Vereinbarung zur Auftragsverarbeitung (AVV) für das Reservierungssystem RESTL der ARQOS GmbH

Fassung 13.11.2026 — gültig ab 13.11.2026

Vertragsparteien

Verantwortlicher (Auftraggeber): der Kunde, der mit der ARQOS GmbH einen Vertrag über die Nutzung des Reservierungssystems RESTL geschlossen hat (Hauptvertrag), mit den Angaben aus der Auftragsbestätigung und dem Kundenkonto.

Auftragsverarbeiter: ARQOS GmbH, Kuefsteinstraße 14/9, 3107 Viehofen, Österreich, FN 677203m, Landesgericht St. Pölten, UID ATU83198736. Kontakt für Datenschutzanfragen: info@restl.at.

§ 1 Gegenstand, Abschluss, Dauer und Rangordnung

1.1. Der Auftragsverarbeiter stellt dem Verantwortlichen das Reservierungssystem RESTL als webbasierte Software zur Verfügung. Er verarbeitet dabei personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien.

1.2. Der Verantwortliche bleibt für die Rechtmäßigkeit der Verarbeitung, insbesondere für die Rechtsgrundlagen und die Information seiner Gäste, allein verantwortlich. Er ist Verantwortlicher im Sinne des Art. 4 Z 7 DSGVO, der Auftragsverarbeiter ist Auftragsverarbeiter im Sinne des Art. 4 Z 8 DSGVO. Als Vorlage für die Information seiner Gäste stellt der Auftragsverarbeiter je Betrieb Datenschutzhinweise unter <betrieb>.restl.at/datenschutz bereit; der Verantwortliche prüft, ob sie für seinen Betrieb vollständig sind.

1.3. Diese Vereinbarung ist Bestandteil des Hauptvertrags (AGB Punkt 10.2). Sie wird mit dem Hauptvertrag geschlossen — durch Bestätigung bei der Anmeldung, im Zahlungslink, durch Unterschrift auf dem Auftragsformular oder durch Bestätigung im Kundenbereich. Die elektronische Form genügt (Art. 28 Abs. 9 DSGVO). Für Hauptverträge, die vor dem 13.11.2026 geschlossen wurden, konkretisiert diese Fassung die in AGB Punkt 10.2 vereinbarte Auftragsverarbeitung.

1.4. Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Sie endet mit dessen Beendigung, ohne dass es einer gesonderten Kündigung bedarf. Die Pflichten aus § 9 (Rückgabe und Löschung) bestehen darüber hinaus fort.

1.5. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen in datenschutzrechtlichen Fragen die Regelungen dieser Vereinbarung vor.

1.6. Nutzt der Verantwortliche das Zusatzmodul für Räume und verarbeiten Mieter:innen in RESTL Daten ihrer eigenen Kund:innen und Teilnehmer:innen, sind die Mieter:innen dafür selbst Verantwortliche. Für diese Verarbeitung gilt diese Vereinbarung im Verhältnis zwischen der jeweiligen Mieter:in und dem Auftragsverarbeiter entsprechend (Nutzungsbedingungen für Mieter:innen).

§ 2 Art, Zweck und Umfang der Verarbeitung

2.1. **Zweck:** Entgegennahme und Verwaltung von Tischreservierungen über alle Kanäle des Systems (Buchungsfenster auf der Website des Verantwortlichen, Reservierungsseite, KI-Assistenten der Gäste, Eingabe durch das Personal); Tisch- und Kapazitätsplanung; Kommunikation mit dem Gast über die Reservierung (Bestätigung, Erinnerung, Änderung, Stornierung, Hinweise nach Nichterscheinen); Kartenhinterlegung gegen Nichterscheinen, soweit der Verantwortliche sie nutzt; Führung einer Gästekartei zur Betriebsorganisation; Werbekommunikation an Gäste, die eingewilligt haben; im Zusatzmodul Räume die Bearbeitung von Raumanfragen und die Verwaltung von Kursen, Teilnehmer:innen und Kursbuchungen (§ 1.6).

2.2. **Art der Verarbeitung:** Erheben, Erfassen, Speichern, Ordnen, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln (E-Mail-Versand, Benachrichtigungen an Geräte der Nutzer:innen, Kartenhinterlegung), Abgleichen, Einschränken, Löschen und Vernichten.

