Vereinbarung zur Auftragsverarbeitung

dem Unternehmen, das das saicretary bei der ext.dev GmbH beauftragt — nachfolgend **„Verantwortlicher"** —

und

ext.dev GmbH, Vor dem Bardowicker Tore 6A, 21339 Lüneburg — nachfolgend **„Auftragsverarbeiter"** —

treffen die folgende Vereinbarung nach Art. 28 Abs. 3 DSGVO. Sie ergänzt die Beauftragung des Auftragsverarbeiters mit Einrichtung, Betrieb und Weiterentwicklung des saicretary, abgerechnet nach Aufwand bzw. nach den vereinbarten Pauschalen (nachfolgend **„Hauptvertrag"**). Sie gilt auch für den Testmonat nach § 12.

§ 1 Zustandekommen

1. Diese Vereinbarung wird nach Art. 28 Abs. 9 DSGVO in elektronischem Format geschlossen. **Eine Unterschrift ist nicht erforderlich.**
2. Sie wird mit der Beauftragung vereinbart: mit der Annahme des Angebots oder dem Beginn des Testmonats (§ 12), je nachdem, was zuerst eintritt. Das Angebot verweist auf diese Fassung. Einer gesonderten Bestätigung bedarf es nicht.
3. Sie gilt für alle Verarbeitungen seit Beginn der Tätigkeit des Auftragsverarbeiters für den Verantwortlichen, einschließlich des Testmonats nach § 12.
4. Diese Fassung ist dauerhaft unter www.saicretary.com/avv/ abrufbar. Eine neue Fassung kündigt der Auftragsverarbeiter mindestens vier Wochen vor ihrem Inkrafttreten in Textform an. Widerspricht der Verantwortliche nicht in dieser Frist, gilt sie; widerspricht er, bleibt die bisherige Fassung maßgeblich, und jede Partei kann den Hauptvertrag zum Inkrafttreten kündigen. Abweichende Vereinbarungen im Einzelfall gehen dieser Fassung vor.

§ 2 Gegenstand

1. Der Auftragsverarbeiter richtet für den Verantwortlichen ein System zur Ablage, Erschließung und Bereitstellung seiner Unterlagen und Informationen ein (**„saicretary"**), betreibt, administriert, wartet und entwickelt es weiter. Dazu gehören, heute und künftig, insbesondere:
   - das Dokumentenarchiv mit Texterkennung, Verschlagwortung, Suche und Rechtevergabe;
   - die Übernahme und der laufende Abgleich von Daten aus den Quellen des Verantwortlichen, etwa Cloud-Speicher (etwa Dropbox, SharePoint), E-Mail-Postfächer, Scanner, Microsoft 365 und Fachanwendungen;
   - die Wissensdatenbank und ihre Pflege durch das KI-Modell des Verantwortlichen (§ 5);
   - der Zugang aus KI-Anwendungen auf Archiv und Wissensdatenbank (MCP-Schnittstelle);
   - ein Portal für die Beschäftigten des Verantwortlichen, auch mit Kunden- und Vertragsverwaltung, Aufgaben- und Ticketverwaltung, Auswertungen und Statusseiten;
   - die Anmeldung der Nutzer des Verantwortlichen über den Anmeldedienst des Auftragsverarbeiters (gitlab.ext.dev) sowie die Benutzer- und Rechteverwaltung;

- Sicherung und Wiederherstellung, Überwachung der Erreichbarkeit, Fehlersuche, Datenübernahmen und -migrationen sowie Löschungen;
- die Projektkommunikation, Aufgabenverwaltung und der Support, auch über gitlab.ext.dev und E-Mail.

2. Die Verarbeitung findet statt
   - auf Systemen in den Konten des Verantwortlichen (in der Regel ein Server im Hetzner-Projekt des Verantwortlichen), auf die der Auftragsverarbeiter als Administrator zugreift,
   - während des Testmonats auf einem Server im Konto des Auftragsverarbeiters (§ 12), und
   - auf Systemen des Auftragsverarbeiters (Anmeldedienst, Projektverwaltung, E-Mail, Überwachung, Sicherungen).

Weitere Systeme, die der Auftragsverarbeiter für den Verantwortlichen einrichtet oder in dessen Auftrag bedient, sind gleichermaßen erfasst.

1. Neue Funktionen und Systeme im Rahmen von Absatz 1 erfordern keine Änderung dieser Vereinbarung. Eine Weisung in Textform (§ 6) genügt.
2. Die Vereinbarung läuft, solange der Auftragsverarbeiter Leistungen nach dem Hauptvertrag erbringt oder Zugang zu Daten des Verantwortlichen hat, und endet nach § 14.

