Reservly

Vertrag über Auftragsverarbeitung nach Art. 28 DSGVO

(„Auftragsverarbeitungsvertrag“ / „Data Processing Agreement“)

Stand: 15.10.2026 Version: 4.5

zwischen

Lukas Gerber, Einzelunternehmer, handelnd unter „Reservly“

Wassergasse 32, 1030 Wien, Österreich

GISA-Zahl: 40050812

E-Mail: support@reservly.at

Kontakt für Datenschutzanfragen: support@reservly.at

– nachfolgend „Auftragsverarbeiter“ –

und

dem jeweils im Registrierungs- und Onboarding-Prozess benannten Restaurant / Unternehmen, dessen Stammdaten im Kundenkonto des Reservierungssystems hinterlegt sind

– nachfolgend „Verantwortlicher“ –

gemeinsam auch die „Parteien“.

> Hinweis zur elektronischen Form: Dieser Vertrag wird elektronisch im Rahmen des Online-Onboardings abgeschlossen. Mit der dort vorgesehenen ausdrücklichen Bestätigung (z. B. Checkbox) akzeptiert der Verantwortliche diesen Vertrag in der jeweils angezeigten Version. Diese elektronische Form genügt dem Schriftformerfordernis im Sinne von Art. 28 Abs. 9 DSGVO.

1. Präambel

(1) Der Auftragsverarbeiter betreibt ein webbasiertes Online-Reservierungssystem („Reservierungssystem“), bestehend insbesondere aus

- einem vom Auftragsverarbeiter gehosteten, per iFrame einbindbaren Reservierungs-Widget für Gäste, das (a) auf vom Verantwortlichen betriebenen Websites oder (b) auf vom Auftragsverarbeiter im Auftrag des Verantwortlichen bereitgestellten öffentlichen Restaurant-Unterseiten (z. B. unter reservly.at/restaurant/…), die durch den Auftragsverarbeiter über ein CMS/Hosting bereitgestellt werden, eingebunden werden kann, sowie
- einem webbasierten Backoffice-Dashboard (Multi-Tenant-Webanwendung) für Restaurants zur Einsicht und Verwaltung der über das Reservierungssystem eingegangenen Reservierungen. Das reservierungsbezogene Nachrichtencenter ist regulärer Bestandteil des Reservierungssystems für Restaurants und setzt keine gesonderte Freischaltung voraus. Für den Zugriff gelten die jeweiligen Benutzerrechte.

(2) Der Auftragsverarbeiter stellt dem Verantwortlichen das Reservierungssystem im Modell „Software as a Service“ (SaaS) zur Verfügung. Der Verantwortliche entscheidet allein darüber, auf welchen Websites oder Online-Auftritten das Reservierungs-Widget über ein iFrame eingebunden wird, bzw. ob er die vom Auftragsverarbeiter bereitgestellten öffentlichen Restaurant-Unterseiten nutzt, und wie die eingehenden Reservierungen organisatorisch genutzt werden.

(3) Der Verantwortliche nutzt das Reservierungssystem zur Annahme und Verwaltung von Reservierungen seiner Gäste. Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen im Sinne von Art. 4 Nr. 7 und Nr. 8 sowie Art. 28 DSGVO.

(4) Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag.

2. Begriffsbestimmungen

(1) Es gelten die Begriffsbestimmungen der Datenschutz-Grundverordnung (DSGVO), insbesondere die in Art. 4 DSGVO definierten Begriffe wie „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „Empfänger“, „Dritter“, „Verletzung des Schutzes personenbezogener Daten“ und „Aufsichtsbehörde“.

(2) Soweit in diesem Vertrag Begriffe verwendet werden, die in der DSGVO definiert sind, sind diese im Sinne der DSGVO zu verstehen.

3. Gegenstand und Dauer der Verarbeitung

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung und des Betriebs des Reservierungssystems für den Verantwortlichen.

(2) Die Einzelheiten der Leistung (Funktionsumfang, Laufzeit, Vergütung) ergeben sich aus dem jeweils zugrunde liegenden Hauptvertrag (SaaS-/Nutzungsvertrag) zwischen den Parteien.

(3) Die Dauer dieses Auftragsverarbeitungsvertrags entspricht der Laufzeit des Hauptvertrags. Er endet automatisch mit Beendigung des Hauptvertrags, sofern sich aus diesem Vertrag keine darüber hinausgehenden Pflichten (insbesondere Lösch- und Nachweispflichten) ergeben.