2.3. **Betroffene Personen:** Gäste des Verantwortlichen und deren Begleitpersonen, soweit vom Gast angegeben; Interessent:innen für Räume; Teilnehmer:innen von Kursen im Zusatzmodul Räume (§ 1.6); Beschäftigte und sonstige Nutzer:innen, denen der Verantwortliche Zugang zum System einräumt.

2.4. **Gästedaten:** Name, E-Mail-Adresse, Telefonnummer, Sprache, optional Postanschrift und Geburtstag; Reservierungsdaten (Datum, Uhrzeit, Dauer, Personenzahl, Tisch und Bereich, Status, Buchungsweg, Anlass, Wunsch nach barrierefreiem Zugang oder Kindersitzen, Anmerkungen des Gastes und des Personals); Besuchshistorie einschließlich der Zahl der Besuche, Stornierungen und Fälle von Nichterscheinen; vom Verantwortlichen vergebene Merkmale, Vorlieben, Notizen, Verknüpfungen mit anderen Gästen, VIP- und Sperrvermerke; Nachrichten an den Gast; Angaben zu Allergien, Unverträglichkeiten und Ernährungsformen; Einwilligung in Werbekommunikation samt Nachweis (Zeitpunkt, IP-Adresse); bei Kartenhinterlegung die Kennung des Gastes beim Zahlungsdienstleister sowie Betrag und Status der Hinterlegung oder einer eingezogenen Gebühr — Kartennummern erhält der Auftragsverarbeiter nicht.

2.5. **Daten von Interessent:innen und Kursteilnehmer:innen im Zusatzmodul Räume:** Name, Kontaktdaten, Wunschtermin und Nachricht; bei Kursen gebuchte Einheiten, Warteliste, Stornierungen und Guthaben (Blöcke und Abos).

2.6. **Nutzerdaten:** Name, E-Mail-Adresse, Rolle und Berechtigungen, Anmeldezeitpunkte, Kennungen der Geräte, auf denen Benachrichtigungen aktiviert wurden, sowie Protokolle sicherheitsrelevanter Vorgänge einschließlich IP-Adresse.

2.7. **Besondere Kategorien (Art. 9 DSGVO):** Angaben zu Lebensmittelallergien und Unverträglichkeiten sind Gesundheitsdaten im Sinne des Art. 4 Z 15 DSGVO. Sie werden nur verarbeitet, wenn der Gast sie selbst angibt oder das Personal des Verantwortlichen sie einträgt. Der Auftragsverarbeiter übernimmt Angaben aus der Anmerkung eines Gastes nicht selbsttätig in die Gästekartei. Der Verantwortliche stellt die Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO sicher — insbesondere die ausdrückliche Einwilligung des Gastes, bevor solche Angaben dauerhaft in der Gästekartei gespeichert werden. Gesundheitsdaten werden keinem Sprachmodell übergeben.

2.8. **Ort der Verarbeitung:** Rechenzentrum der Hetzner Online GmbH in Helsinki, Finnland. Sicherungen des Servers verbleiben bei Hetzner in der Europäischen Union; zusätzlich werden die Datenbanken täglich verschlüsselt am Unternehmenssitz des Auftragsverarbeiters in Österreich gesichert. Eine Verarbeitung außerhalb der Europäischen Union findet nur im Rahmen von § 7 und Anlage 2 statt.

2.9. **Abgrenzung:** Nicht Gegenstand dieser Vereinbarung sind personenbezogene Daten, die der Auftragsverarbeiter zur Erfüllung eigener gesetzlicher oder vertraglicher Pflichten gegenüber dem Verantwortlichen verarbeitet — insbesondere Vertrags-, Rechnungs- und Zahlungsdaten des Verantwortlichen selbst. Insoweit ist der Auftragsverarbeiter eigener Verantwortlicher.

§ 3 Weisungsrecht

3.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet. In einem solchen Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2. Die Nutzung der Funktionen des Systems durch den Verantwortlichen und die von ihm berechtigten Nutzer:innen gilt als Weisung im Sinne dieser Vereinbarung. Darüber hinausgehende Einzelweisungen bedürfen der Textform.

