Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Stand: November 2026

zwischen

dem Kunden des Auftragsverarbeiters

– nachfolgend „Verantwortlicher“ –

und

CAFM Systems GmbH
Grünbergstraße 15, Stiege 1, 5. OG
1120 Wien
FN 239136 x

– nachfolgend „Auftragsverarbeiter“; beide gemeinsam „Vertragsparteien“ –

1. Gegenstand und Dauer

1.1 Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der zwischen den Vertragsparteien bestehenden Verträge, Angebote und Aufträge (gemeinsam „Leistungsvereinbarung“).

1.2 Diese Vereinbarung gilt für alle bestehenden und künftigen Leistungsvereinbarungen zwischen den Vertragsparteien. Ihre Laufzeit entspricht der Laufzeit der Leistungsvereinbarung. Sie endet jedoch nicht, solange der Auftragsverarbeiter noch personenbezogene Daten des Verantwortlichen verarbeitet.

1.3 Diese Vereinbarung ersetzt frühere Vereinbarungen der Vertragsparteien zur Auftragsverarbeitung, auch solche, die noch unter dem früheren Firmennamen des Auftragsverarbeiters abgeschlossen wurden. Haben die Vertragsparteien eine Vereinbarung zur Auftragsverarbeitung auf Grundlage einer Vorlage des Verantwortlichen abgeschlossen, geht diese vor.

2. Art und Zweck der Verarbeitung

2.1 Der Auftragsverarbeiter erbringt für den Verantwortlichen je nach Leistungsvereinbarung folgende Leistungen, bei denen personenbezogene Daten verarbeitet werden können:

- SaaS – Bereitstellung der CAFM-Software REDIX (vorher REDi4) zur Nutzung über das Internet, einschließlich Hosting, Betrieb, Datensicherung und Wartung der Plattform.
- Support und Wartung – Hotline, Fehleranalyse, Bearbeitung von Anfragen per E-Mail, Fernwartung (nur nach Freigabe durch den Verantwortlichen), Leistungen vor Ort und Schulungen.
- Implementierung – Einrichtung, Konfiguration, Datenübernahme (Migration) und Schnittstellen.

- Datenaufbereitung – Erfassung, Aufbereitung und Pflege von Gebäude-, Flächen- und Anlagendaten, Plänen (CAD/BIM), Raumbüchern und 3D-Scans. Pläne können Namen, Kürzel und Kontaktdaten von Planverfassern, Projektbeteiligten oder Raumnutzern enthalten. 3D-Scans können Personen abbilden; diese werden unkenntlich gemacht.

2.2 Die Verarbeitung erfolgt ausschließlich zur Erbringung dieser Leistungen. Der konkrete Umfang ergibt sich aus der jeweiligen Leistungsvereinbarung.

2.3 Kategorien betroffener Personen:

- Beschäftigte des Verantwortlichen (insbesondere Nutzer der Software, Raum- und Arbeitsplatznutzer)
- Lieferanten, Dienstleister und Geschäftspartner des Verantwortlichen sowie deren Ansprechpartner
- Mieter und Nutzer der Liegenschaften des Verantwortlichen
- Planverfasser und sonstige Projektbeteiligte
- sonstige Personen, deren Daten der Verantwortliche in die Leistungen einbringt

2.4 Arten personenbezogener Daten:

- Personenstammdaten (Name, akademischer Grad, Funktion, Rolle, Organisationseinheit)
- dienstliche Kontaktdaten (Telefon, E-Mail, Anschrift)
- Benutzerkonto-, Anmelde- und Protokolldaten
- Zuordnung von Arbeitsplätzen, Räumen, Schließfächern und Schlüsseln zu Personen
- Auftrags-, Störungs- und Wartungsdaten mit Personenbezug
- Vertrags-, Bestell- und Mieterdaten, Korrespondenz und Dokumente
- Abrechnungs- und Kostendaten (z. B. Rechnungen an Mieter oder Kunden im Modul Kostenmanagement)
- Namen, Kürzel und Kontaktdaten in Plänen und Raumbüchern; Bilddaten in 3D-Scans

2.5 Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nicht vorgesehen. Der Verantwortliche informiert den Auftragsverarbeiter vorab, falls solche Daten übermittelt werden sollen.