4. Art, Zweck und Rechtsgrundlagen der Verarbeitung

4.1 Art und Zweck der Verarbeitung im Auftrag

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zu folgenden Zwecken:

1. **Online-Reservierungen**
    - Entgegennahme, Verarbeitung und Speicherung von Online-Reservierungsanfragen über das Reservierungs-Widget (z. B. Next.js-Widget, eingebettet per iFrame auf der Website des Verantwortlichen).
    - Berechnung und Anzeige von verfügbaren Zeitfenstern (Slots) anhand von Öffnungszeiten, Tischkapazitäten, Pacing-Regeln und Turnover-Zeiten.
    - Erstellung, Änderung und Stornierung von Reservierungen.
    - Je nach Einstellung des Verantwortlichen sofortige Bestätigung einer Onlinebuchung oder Speicherung als Reservierungsanfrage, die das Restaurant annimmt oder ablehnt; die Einstellung kann für alle Buchungen oder nach Regeln zu Wochentag, Uhrzeit und Personenzahl gelten. Verarbeitet werden zusätzlich der Anfragestatus (angefragt, bestätigt, abgelehnt, abgelaufen), die Bearbeiterkennung sowie eine optionale Nachricht des Restaurants zur Entscheidung. Der Gast erhält E-Mails zu Eingang, Annahme, Ablehnung oder Ablauf der Anfrage, das Restaurant eine Benachrichtigung über neue Anfragen. Nicht bearbeitete Anfragen verfallen zum Reservierungszeitpunkt. Die Nachricht zur Entscheidung wird nach dem Versand aus dem Ereignisprotokoll entfernt und bleibt nur als Kopie der versandten E-Mail im Nachrichtencenter nach dessen Frist erhalten. Die Regeln entscheiden nur, ob das Restaurant eine Buchung selbst prüft; eine ausschließlich automatisierte Entscheidung nach Art. 22 DSGVO findet nicht statt.
2. **Öffentliche Restaurant-Unterseiten** (optional)
    - Bereitstellung und Betrieb öffentlicher Restaurant-Unterseiten (z. B. reservly.at/restaurant/…) inkl. Einbindung des Reservierungs-Widgets per iFrame

sowie Verarbeitung technisch notwendiger Zugriffsdaten zur Auslieferung, Sicherheit und Fehleranalyse.

3. **Dashboard / Backoffice**
    - Bereitstellung eines mandantenbezogenen Dashboards zur Verwaltung von Reservierungen und Gästekontakten, einschließlich Suche, Zuordnung wiederkehrender Reservierungen, Gästehistorie und erforderlicher Zusammenführung doppelter Gastprofile. Die Verarbeitung erfolgt ausschließlich für den jeweiligen Restaurantbetrieb und auf dessen Weisung. Betriebliche Statistiken werden soweit möglich aggregiert erstellt. Pseudonymisierte oder einem Gast zuordenbare Historien bleiben personenbezogen. Zum restaurantbezogenen Gästebuch gehören auch manuell angelegte Kontakte ohne Rewards-Konto, Firma, bevorzugte Sprachen, Tags, manuelle Gruppenzuordnungen, Textnotizen mit Erinnerungsdatum und Dateianhänge. Bei Dateien werden Inhalt, Dateiname, Dateityp, Größe, Speicherpfad, Gast- und Restaurantzuordnung sowie Uploadzeitpunkt verarbeitet; bei Notizen und Gruppen können Erstellerkennung und Bearbeitungszeitpunkte hinzukommen. Ein vollständiges Geburtsdatum kann bei selbst angelegten Kontakten erfasst und bearbeitet werden. Bei aus Rewards übernommenen Geburtstagsdaten bleibt die Restaurantanzeige auf Tag und Monat beschränkt. Smartgruppen bestimmen die Zugehörigkeit anhand gespeicherter Regeln und aktuell verfügbarer Daten. Technisch verfügbare Kriterien betreffen unter anderem Reservierungen, bestätigte Besuche, Mitgliedschaft, Punkte, Prämien, Gutscheine, Geburtstag, zulässige Tags und Kommunikationsfreigaben. Die Verfügbarkeit eines Kriteriums erlaubt dessen werbliche Nutzung noch nicht. Zulässige Kriterien und Kombinationen richten sich nach der jeweiligen Einwilligung. Die Bewertung persönlicher Aspekte oder Verhaltensweisen ist Profiling; eine rechtliche oder ähnlich erhebliche Wirkung nach Art. 22 DSGVO ist hierfür nicht erforderlich.
    - Notizinhalte, Reservierungsnachrichten und Dateianhänge dürfen weder unmittelbar noch über daraus abgeleitete Tags oder manuelle Gruppen zur Auswahl von Werbung verwendet werden. Besondere Datenkategorien nach Art. 9 DSGVO, insbesondere Gesundheitsdaten, sowie daraus abgeleitete sensible Merkmale und diskriminierende Kriterien sind für diese Auswahl ausgeschlossen. Auch sonstige Tags und Gruppen dürfen keine solchen Merkmale enthalten. Daten aus anderen Restaurantprogrammen und externes Tracking werden für diese Auswahl nicht herangezogen.
    - Für die hier geregelte personalisierte Restaurantwerbung beruhen Versand und personenbezogene Angebotsauswahl auf einer freiwilligen, informierten Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO; für elektronische Werbung gilt zusätzlich § 174 TKG 2021. Die Reservierungszustimmung erlaubt personalisierte E-Mail-Werbung anhand der erläuterten Reservierungs- und, bei Teilnahme, Treueprogrammdaten desselben Restaurants. Die Loyalty-Zustimmung erlaubt zusätzlich personalisierte Angebote in der App und per Push; Push setzt außerdem die Gerätefreigabe voraus. Die vor Zustimmung unmittelbar zugänglichen Datenschutzhinweise konkretisieren Reservierungsmerkmale, Mitgliedschaft, Besuche, Punkte beziehungsweise Stempel, Prämien und Gutscheine sowie deren Verknüpfung, auch bei späterer Teilnahme. Ein gemeinsames Gästeprofil und ein gemeinsamer Marketing-Schalter bleiben möglich; die zugehörigen Nachweise bestimmen die tatsächlich erlaubten Kanäle und Datenarten. Beim Loyalty-Beitritt ohne Marketingzustimmung bleibt eine bereits wirksam bestehende E-Mail-Erlaubnis erhalten; App- und Push-Werbung werden nicht freigegeben beziehungsweise ausgeschaltet. Ohne bestehende E-Mail-Erlaubnis entsteht dadurch keine neue Werbeerlaubnis. Ein vollständiger Widerruf über „Alle Angebote deaktivieren“ oder die vollständige Abmeldung über den