3.3. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt. Er ist berechtigt, die Durchführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

§ 4 Pflichten des Auftragsverarbeiters

4.1. Der Auftragsverarbeiter verpflichtet alle zur Verarbeitung befugten Personen zur Vertraulichkeit, soweit diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

4.2. Der Kreis der zugriffsberechtigten Personen ist auf das für den Betrieb und die Wartung erforderliche Maß beschränkt. Der Auftragsverarbeiter führt hierüber eine Übersicht und legt sie dem Verantwortlichen auf Verlangen vor.

4.3. Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Diese sind in Anlage 1 beschrieben. Er darf sie fortentwickeln, sofern das Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er.

4.4. Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

4.5. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, soweit sie sich auf diese Auftragsverarbeitung beziehen.

§ 5 Unterstützung des Verantwortlichen

5.1. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit angemessenen technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art. 15 bis 22 DSGVO) zu erfüllen. Das System bietet dafür insbesondere das Bearbeiten und das unwiderrufliche Löschen von Gästekarten samt der Kopien in deren Reservierungen.

5.2. Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst.

5.3. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, bei der Meldung von Verletzungen des Schutzes personenbezogener Daten und bei einer allfälligen Datenschutz-Folgenabschätzung.

5.4. Für Unterstützungsleistungen, die über den vertragsgemäßen Funktionsumfang des Systems hinausgehen und vom Verantwortlichen zu vertreten sind, kann der Auftragsverarbeiter eine angemessene Vergütung verlangen. Leistungen nach 5.1 bis 5.3 im üblichen Umfang sind mit dem Entgelt aus dem Hauptvertrag abgegolten.

§ 6 Verletzung des Schutzes personenbezogener Daten

6.1. Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch binnen 24 Stunden ab Kenntnis. Die Meldung geht an die E-Mail-Adresse des Kundenkontos.

6.2. Die Meldung enthält, soweit bekannt, eine Beschreibung der Art der Verletzung, die betroffenen Kategorien und die ungefähre Zahl betroffener Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Gegenmaßnahmen. Fehlende Angaben werden ohne unangemessene Verzögerung nachgereicht.

6.3. Der Auftragsverarbeiter ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und dokumentiert den Vorfall.

§ 7 Unterauftragsverarbeiter

7.1. Der Verantwortliche erteilt hiermit seine allgemeine Genehmigung zur Beauftragung weiterer Auftragsverarbeiter. Die bei Abschluss dieser Fassung eingesetzten Unterauftragsverarbeiter sind in Anlage 2 Teil A abschließend aufgeführt und gelten als genehmigt.

7.2. Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier Wochen vor jeder beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform an die E-Mail-Adresse des Kundenkontos. Der Verantwortliche kann binnen zwei Wochen ab Zugang aus wichtigem, datenschutzrechtlich begründetem Anlass widersprechen. Im Fall eines berechtigten Widerspruchs, der eine Fortführung der Leistung unmöglich macht, ist jede Partei berechtigt, den Hauptvertrag mit einer Frist von einem Monat zu kündigen.

7.3. Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter durch Vertrag im Wesentlichen dieselben Datenschutzpflichten auf, die ihm selbst obliegen. Er bleibt dem Verantwortlichen gegenüber für die Einhaltung verantwortlich.

7.4. Eine Übermittlung in ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind; die Grundlage ist in Anlage 2 je Dienst genannt.

7.5. Nicht als Unterauftragsverarbeitung gelten Nebenleistungen ohne Zugriff auf die vertragsgegenständlichen Daten (etwa Telekommunikation, Postdienste, Wartung ohne Zugriff auf personenbezogene Daten) sowie die in Anlage 2 Teil B genannten Dienste.

§ 8 Kontrollrechte des Verantwortlichen

8.1. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen.

8.2. Der Nachweis kann durch aktuelle Selbstauskünfte, durch die Beschreibung der Maßnahmen nach Anlage 1 oder durch Zertifikate und Prüfberichte anerkannter Stellen erbracht werden.

8.3. Vor-Ort-Kontrollen sind während der üblichen Geschäftszeiten nach Ankündigung mit angemessener Frist, in der Regel zwei Wochen, zulässig. Sie dürfen den Betriebsablauf nicht unverhältnismäßig stören. Der Verantwortliche trägt die ihm entstehenden Kosten; für den Aufwand des Auftragsverarbeiters kann bei wiederholten Kontrollen innerhalb eines Jahres eine angemessene Vergütung vereinbart werden.

