

## Allgemeine Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO

Der **Verantwortliche** ist der jeweilige Lizenznehmer der Software der ireo GmbH, im Folgenden **Auftraggeber** genannt.

Der **Auftragsverarbeiter** ist die ireo GmbH, Griesgasse 1, 8020 Graz, im Folgenden **Auftragnehmer** genannt.

### 1. GEGENSTAND DER VEREINBARUNG

---

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

- a. Bereitstellung der vereinbarten Funktionalität der Software,
- b. gegebenenfalls auch die Bereitstellung des Hostings der Software, sofern vertraglich vereinbart.

Diese Vereinbarung ist als Ergänzung zur Lizenzvereinbarung, den allgemeinen Geschäftsbedingungen und des abgeschlossenen Werkvertrages in der jeweilig geltenden Version zu verstehen.

On Premises-Hosting unterliegt besonderen Bedingungen. Dabei werden viele Dienste in Verantwortung des Auftraggebers gegeben. Die Dienste, die dadurch ausgeschlossen werden, sind durch **[Nicht bei on premises]** gekennzeichnet.

- (2) **[Nicht bei on premises]** Folgende Datenkategorien werden möglicherweise verarbeitet: Alle der Software zur Verfügung gestellten Daten (Bilder, Kommentare, Text- und Zahlenwerte, Bewertungen und weitere), also: sämtliche Daten, die vom Auftraggeber in die Software eingegeben oder hochgeladen werden.
- (3) **[Nicht bei on premises]** Der Auftraggeber verpflichtet sich ausdrücklich, weder sensible Daten gemäß Art 9 Abs 1 DSGVO, noch strafrechtlich relevante Daten gemäß Art 10 DSGVO in die Software der ireo GmbH einzugeben und/oder der Verarbeitung zu übergeben. Eine Verarbeitung sensibler Daten benötigt weitergehende Schutzmaßnahmen und muss daher gesondert schriftlich vereinbart werden.
- (4) **[Nicht bei on premises]** Folgende Kategorien betroffener Personen unterliegen möglicherweise der Verarbeitung: Die übergebenen Daten aller Personen, die die Software benutzen, Kunden und Lieferanten des Auftraggebers und deren Kontaktpersonen, sowie Dritte (z.B. Gesprächspartner, Beteiligte, anwesende Personen, während der Dokumentationsvorhaben), deren Daten durch den Auftraggeber in die Software eingegeben werden.

- (5) Welche Kategorie und Art an Daten in die Software eingegeben wird, kann durch den Auftragnehmer nicht beeinflusst werden, daher sind die Auflistungen in (2) und (4), sowie andere Listen in diesem Dokument nicht abschließend.

## 2. DAUER DER VEREINBARUNG

---

Die Vereinbarung wird auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit durch die Beendigung des Lizenzabkommens jederzeit gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Die Vereinbarung wird automatisch gelöst, falls keine Lizenz zur Benutzung der Software mehr vorhanden ist.

## 3. PFLICHTEN DES AUFTRAGNEHMERS

---

- (1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung von persönlichen Daten, die zur Verarbeitung übergeben wurden, für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.
- (2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
- (3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1 zu entnehmen).
- (4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen. Diese Zusage wird nur für Felder angeboten, die zur Erfassung dieser Daten gedacht sind. Die Eingabe von persönliche Daten in Felder, die dafür nicht gedacht sind, wie z.B. Beschreibungen oder allgemeine Textfelder, sind davon explizit ausgenommen.

- (5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
- (6) Der Auftraggeber wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat. Aufgrund der Vielfältigkeit und Konfigurierbarkeit der Nutzung der Software storywise kann das Verarbeitungsverzeichnis nicht durch den Auftragnehmer erstellt werden.
- (7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
- (8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, in dessen Auftrag zu vernichten, sofern keine rechtliche Grundlage besteht diese zu behalten (z.B. Buchhaltungsdaten, 7 Jahre). Der Auftraggeber muss hierzu rechtzeitig, d.h. mindestens einen Monat vor Beendigung dieser Vereinbarung, schriftlich eine Aufbewahrung über die Vertragslaufzeit hinaus beantragen.
- (9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

#### 4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG **[NICHT BEI ON PREMISES]**

---

Alle Datenverarbeitungstätigkeiten der ireo GmbH werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

#### 5. SUB-AUFTRAGSVERARBEITER **[NICHT BEI ON PREMISES]**

---

Der Auftragnehmer ist befugt, folgende Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