3. Ort der Verarbeitung

3.1 Die Verarbeitung erfolgt grundsätzlich in der Europäischen Union oder im Europäischen Wirtschaftsraum.

3.2 Eine Verarbeitung in einem Drittland erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (z. B. Schweiz) oder von Standardvertragsklauseln. Die betroffenen Unterauftragsverarbeiter sind in Anlage 1 angeführt.

4. Weisungen

4.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist durch Unionsrecht oder österreichisches Recht zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen diese Verpflichtung vorab mit, sofern das Recht dies nicht verbietet.

4.2 Die Weisungen ergeben sich aus der Leistungsvereinbarung und dieser Vereinbarung. Einzelweisungen erteilt der Verantwortliche schriftlich oder per E-Mail.

4.3 Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Verantwortlichen unverzüglich. Er darf die Durchführung der Weisung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

4.4 Auskünfte an Dritte oder an betroffene Personen erteilt der Auftragsverarbeiter nur nach vorheriger Weisung des Verantwortlichen.

5. Pflichten des Auftragsverarbeiters

5.1 Vertraulichkeit – Der Auftragsverarbeiter verpflichtet alle Personen, die Zugang zu den Daten haben, vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit und zur Wahrung des Datengeheimnisses gemäß § 6 DSG. Diese Verpflichtung gilt auch nach Ende ihrer Tätigkeit.

5.2 Sicherheit der Verarbeitung – Der Auftragsverarbeiter trifft die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, die in Anlage 2 beschrieben sind, um einen angemessenen Schutz der personenbezogenen Daten sicherzustellen. Er betreibt ein Informationssicherheits-Managementsystem nach ISO/IEC 27001. Die Maßnahmen dürfen an den Stand der Technik angepasst werden, sofern das Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

5.3 Rechte betroffener Personen – Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung der Rechte betroffener Personen. Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, leitet er das Ersuchen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht ohne dessen Weisung.

5.4 Unterstützung – Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation der Aufsichtsbehörde)..

5.5 Verletzungen des Schutzes personenbezogener Daten – Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden ab Kenntnis. Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO. Fehlende Angaben werden nachgereicht.

5.6 Behörden – Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen, Anfragen und Maßnahmen von Aufsichtsbehörden, die Daten des Verantwortlichen betreffen, sowie über behördliche Herausgabeverlangen, soweit dies rechtlich zulässig ist.

6. Unterauftragsverarbeiter

6.1 Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die bei Abschluss dieser Vereinbarung eingesetzten Unterauftragsverarbeiter sind in Anlage 1 angeführt und gelten als genehmigt.

6.2 Der Auftragsverarbeiter informiert den Verantwortlichen vor jeder beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters schriftlich oder per E-Mail. Der Verantwortliche kann

binnen zwei Wochen widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Bei Widerspruch suchen die Vertragsparteien eine einvernehmliche Lösung. Gelingt dies nicht, kann der Verantwortliche die Leistungsvereinbarung zum Ende des nächstfolgenden Quartals kündigen; bis dahin erbringt der Auftragsverarbeiter die Leistung unverändert.

6.3 Der Auftragsverarbeiter legt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO). Er haftet gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten durch den Unterauftragsverarbeiter.

6.4 Nicht als Unterauftragsverarbeitung gelten Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt, etwa Telekommunikations-, Post- und Transportdienstleistungen oder die Entsorgung von Datenträgern.

7. Nachweise und Kontrollen

7.1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung und des Art. 28 DSGVO erforderlich sind.

7.2 Der Nachweis kann insbesondere durch aktuelle Zertifikate (z. B. ISO/IEC 27001), Berichte unabhängiger Prüfer oder Auditberichte erbracht werden.

7.3 Der Verantwortliche ist berechtigt, Überprüfungen einschließlich Inspektionen selbst oder durch einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer durchzuführen. Vor-Ort-Prüfungen sind mindestens 30 Tage vorher anzukündigen und finden zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs statt. Jede Vertragspartei trägt ihre eigenen Kosten.