8.4. Kontrollpersonen, die zu einem Wettbewerber des Auftragsverarbeiters in einem Naheverhältnis stehen, kann der Auftragsverarbeiter aus berechtigtem Grund ablehnen.

§ 9 Rückgabe und Löschung

9.1. Der Verantwortliche kann die von ihm verarbeiteten Daten während der gesamten Vertragslaufzeit über die Funktionen des Systems einsehen. Einen Export in einem gängigen, maschinenlesbaren Format stellt der Auftragsverarbeiter auf Verlangen in Textform binnen 14 Tagen bereit.

9.2. Nach Beendigung des Hauptvertrags stellt der Auftragsverarbeiter dem Verantwortlichen die Daten für 30 Kalendertage zum Export bereit; der Export erfolgt auf Verlangen in Textform in einem gängigen, maschinenlesbaren Format. Nach Ablauf dieser Frist löscht er sämtliche vertragsgegenständlichen personenbezogenen Daten aus den produktiven Systemen; ein bis dahin verlangter Export wird binnen 14 Tagen übergeben, gelöscht wird in diesem Fall erst danach.

9.3. In Sicherungskopien enthaltene Daten werden nicht gesondert gelöscht, sondern verfallen mit dem regulären Rotationszyklus der Sicherungen von höchstens 14 Tagen; die vollständige Löschung ist damit spätestens 14 Tage nach der Löschung aus den produktiven Systemen abgeschlossen. Bis dahin unterliegen die Sicherungen unverändert dieser Vereinbarung.

9.4. Von der Löschung ausgenommen sind Daten, für die den Auftragsverarbeiter eine gesetzliche Aufbewahrungspflicht trifft, insbesondere nach § 132 BAO. Diese Daten werden für die Dauer der Aufbewahrungspflicht gesperrt und ausschließlich zu diesem Zweck verarbeitet.

9.5. Der Auftragsverarbeiter bestätigt die Löschung auf Verlangen in Textform.

§ 10 Haftung

10.1. Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO.

10.2. Im Innenverhältnis haftet jede Partei für Schäden, die aus einer von ihr zu vertretenden Verletzung dieser Vereinbarung oder datenschutzrechtlicher Bestimmungen entstehen, nach den allgemeinen gesetzlichen Vorschriften. Die Haftungsbeschränkung des Hauptvertrags (AGB Punkt 9) gilt auch für diese Vereinbarung, soweit sie nicht Ansprüche betroffener Personen nach Art. 82 DSGVO betrifft und soweit dies gesetzlich zulässig ist.

§ 11 Schlussbestimmungen

11.1. Änderungen dieser Vereinbarung erfolgen durch eine neue Fassung. Der Auftragsverarbeiter teilt sie dem Verantwortlichen mindestens sechs Wochen vor Inkrafttreten in Textform mit und weist auf das Recht hin, zu widersprechen. Widerspricht der Verantwortliche nicht bis zum Inkrafttreten, gilt die neue Fassung. Widerspricht er, gilt die bisherige Fassung weiter; jede Partei kann den Hauptvertrag dann mit einer Frist von einem Monat kündigen. Für neue Unterauftragsverarbeiter gilt § 7 Abs. 2. Jede Fassung bleibt unter restl.at/avv/<datum> abrufbar.

11.2. Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame zu ersetzen, die dem Zweck am nächsten kommt.

11.3. Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen des Internationalen Privatrechts und des UN-Kaufrechts. Zwingende Bestimmungen der DSGVO bleiben unberührt.

11.4. Ausschließlicher Gerichtsstand für Streitigkeiten aus dieser Vereinbarung ist das sachlich zuständige Gericht am Sitz des Auftragsverarbeiters, sofern der Verantwortliche Unternehmer ist.

11.5. Bestandteil dieser Vereinbarung sind Anlage 1 (Technische und organisatorische Maßnahmen) und Anlage 2 (Unterauftragsverarbeiter).

Anlage 1 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Zutrittskontrolle. Die Server stehen in Rechenzentren der Hetzner Online GmbH (Helsinki, Finnland; ein weiterer Server für Fehler-Tracking und Erreichbarkeitsprüfung in Nürnberg, Deutschland). Den physischen Zutritt kontrolliert der Betreiber (Zutrittssystem, Videoüberwachung, Protokollierung); der Auftragsverarbeiter hat selbst keinen physischen Zutritt. Die Sicherungskopien am Unternehmenssitz liegen in einem versperrten Raum.