- Midlight GmbH, Griesgasse 1, 8020 Graz
  - IT-Dienstleistungen, Backup
- Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen (DE)
  - Hosting unserer Systeme (Backend, **Datenbanken**) in Datenzentren in Deutschland
  - Backup

- Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München (DE)
  - Keine permanente Datenspeicherung
  - Azure AI Services, privater Inference-Endpoint (vorrangig gehosted in Frankfurt, andere Standorte innerhalb der EU möglich)
  - Virtual machines (.docx to PDF generation)
- Amazon Web Services EMEA SARL ("AWS Europe"), 38 Avenue John F. Kennedy, L-1855 Luxembourg
  - Dokumentenablage (S3)
  - externes Backup (S3)

Datenspeicherung an einem Standort in Frankfurt, Irland, London, Paris oder Stockholm

Die Benutzer des Systems sind in der Lage, Verbindungen zu externen Diensten selbsttätig herzustellen. Dies erfolgt in voller Eigenverantwortung des Benutzers. Stand 01/2025 sind das folgende Dienste:

JIRA (Atlassian Pty Ltd., Level 6, 341 George Street, Sydney, NSW 2000, Australia)

Youtrack (JetBrains s.r.o., Na hřebenech II 1718/8, Prague, 14000, Czech Republic)

Azure Devops (Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München (DE))

Zapier (Zapier, Inc., 548 Market St. #62411, San Francisco, CA 94104-5401, USA)

Miro (RealtimeBoard, Inc., 201 Spear Street, Suite 1100, San Francisco, CA 94105, USA)

Login with Google: (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland)

Login with LinkedIn: (LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland)

Login with Microsoft: (Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München (DE))

Die folgenden AI Systeme sind optional verfügbar:

OpenAI (OpenAI, L.L.C., 3180 18th St., San Francisco, CA 94110, United States of America)

Together Computer Inc. (801 El Camino Real, Menlo Park, CA 94025, United States of America)

Anthropic PBC (548 Market Street, PMB 90375 San Francisco CA 94104, United States of America)

Cerebras Systems Inc (1237 E Arques Ave, Sunnyvale, CA 94085, United States of America)

Groq, Inc. (301 Castro St., Suite 200, Mountain View, CA 94041, United States of America)

Gemini by Google (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland)

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingetht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

## 6. ANLAGE 1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN [NICHT BEI ON PREMISES]

---

### A. VERTRAULICHKEIT

---

**Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

- Videoanlage
- Elektrische Türöffner
- Schlüssel
- Einbruchshemmende Fenster und/oder Sicherheitstüren
- Begleitung von Besuchern im Unternehmensgebäude

**Zugangskontrolle:** Schutz vor unbefugter Systembenutzung durch:

- Kennwörter (einschließlich entsprechender Policy)
- Automatische Sperrmechanismen
- Zwei-Faktor-Authentifizierung
- Verschlüsselung von Datenträgern
- Least-Privilege-System, Zugriff aufs Live-System auf Datenbankebene nur für einzelne Benutzer

**Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

- Standard-Berechtigungsprofile auf „need to know-Basis“
- Periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
- Sichere Aufbewahrung von Speichermedien
- Datenschutzgerechte Wiederverwendung von Datenträgern
- Clear-Desk/Clear-Screen Policy

## B. DATENINTEGRITÄT<sup>1</sup>

---

**Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

- Verschlüsselung von Datenträgern, u.a. Zwang für Verschlüsselung der System- & Datenplatten
- Verschlüsselung von Dateien
- Verschlüsselung der Kommunikation, auch im Produkt (Frontend-Backend-Verbindung)
- Virtual Private Networks (VPN), unternehmensinterne Zugänge nur über VPN möglich
- Elektronische Signatur
- Two-Factor-Authentifikation für Zugänge inkl. Datenspeicherung und Kommunikationskanäle

**Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

- Protokollierung
- Dokumentenmanagement

## C. VERFÜGBARKEIT UND BELASTBARKEIT

---

**Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

- Backup-Strategie (online/offline; on-site/off-site)
- Unterbrechungsfreie Stromversorgung (USV)
- Virenschutz
- Firewall
- Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum
- Security Checks auf Infrastruktur- und Applikationsebene
- Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
- Rasche Wiederherstellbarkeit der Daten

---

<sup>1</sup> Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

## D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

---

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen
- Datenschutzfreundliche Voreinstellungen

**Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers durch eindeutige Vertragsgestaltung und Verpflichtung der Subunternehmer zu ebendiesen Pflichten.