8. Löschung und Rückgabe der Daten

8.1 Nach Ende der Leistungserbringung gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten in einem gängigen, maschinenlesbaren Format zurück oder löscht sie. In beiden Fällen löscht er sämtliche bei ihm vorhandenen Kopien, sofern nicht nach Unionsrecht oder österreichischem Recht eine Pflicht zur Speicherung besteht. Für Daten in Datensicherungen gilt ergänzend Punkt 8.2.

8.2 Personenbezogene Daten in Datensicherungen, deren isolierte Löschung technisch nicht möglich ist, werden im Rahmen des regulären Sicherungszyklus innerhalb einer vorab mit dem Verantwortlichen vereinbarten und dokumentierten Höchstfrist gelöscht oder überschrieben. Bis dahin werden sie geschützt aufbewahrt, dem produktiven Zugriff entzogen und nicht für andere Zwecke verarbeitet. Eine Wiederherstellung ist ausschließlich erforderlichkeitsbezogen zur Wiederherstellung der Systeme zulässig; dabei wiederhergestellte Daten, die bereits zu löschen waren, werden vor einer erneuten produktiven Nutzung erneut gelöscht. Gesetzliche Speicherungspflichten nach Punkt 8.1 bleiben unberührt. Auf die Bestimmung des § 4 Abs 2 DSG wird hingewiesen.

8.3 Die Löschung wird dokumentiert. Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung schriftlich.

9. Pflichten des Verantwortlichen

9.1 Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich.

9.2 Er informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

10. Schlussbestimmungen und Vergütung

10.1 Diese Vereinbarung ist Bestandteil der Leistungsvereinbarung und der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters. Eine gesonderte Unterzeichnung ist nicht erforderlich.

10.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform; eine E-Mail genügt. Änderungen der Anlagen 1 und 2 erfolgen nach Punkt 6.2 bzw. 5.2.

10.3 Bei Widersprüchen zwischen dieser Vereinbarung und der Leistungsvereinbarung oder den Allgemeinen Geschäftsbedingungen geht in Fragen des Datenschutzes diese Vereinbarung vor.

10.4 Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine wirksame, die ihrem Zweck am nächsten kommt.

10.5 Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen und des UN-Kaufrechts. Ausschließlicher Gerichtsstand ist das für den ersten Wiener Gemeindebezirk sachlich zuständige Gericht.

10.6 Vergütung – Unterstützungsleistungen nach diesem Vertrag und nach dem Gesetz, die über die Leistungsvereinbarung hinausgehen, werden zu den jeweils gültigen Stundensätzen verrechnet, außer sie sind auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen.

Anlage 1 – Unterauftragsverarbeiter
Anlage 2 – Technische und organisatorische Maßnahmen

Anlage 1 – Unterauftragsverarbeiter

Stand: November 2026. Welche Unterauftragsverarbeiter tätig werden, hängt von den beauftragten Leistungen ab.

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung / Garantie
Akenes SA (Exoscale), Lausanne, Schweiz	Hosting und Betrieb der Plattform REDIX (Rechenzentren); weiterer Unterauftragsverarbeiter Aiven Oy, Helsinki	Schweiz, EU (Angemessenheitsbeschluss Schweiz)
conova communications GmbH, Salzburg, Österreich	Externe Datensicherung (Off-site-Backup)	Österreich
Microsoft Ireland Operations Ltd., Dublin, Irland	Microsoft 365: E-Mail, Dateiablage und Zusammenarbeit (Supportanfragen, Projektunterlagen)	EU (EU Data Boundary); Standard-Unterauftragsverarbeiter von Microsoft; Übermittlung USA über EU-US Data Privacy Framework
Autodesk Ireland Operations UC, Dublin, Irland	Autodesk Forma Data Management: Plandaten bei der Datenaufbereitung	EU; Übermittlung USA über EU-US Data Privacy Framework
Matterport, Inc., USA	3D-Scans aus Kundenprojekten; personenbezogene Daten nur E-Mail-Adressen	USA (Standardvertragsklauseln); Personen in Scans werden unkenntlich gemacht
MPskin GmbH, Deutschland	Zusatzfunktionen für Matterport-Touren	Deutschland (Hosting Hetzner)
secnetic GmbH, Österreich	Sicherheitsüberwachung der Plattform REDIX (SIEM/Monitoring)	Österreich; keine Weitergabe von Kundendaten an weitere Anbieter
Anthropic, PBC, USA	KI-Assistenz Claude Team (Fehleranalyse, Auswertung von Support-Daten)	USA (Standardvertragsklauseln laut DPA)
Mistral AI SAS, Paris, Frankreich	KI-Auswertung von Mails und Dokumenten im AgentCenter	EU (Frankreich); DPA vom 27.07.2026