Zugangskontrolle. Anmeldung ausschließlich über einen selbst betriebenen Identity Provider (Keycloak) mittels OpenID Connect, mit Passkeys (WebAuthn, Touch ID, Face ID, Windows Hello) oder Passwort. Passwortrichtlinie: mindestens zwölf Zeichen, Sperre der letzten fünf Passwörter, Verbot von Benutzername und E-Mail-Adresse als Passwort; automatische Sperre nach wiederholten Fehlversuchen. Die Anwendung selbst speichert keine Passwörter. Sitzungen sind an den jeweiligen Host gebunden. Serverzugang ausschließlich über SSH-Schlüssel, Passwortanmeldung deaktiviert, automatische IP-Sperre bei Angriffsmustern.

Zugriffskontrolle. Rollenbasierte Berechtigungen je Betrieb (Eigentümer:in, Administrator:in, Mitarbeiter:in, Beobachter:in, Mieter:in) mit abgestuftem Funktionsumfang; Mieter:innen sehen nur ihre eigenen Daten. Die Rechteprüfung ist zentral umgesetzt und automatisiert getestet.

Trennungskontrolle. Mandantentrennung auf Datenbankebene durch Row Level Security mit erzwungener Anwendung (FORCE) auf allen mandantenbezogenen Tabellen. Die Anwendung verbindet sich mit einer eingeschränkten Datenbankrolle und setzt den Mandantenbezug je Anfrage; ein fehlerhaft eingeschränkter Zugriff liefert dadurch keine fremden Daten, sondern ein leeres Ergebnis. Zwei automatisierte Prüfungen verhindern die Einführung ungeschützter Tabellen. Neue Versionen werden vor dem Einsatz in einer getrennten Testumgebung mit eigener Anmeldung und ohne Daten der Kund:innen geprüft.

Anonymisierung. Gästekarten können auf Veranlassung des Verantwortlichen unwiderruflich gelöscht werden; dabei werden Name, Kontaktdaten, Anschrift, Gesundheits- und Ernährungsangaben, Merkmale und Notizen auch aus den Reservierungen entfernt, während die statistische Auswertbarkeit erhalten bleibt.

Sichtschutz am Arbeitsplatz. Im Verwaltungsbereich werden Namen, Kontaktdaten, Anmerkungen und Gesundheitsangaben nach 60 Sekunden ohne Bedienung sowie beim Wechsel in den Hintergrund unscharf dargestellt, damit sie am Tresen nicht von Dritten mitgelesen werden können.

Übertragungskontrolle. Sämtliche Verbindungen ausschließlich über TLS (mindestens Version 1.2) mit HTTP Strict Transport Security. Die Server sind über ausgehende, authentifizierte Tunnel angebunden; eingehende Ports der Anwendung sind nicht öffentlich erreichbar; Verbindungen zwischen den Servern laufen über ein verschlüsseltes privates Netz (WireGuard). E-Mail-Versand über TLS-gesicherte Verbindung (STARTTLS erzwungen). Benachrichtigungen an Geräte der Nutzer:innen werden Ende-zu-Ende verschlüsselt (RFC 8291).

Eingabekontrolle. Protokollierung sicherheits- und datenschutzrelevanter Vorgänge mit Zeitpunkt und handelnder Person. Auffällige Zugriffsversuche werden als Sicherheitsereignis erfasst und bei kritischer Einstufung unverzüglich gemeldet; Sicherheitsmeldungen an den Auftragsverarbeiter (Telegram, E-Mail) enthalten weder Namen noch E-Mail- oder IP-Adressen, die Einzelheiten stehen nur im geschützten Verwaltungsbereich. Fehlermeldungen an das eigene Fehler-Tracking enthalten weder den Fehlertext noch personenbezogene Daten.

Verschlüsselung ruhender Daten. Die Datenträger der Server sind nicht zusätzlich verschlüsselt; der Schutz beruht auf der physischen Sicherung des Rechenzentrums, der Zugangsbeschränkung und der Löschung der Datenträger durch den Betreiber bei Außerbetriebnahme. Die Datenbanksicherungen am Unternehmenssitz sind verschlüsselt (CMS); der Schlüssel zum Entschlüsseln wird getrennt von den Sicherungen aufbewahrt. Passwörter liegen ausschließlich als kryptografische Hashwerte im Identity Provider.