§ 3 Art und Zweck der Verarbeitung

1. **Art der Verarbeitung:** alle Vorgänge nach Art. 4 Nr. 2 DSGVO, insbesondere Erheben, Übernehmen, Speichern, Ordnen, Erkennen von Text, Verschlagworten, Auslesen, Abfragen, Verknüpfen, Bereitstellen, Übermitteln an die Nutzer des Verantwortlichen, Einschränken, Sichern, Wiederherstellen und Löschen.
2. **Zweck** ist allein die Erbringung der Leistungen nach § 2. Der Auftragsverarbeiter verarbeitet die Daten nicht für eigene Zwecke, gibt sie nicht weiter und nutzt sie nicht zum Training von KI-Modellen.

§ 4 Daten und betroffene Personen

1. **Daten:** alle personenbezogenen Daten, die in den Unterlagen, Systemen und Quellen des Verantwortlichen enthalten sind oder bei der Nutzung des saicretary entstehen, insbesondere:
   - Stamm- und Kontaktdaten (Name, Anschrift, Telefon, E-Mail, Geburtsdatum);
   - Vertrags-, Auftrags- und Abrechnungsdaten, etwa Kunden-, Miet-, Liefer- und Dienstleistungsverträge, Tarife, Provisionen und Rechnungen;
   - Bank- und Zahlungsdaten;
   - Kopien von Ausweisdokumenten und Angaben aus ihnen;
   - Personal- und Bewerbungsunterlagen, Lohn- und Gehaltsdaten, Arbeitszeiten, Beurteilungen;
   - Kommunikationsinhalte (Schreiben, E-Mails, Notizen);
   - besondere Kategorien nach Art. 9 DSGVO, soweit sie in den Unterlagen enthalten sind, etwa Gesundheitsdaten in Arbeitsunfähigkeitsbescheinigungen, Schwerbehinderung oder Religionszugehörigkeit in Lohnunterlagen;

- Daten über strafrechtliche Verurteilungen nach Art. 10 DSGVO, soweit sie in den Unterlagen enthalten sind, etwa Führungszeugnisse;
- Nutzungs- und Anmeldedaten der Nutzer (Benutzername, E-Mail-Adresse, Rollen und Rechte, Anmelde- und Zugriffsprotokolle).

2. **Betroffene Personen:** Kunden und Interessenten, Beschäftigte, ehemalige Beschäftigte, Bewerber und deren Angehörige, Gesellschafter und Organe, Geschäftspartner, Lieferanten, Vermieter und Mieter, Ansprechpartner aller Genannten sowie die Nutzer des saicretary. Dazu gehören auch Personen aus den übrigen Geschäftsbereichen, deren Unterlagen in den Quellen des Verantwortlichen liegen.

§ 5 Künstliche Intelligenz

1. Das KI-Modell, mit dem das saicretary Inhalte liest und erschließt, bezieht der Verantwortliche in eigenem Namen (etwa Claude der Anthropic Ireland, Limited), auch schon im Testmonat. Den Vertrag mit dem Anbieter schließt der Verantwortliche selbst. Der Anbieter ist kein Unterauftragsverarbeiter des Auftragsverarbeiters. Der Auftragsverarbeiter richtet die Anbindung ein und betreibt sie.

2. Der Auftragsverarbeiter darf für Entwicklung, Administration und die Erbringung der Leistungen nach § 2 eigene KI-Dienste der Unterauftragsverarbeiter nach § 11 einsetzen, auch soweit sie dabei personenbezogene Daten erhalten. Er setzt sie nur für die Zwecke nach § 3 Abs. 2 ein und nur über Verträge, nach denen der Anbieter die Daten nicht zum Training seiner Modelle verwendet.

§ 6 Weisungen

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch bei Übermittlungen in Drittländer, es sei denn, das Recht der EU oder Deutschlands verpflichtet ihn dazu. In diesem Fall teilt er dem Verantwortlichen dies vorab mit, sofern das zulässig ist.

2. Der Hauptvertrag und diese Vereinbarung sind die Weisung. Weitere Weisungen ergehen in Textform, etwa per E-Mail, per Messenger oder als Ticket im Projekt des Verantwortlichen auf gitlab.ext.dev. Mündliche Weisungen bestätigt der Auftragsverarbeiter in Textform.

3. Weisungsberechtigt sind die Geschäftsführung, die im Angebot oder im Auftrag benannten Personen sowie weitere Personen, die einer von ihnen in Textform benennt. Weisungen nimmt Christopher Zechendorf entgegen.

4. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies unverzüglich mit. Er darf ihre Ausführung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

§ 7 Pflichten des Auftragsverarbeiters

1. Die mit der Verarbeitung befassten Personen sind zur Vertraulichkeit verpflichtet. Die Pflicht besteht nach dem Ende ihrer Tätigkeit fort.