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Maßnahme	Ziel	Umsetzung
1. Zutrittskontrolle	Kein Zutritt Unbefugter zu Datenverarbeitungsanlagen	Server in zertifizierten Rechenzentren von Exoscale mit physischer Zutrittskontrolle (Chipkarten, Videoüberwachung, Sicherheitspersonal). Büroräume durch Schließanlage gesichert, Zutritt nur für berechtigte Mitarbeitende.
2. Zugangskontrolle	Keine Nutzung der Systeme durch Unbefugte	Anmeldung über Single Sign-on mit Mehr-Faktor-Authentifizierung. Administrativer Zugang nur für berechtigte Mitarbeitende. Fernwartung beim Verantwortlichen nur nach dessen Freigabe.
3. Zugriffskontrolle	Zugriff nur auf die jeweils berechtigten Daten	Rollenbasiertes Berechtigungskonzept. Konten ausscheidender Mitarbeitender werden sofort gesperrt.
4. Trennungskontrolle	Getrennte Verarbeitung je Zweck und Kunde	Mandantentrennung durch eigene Datenbanken bzw. Umgebungen je Kunde. Trennung von Produktiv- und Testumgebung.
5. Pseudonymisierung	Kein Personenbezug, wo nicht nötig	Pseudonymisierung, soweit nach Zweck möglich und verhältnismäßig. Technische IDs statt Klarnamen, wo praktikabel. Personen in 3D-Scans werden unkenntlich gemacht.
6. Weitergabekontrolle	Schutz bei Übertragung und Transport	Verschlüsselte Übertragung (TLS/HTTPS). Schnittstellen nur über authentifizierte, verschlüsselte Verbindungen. Kein unverschlüsselter Versand personenbezogener Daten per E-Mail.
7. Eingabekontrolle	Nachvollziehbarkeit von Änderungen	Protokollierung von Eingabe, Änderung und Löschung mit Benutzerkennung und Zeitstempel (Audit-Logs).
8. Verfügbarkeit und Wiederherstellbarkeit	Schutz vor Verlust, rasche Wiederherstellung	Redundante Infrastruktur bei Exoscale. Tägliche automatische Datensicherung. Zusätzliche externe Sicherung bei conova (Österreich). Sicherheitsüberwachung der Plattform.
9. Auftragskontrolle	Verarbeitung nur nach Weisung	Verarbeitung nur gemäß dieser Vereinbarung. Verpflichtung zum

Maßnahme	Ziel	Umsetzung
		Datengeheimnis nach § 6 DSG. Unterauftragsverarbeiter nur mit Auftragsverarbeitungsvertrag; regelmäßige Lieferantenbewertung.
10. Organisation	Wirksamer Datenschutz im Betrieb	Informationssicherheits-Managementsystem nach ISO/IEC 27001 mit festgelegten Zuständigkeiten. Verpflichtung aller Mitarbeitenden zur Vertraulichkeit. Regelmäßige Schulungen. Meldeprozess für Sicherheitsvorfälle. Sichere Entsorgung von Datenträgern und Papier.
11. Überprüfung	Regelmäßige Wirksamkeitskontrolle	Regelmäßige Überprüfung und Bewertung der Maßnahmen im Rahmen des ISMS (interne Audits, Managementbewertung).