Datensicherung. Tägliche vollständige Sicherung der Datenbanken um 02:30 Uhr, verschlüsselt übertragen und abgelegt an einem räumlich getrennten Ort am Unternehmenssitz in Österreich, Aufbewahrung 14 Tage im rollierenden Verfahren; Erfolg und Fehlschlag werden automatisch überwacht und gemeldet. Zusätzlich Sicherungen des Servers durch Hetzner (sieben Stände) und vor dem Einspielen einer neuen Version oder vor Eingriffen in die Anmeldung ein Abzug der betroffenen Datenbank auf dem Server selbst, der spätestens nach sieben Tagen automatisch gelöscht wird — zusammen mit den Serversicherungen verfallen damit alle Sicherungen nach höchstens 14 Tagen.

Wiederherstellbarkeit. Wiederherstellung aus der jeweils letzten Sicherung nach dokumentiertem Verfahren; vor dem Einspielen einer neuen Version wird die Datenbank gesichert, und eine frühere Version kann ohne Neubau wiederhergestellt werden. Ein Bereitschaftssystem mit automatischer Umschaltung besteht nicht — im Störungsfall ist mit einer Wiederherstellungsdauer im Bereich von Stunden zu rechnen.

Schutz vor Angriffen. Vorgelagerter Schutz gegen Überlastungsangriffe und Angriffe auf Anwendungsebene durch den CDN-Anbieter; Begrenzung der Anfragen je Absender auf den öffentlichen Buchungswegen; sicherheitsrelevante HTTP-Kopfzeilen; die Anwendung läuft in Containern ohne erweiterte Rechte.

Überprüfung. Eine Sicherheitsüberprüfung nach den OWASP-Kriterien wurde zuletzt am 24. September 2026 durchgeführt und dokumentiert; die Behebung der Feststellungen wird nachgehalten. Der Programmcode ist durch mehr als 2.500 automatisierte Tests abgesichert, darunter Prüfungen, die verhindern, dass Personendaten in Fehlermeldungen, Gast-Mails oder öffentliche Antworten gelangen.

Verfahren zur regelmäßigen Überprüfung. Die Maßnahmen werden mindestens jährlich sowie anlassbezogen überprüft und an den Stand der Technik angepasst. Datenschutzvorfälle werden nach § 6 behandelt und dokumentiert. Administrativen Zugriff auf Server und Datenbanken hat ausschließlich der Geschäftsführer der ARQOS GmbH. Den internen Verwaltungsbereich von RESTL nutzen zusätzlich einzelne Mitarbeiter:innen, soweit sie ihn für die Betreuung der Kund:innen und die Bearbeitung von Sicherheitsereignissen benötigen. Sie sind vorher auf die Vertraulichkeit verpflichtet (§ 4.1) und in der Übersicht nach § 4.2 geführt; wer hinzukommt, wird ebenso vorher verpflichtet und aufgenommen.

Anlage 2 — Unterauftragsverarbeiter

Teil A — genehmigte Unterauftragsverarbeiter (Stand 13.11.2026):

1. Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland. Leistung: Bereitstellung der Server- und Speicherinfrastruktur (Hosting) einschließlich der Sicherungen des Servers. Daten: sämtliche vertragsgegenständlichen Daten. Ort: Rechenzentren in Helsinki, Finnland, und Nürnberg, Deutschland; kein Drittlandtransfer.

2. Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA. Leistung: Netz vor allen Diensten des Systems (Transportverschlüsselung, Weiterleitung, Schutz vor Angriffen, Namensauflösung); Speicherung hochgeladener Bilder (Logos, Raumfotos) in einem Speicher mit EU-Bindung. Daten: sämtliche übertragenen Inhalte im Durchlauf, ohne dauerhafte Speicherung, sowie Verbindungsdaten (insbesondere IP-Adresse und Zeitpunkt); hochgeladene Bilder. Ort und Grundlage: weltweites Netz, Unternehmen in den USA; Zertifizierung nach dem EU-US Data Privacy Framework und Standardvertragsklauseln der EU.

