendaten* verarbeitet. Es kommen ausschließlich synthetische Demo- und Testdaten zum Einsatz, die von Procevia selbst erzeugt werden und keinen Personenbezug zu Kunden des Auftraggebers aufweisen.

- Eine Übertragung produktiver Daten aus der Prod-Umgebung in Dev oder Staging ist organisatorisch ausgeschlossen und technisch durch getrennte Konten und fehlende Cross-Account-Berechtigungen verhindert.
- Code- und Konfigurationsänderungen durchlaufen einen definierten Promotion-Workflow von Dev über Staging nach Prod. Direkter Zugriff auf Prod-Daten oder -Konfiguration ist auf einen eng begrenzten Personenkreis mit dokumentierter Berechtigung beschränkt.
- Logging und Monitoring sind je Stage separiert; Logs der Prod-Umgebung sind weder von Dev noch von Staging aus einsehbar.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Transport-Verschlüsselung: TLS 1.2 oder höher für alle Datenübertragungen.
- API-Zugriffe nur über authentifizierte und verschlüsselte Verbindungen.
- WebSocket-Verbindungen über WSS (verschlüsselt).

2.2 Eingabekontrolle

- Protokollierung von Erstellungs-, Änderungs- und Löschvorgängen auf Ebene der Nutzerinhalte (Audit-Log).
- Benutzerkennung bei jedem Eingabevorgang.
- Input-Validierung serverseitig.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

3.1 Verfügbarkeitskontrolle

- Redundante Systemarchitektur über mehrere Availability Zones.
- Regelmäßige Backups mit getesteter Wiederherstellbarkeit.
- Monitoring und Alerting für Infrastruktur und Applikation.
- DDoS-Schutz auf Infrastruktur-Ebene.

3.2 Rasche Wiederherstellbarkeit

- Disaster-Recovery-Verfahren mit definierten RTO/RPO-Zielen.
- Backups werden geografisch getrennt vom Primär-Standort gespeichert.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Regelmäßige Überprüfung der Wirksamkeit der TOMs (mindestens einmal jährlich).
- Sicherheits-Updates an eingesetzter Infrastruktur und Software zeitnah nach Veröffentlichung.
- Dokumentation der Überprüfungen.
- Jährliche Prüfung der Vereinbarungen zur Auftragsverarbeitung mit den Subauftragsverarbeitern (AWS, Mistral, Sentry) sowie der Datenschutzbedingungen weiterer Empfänger (Stripe).

5. Auftragskontrolle

- Schriftliche Vereinbarungen mit allen Subauftragsverarbeitern (Anlage 2).
- Regelmäßige Überprüfung der Datenschutz-Compliance der Subauftragsverarbeiter.

6. Verschlüsselung

- Verschlüsselung gespeicherter personenbezogener Daten („at rest") nach AES-256 oder vergleichbarem Standard.
- Verschlüsselte Übertragung („in transit") via TLS 1.2 oder höher.

Anlage 2: Genehmigte Subauftragsverarbeiter

Der Verantwortliche erteilt mit Abschluss dieses AVV eine allgemeine Genehmigung zur Hinzuziehung der nachstehend aufgeführten Subauftragsverarbeiter:

Subauftragsverarbeiter	Leistung	Ort der Verarbeitung	Rechtsgrundlage Drittland
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxemburg	Bereitstellung der Cloud-Infrastruktur (Hosting, Datenbanken, Speicher, Authentifizierung, E-Mail-Versand, CDN)	EU (Primärregion Paris; Irland für den E-Mail-Eingang)	Nicht anwendbar (EU-Verarbeitung)
Mistral AI SAS 15 rue des Halles, 75001 Paris, Frankreich	KI-gestützte Verarbeitung von Text-, Dokument- und Bildeingaben zur Erstellung und Bearbeitung von Prozessmodellen und Prozessdokumentation. Kundendaten werden gemäß Mistral-DPA nicht zum Training der Modelle verwendet	Frankreich (EU)	Nicht anwendbar (EU-Verarbeitung)
Functional Software, Inc. (Sentry) 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Error-Tracking, Performance-Monitoring und maskiertes Session-Replay zur Plattform-Stabilität (Texteingaben, Textinhalte und Medien werden clientseitig maskiert und nicht übertragen)	Deutschland (Sentry EU-Region)	Standardvertragsklauseln gemäß § 13 Abs. 2 lit. a dieses AVV

Weitere Empfänger (eigenständige Verantwortliche)

Stripe Payments Europe, Ltd., The One Building, 1 Grand Canal Street Lower, Dublin 2, D02 H210, Irland (Zahlungsabwicklung). Die Zahlungsabwicklung erfolgt durch Stripe als eigenständigen Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO; Stripe ist kein Subauftragsverarbeiter des Auftragsverarbeiters. Zahlungsdaten gibt der Verantwortliche unmittelbar bei Stripe ein (Stripe Checkout beziehungsweise Customer Portal). Stripe-interne Übermittlungen in die USA erfolgen auf Grundlage von Standardvertragsklauseln beziehungsweise des EU-U.S. Data Privacy Framework. Informationen zur Verarbeitung durch Stripe: stripe.com/de/privacy

Stand der Liste: Juli 2026. Änderungen der Subauftragsverarbeiter werden gemäß § 8 Abs. 3 angekündigt.

Procevia GmbH
Geschäftsführer: Iordanis Kleinöder Stafidis
Linder Weg 115, 51147 Köln
HRB 128157 – Amtsgericht Köln
E-Mail: legal@procevia.de

Stand: Juli 2026 | AVV gem. Art. 28 DSGVO

OPTIONALE UNTERZEICHNUNG

Vertragsabschluss und optionale Unterzeichnung

Dieser Auftragsverarbeitungsvertrag ist elektronisch unmittelbar nutzbar. Er wird mit der Online-Zustimmung im Rahmen der Registrierung automatisch Bestandteil des Vertrages (Präambel Abs. 3) und erfüllt das Formerfordernis des Art. 28 Abs. 9 DSGVO im elektronischen Format. Zeitpunkt und Versionsstand der Zustimmung dokumentiert Procevia serverseitig. **Eine Unterzeichnung dieser Seite ist für die Wirksamkeit nicht erforderlich.**

Wünschen Sie für Ihre Vertragsakte zusätzlich eine gezeichnete Fassung, vervollständigen Sie die Angaben auf der folgenden Seite, signieren digital oder auf dem Ausdruck und senden das Dokument an legal@procevia.de. Procevia gegenzeichnet und sendet eine Kopie an die angegebene Datenschutz-Kontaktadresse.

AUSFÜLLBARE ANGABEN

Angaben der Vertragsparteien

Verantwortlicher (Auftraggeber)

Vom Kunden auszufüllen

FIRMA / ORGANISATION

RECHTSFORM

UST-IDNR (OPTIONAL)

ANSCHRIFT (STRASSE, PLZ, ORT, LAND)

VERTRETEN DURCH (NAME, FUNKTION)

E-MAIL DATENSCHUTZKONTAKT

ORT, DATUM

UNTERSCHRIFT VERANTWORTLICHER

Auftragsverarbeiter

Wird von Procevia ausgefüllt

Procevia GmbH
Geschäftsführer: Iordanis Kleinöder Stafidis
Linder Weg 115, 51147 Köln, Deutschland
HRB **128157** · AG Köln
legal@procevia.de

ORT, DATUM

UNTERSCHRIFT