2. Auf Inhalte greift der Auftragsverarbeiter nur zu, soweit es für die Leistungen nötig ist, etwa zur Fehlersuche, zur Prüfung von Datenübernahmen, zur Wiederherstellung oder auf Weisung. Kopien von Daten legt er nur auf den Systemen nach § 2 Abs. 2 an. Entwicklung und Tests erfolgen ohne

Echtdaten oder mit Daten, aus denen personenbezogene Angaben entfernt wurden; die Analyse eines Fehlers an einzelnen Datensätzen auf dem System des Verantwortlichen bleibt zulässig.

3. Der Auftragsverarbeiter unterstützt den Verantwortlichen im angemessenen Umfang bei Anfragen betroffener Personen (Art. 12 bis 23 DSGVO) und bei den Pflichten nach Art. 32 bis 36 DSGVO, auch bei Datenschutz-Folgenabschätzungen. Anfragen, die bei ihm eingehen, leitet er unverzüglich weiter.

4. Verletzungen des Schutzes personenbezogener Daten meldet er unverzüglich, nachdem sie ihm bekannt geworden sind (Art. 33 Abs. 2 DSGVO).

5. Er führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO. Ein Datenschutzbeauftragter ist nicht benannt, weil keine Pflicht dazu besteht.

6. Er stellt alle Informationen bereit, die zum Nachweis dieser Pflichten nötig sind, und ermöglicht Überprüfungen durch den Verantwortlichen oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer. In der Regel genügt eine Auskunft in Textform; Prüfungen vor Ort werden angemessen vorher angekündigt.

Ansprechpartner ist Christopher Zechendorf, christopher.zechendorf@ext.dev.

§ 8 Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und für die Rechte der betroffenen Personen verantwortlich, auch für die Informationspflichten gegenüber seinen Kunden und Beschäftigten.

2. Die Verträge über seine eigenen Konten und Dienste (etwa Server bei Hetzner nach dem Testmonat, die angebundenen Quellen, das KI-Modell nach § 5, Microsoft 365) schließt er selbst, einschließlich der dafür nötigen Vereinbarungen zur Auftragsverarbeitung.

3. Er teilt dem Auftragsverarbeiter unverzüglich mit, wenn eine Person keinen Zugang mehr haben soll, und informiert ihn über Fehler oder Unregelmäßigkeiten, die er bei den Ergebnissen feststellt.

§ 9 Ort der Verarbeitung

1. Die Verarbeitung findet in der Europäischen Union oder im Europäischen Wirtschaftsraum statt.

2. Die mit der Verarbeitung befassten Personen des Auftragsverarbeiters dürfen auch von außerhalb der EU auf die Systeme zugreifen, etwa auf Reisen, über verschlüsselte Verbindungen und mit Geräten des Auftragsverarbeiters. Die Daten werden dabei nicht dauerhaft außerhalb der EU gespeichert.

3. Weitere Übermittlungen in Drittländer finden nur nach Art. 44 ff. DSGVO und nach § 11 statt.

§ 10 Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen Maßnahmen, insbesondere:

    - Die Systeme des Verantwortlichen laufen auf einem eigenen Server, getrennt von den Systemen anderer Kunden – nach dem Testmonat im Konto des Verantwortlichen.

- Der Server ist nur per Schlüssel zugänglich, ohne Passwort-Anmeldung und ohne direkte Anmeldung als Administrator. Administrative Zugänge sind auf die mit dem Betrieb betrauten Personen beschränkt.
- Eine Firewall lässt nur Web-Zugriffe und den Wartungszugang zu. Datenbank, Suche und interne Dienste sind von außen nicht erreichbar. Wiederholte Fehlversuche sperren die Absender-Adresse automatisch.
- Alle Zugriffe über das Netz sind transportverschlüsselt.
- Nutzer greifen nur nach Anmeldung zu und sehen nur die Bereiche, für die sie berechtigt sind. Dienste und Schnittstellen arbeiten mit eigenen Konten mit den geringsten nötigen Rechten. Der Auftragsverarbeiter greift nur mit zweitem Faktor zu: über den Anmeldedienst mit Zwei-Faktor-Anmeldung und auf den Server nur per Schlüssel. Ob seine eigenen Nutzer einen zweiten Faktor verwenden, entscheidet der Verantwortliche.
- Sicherheitsupdates des Betriebssystems werden automatisch eingespielt, die Anwendungen regelmäßig aktualisiert.
- Protokolle werden nur so lange aufbewahrt, wie es für Betrieb und Sicherheit nötig ist, in der Regel höchstens 30 Tage. Protokolle der Datenübernahme enthalten keine Inhalte.
- Gelöschte Dokumente bleiben bis zu 30 Tage wiederherstellbar und werden dann endgültig entfernt.
- Sicherungen außerhalb des Servers werden vor der Übertragung verschlüsselt.
- Rechenzentrum und Betrieb der Server liegen bei den Anbietern nach § 11 bzw. § 8 Abs. 2, die ihre Maßnahmen in ihren Verträgen nachweisen.