3. Sendinblue GmbH („Brevo“), Berlin, Deutschland. Leistung: Versand der E-Mails an Gäste (Bestätigung, Erinnerung, Änderung, Stornierung, Hinweise, Einwilligungsbestätigung, mit Einwilligung Nachrichten nach dem Besuch; im Zusatzmodul Räume Kursbuchungen) und an den Verantwortlichen und seine Nutzer:innen (Benachrichtigungen, Einladungen, Anmelde- und Passwort-E-Mails). Daten: Name und E-Mail-Adresse der Empfänger:innen und der Inhalt der Nachricht, also Reservierungsdaten einschließlich der Anmerkung des Gastes, die Angaben zu Allergien enthalten kann; keine Notizen, Merkmale oder Gesundheitsangaben aus der Gästekartei. Ort: Europäische Union; kein Drittlandtransfer.

4. Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland — nur wenn der Verantwortliche die Kartenhinterlegung nutzt. Leistung: Hinterlegung einer Zahlungskarte gegen Nichterscheinen und Einzug einer Gebühr über das Stripe-Konto des Verantwortlichen (Stripe Connect), für das der Verantwortliche einen eigenen Vertrag mit Stripe schließt. Daten: Name und E-Mail-Adresse des Gastes und eine Kennung der Reservierung; die Kartendaten gibt der Gast unmittelbar bei Stripe ein, der Auftragsverarbeiter erhält sie nicht. Stripe verarbeitet Zahlungsdaten teils als eigener Verantwortlicher. Ort und Grundlage: Europäische Union; Übermittlungen innerhalb der Stripe-Gruppe in die USA auf Grundlage des EU-US Data Privacy Framework und der Standardvertragsklauseln der EU.

5. Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland. Leistung: E-Mail-Postfach des Auftragsverarbeiters (Microsoft 365) für Anfragen des Verantwortlichen, seiner Nutzer:innen und betroffener Personen (Unterstützung, Auskunfts- und Löschbegehren). Daten: der Inhalt dieser E-Mails, soweit er Gäste- oder Nutzerdaten enthält. Ort und Grundlage: Rechenzentren in der Europäischen Union (EU-Datengrenze von Microsoft); Übermittlungen an die Microsoft Corporation in den USA nur im Ausnahmefall auf Grundlage des EU-US Data Privacy Framework und der Standardvertragsklauseln der EU.

Teil B — keine Unterauftragsverarbeiter, zur Information:

Selbst betrieben. Der Identity Provider (Keycloak), das Fehler-Tracking (GlitchTip) und die Erreichbarkeitsprüfung laufen auf Servern des Auftragsverarbeiters bei Hetzner (Teil A Nr. 1). Fehlermeldungen enthalten keine personenbezogenen Daten; die Erreichbarkeitsprüfung ruft nur öffentliche Seiten auf. Die Webanalyse (Matomo, selbst betrieben) läuft nur auf restl.at, nicht im System oder im Buchungsfenster.

Push-Dienste der Geräte- und Browserhersteller (Apple, Google, Mozilla, Microsoft). Aktiviert eine Nutzer:in Benachrichtigungen auf ihrem Gerät, stellt der vom Gerät gewählte Dienst sie zu. Der Inhalt ist Ende-zu-Ende verschlüsselt (RFC 8291) und für den Dienst nicht lesbar; er sieht nur die Gerätekennung und den Zeitpunkt.

KI-Assistenten der Gäste (etwa ChatGPT oder Claude). Bucht ein Gast über seinen KI-Assistenten, wählt er dessen Anbieter selbst, und dieser verarbeitet die Eingaben in eigener Verantwortung. Der Auftragsverarbeiter übermittelt dorthin Verfügbarkeiten und die Bestätigung der Reservierung.

Sprachmodell (Amazon Web Services, Bedrock, EU-Regionen). Erhält ausschließlich die Selbstbeschreibung des Betriebs, um Schlagworte für die Suche vorzuschlagen — keine Gäste- und keine Nutzerdaten.

Eigene Verantwortung des Auftragsverarbeiters. Der Zahlungsdienstleister für die Entgelte des Hauptvertrags (Stripe), die Buchhaltungsablage (Microsoft 365) und das Archiv der Rechnungen und Verträge (Cloudflare) verarbeiten ausschließlich Vertrags- und Rechnungsdaten des Verantwortlichen als Vertragspartner (§ 2.9). Betriebsmeldungen an den Auftragsverarbeiter (Telegram) enthalten keine personenbezogenen Daten.