2. Die Maßnahmen dürfen fortentwickelt werden, solange das Schutzniveau nicht sinkt.

§ 11 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Zurzeit sind dies:

UNTERNEHMEN	LEISTUNG	ORT
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server des Auftragsverarbeiters (Anmeldedienst, Projektverwaltung, E-Mail, Überwachung) sowie der Server des saicretary während des Testmonats (§ 12)	Deutschland bzw. Finnland, EU
Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Irland	KI-Dienste (Sprachmodelle) nach § 5 Abs. 2	Irland, EU; Verarbeitung auch in den USA durch Anthropic PBC und deren Unterauftragsverarbeiter

Übermittlungen in die USA erfolgen auf Grundlage des Angemessenheitsbeschlusses zum Datenschutzrahmen EU-USA, soweit der Empfänger zertifiziert ist, im Übrigen auf Grundlage der Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/914).

1. Über neue oder ersetzte Unterauftragsverarbeiter informiert der Auftragsverarbeiter in Textform vorab. Der Verantwortliche kann innerhalb von 14 Tagen aus wichtigem datenschutzrechtlichem Grund widersprechen.
2. Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten und haftet für sie wie für sich selbst.
3. Keine Unterauftragsverarbeiter sind die Anbieter, mit denen der Verantwortliche selbst Verträge schließt (§ 8 Abs. 2), auch wenn der Auftragsverarbeiter in deren Konten für den Verantwortlichen tätig wird, sowie Leistungen ohne Zugriff auf personenbezogene Daten (etwa Domainverwaltung und TLS-Zertifikate).

§ 12 Testmonat

1. Der Auftragsverarbeiter kann das saicretary für die ersten 30 Tage auf einem Server in seinem eigenen Hetzner-Konto betreiben (**„Testmonat"**). Für diesen Server ist Hetzner Unterauftragsverarbeiter nach § 11. Im Testmonat wird nur der vereinbarte Ausschnitt der Quellen angebunden; Sicherungen außerhalb des Servers werden in dieser Zeit nicht angelegt.
2. Entscheidet sich der Verantwortliche bis zum Ende des Testmonats für den Hauptvertrag, überträgt der Auftragsverarbeiter den Server samt Datenträgern in ein Projekt des Verantwortlichen bei Hetzner. Ab der Übertragung ist der Server ein System des Verantwortlichen nach § 2 Abs. 2, und Hetzner ist dafür kein Unterauftragsverarbeiter mehr (§ 11 Abs. 4). Auf dem Konto des Auftragsverarbeiters verbleiben keine Kopien.
3. Entscheidet er sich nicht dafür oder äußert er sich bis zum Ende des Testmonats nicht, löscht der Auftragsverarbeiter den Server samt Datenträgern und Snapshots innerhalb von 7 Tagen und bestätigt die Löschung in Textform. Die Originale in den Quellen des Verantwortlichen bleiben unberührt. Die Konten der Nutzer im Anmeldedienst werden nach § 14 Abs. 2 gelöscht.
4. Der Testmonat kann in Textform verlängert werden.

§ 13 Haftung

Für die Haftung gilt Art. 82 DSGVO.

§ 14 Ende der Vereinbarung

1. Nach dem Ende gibt der Auftragsverarbeiter alle Zugänge zu den Systemen des Verantwortlichen zurück und übergibt auf Wunsch die Daten in einem gängigen Format. Die Systeme im Konto des Verantwortlichen bleiben bei ihm und laufen weiter. Vor der Rückgabe stellt der Auftragsverarbeiter die Anmeldung der Nutzer auf ein vom Verantwortlichen benanntes Verfahren um (etwa sein eigenes Microsoft- oder Google-Konto oder Passwörter) und übergibt die Zugangsdaten. Updates, Sicherheitsaktualisierungen und Unterstützung leistet er danach nicht mehr.
2. Innerhalb von 30 Tagen löscht er alle personenbezogenen Daten des Verantwortlichen auf seinen eigenen Systemen, auch die Konten der Nutzer im Anmeldedienst, sofern keine gesetzliche Pflicht

zur Speicherung besteht. Verschlüsselte Sicherungen werden mit ihrer regulären Rotation entfernt. Die Löschung bestätigt er in Textform.

§ 15 Schlussbestimmungen

1. Änderungen bedürfen der Textform.
2. Im Widerspruch zum Hauptvertrag geht diese Vereinbarung vor. Ist eine Bestimmung unwirksam, bleibt der Rest wirksam.
3. Es gilt deutsches Recht. Gerichtsstand ist Lüneburg.