Abmeldelink einer Werbe-E-Mail beendet dagegen sämtliche Restaurantwerbung und die zugehörige werbliche Auswahl, auch für noch nicht versendete Kampagnen. Nach einer Abschaltung oder einem Widerruf erlaubt eine neue Reservierungszustimmung nur wieder E-Mail-Werbung; App und Push benötigen eine passende neue Loyalty-Zustimmung. Eine weiterhin wirksame Loyalty-Zustimmung wird durch eine zusätzliche E-Mail-Zustimmung nicht eingeschränkt. Engere Bestandszustimmungen werden nicht automatisch erweitert. Jede tatsächliche Erweiterung, insbesondere auf App und Push, ist auch bei bereits aktivem Marketing neu nachzuweisen. Beitritt, App-Installation, Profilzuordnung und Import ersetzen keine Zustimmung. Geburtstags- und Standortwerbung, freie Tags sowie zusätzliche Kontakt-, Geräte- oder App-Merkmale als Auswahlkriterien sind nicht pauschal umfasst. Eigenständige zusätzliche Zwecke müssen gesondert wählbar sein. Notiz-, Reservierungsnachrichten- und Dateiinhalte sowie sensible Ableitungen bleiben ausgeschlossen. Vor Auswahl und Versand sind Nachweise, Kanal- und Datenumfang, Widerrufe und Teilnahmevoraussetzungen zu beachten.

- Vor der werblichen Gruppenzuordnung und vor der Zustellung ist der aktuelle, nachgewiesene Umfang der Einwilligung zu beachten. Nicht gedeckte Datenquellen und Filterkombinationen sind für die betroffene Person auszuschließen. Eine frühere allgemeine Zustimmung zu Rabatten oder Neuigkeiten wird durch neue Texte, importierte Statuswerte oder einen Programmbeitritt nicht erweitert. Für eine Erweiterung ist vorher eine neue bestätigende Erklärung mit dem dann geltenden Text nachzuweisen. Fehlende Einwilligungen oder Widerrufe werden für diese werbliche Auswahl nicht durch berechtigtes Interesse ersetzt. Erforderliche organisatorische Verarbeitung für Reservierung, Gästebuch und Programm bleibt nach ihrer eigenen Rechtsgrundlage getrennt.
- Eine Einwilligung kann jederzeit für die Zukunft widerrufen werden; außerdem kann Direktwerbung einschließlich der zugehörigen Auswahl und Profilbildung jederzeit kostenfrei und ohne Begründung nach Art. 21 Abs. 2 und 3 DSGVO widersprochen werden. Die betroffene Werbeverarbeitung muss dann enden, auch für bereits vorbereitete Kampagnen. Reservierung, Programmteilnahme und bestehende Punkte oder Prämienansprüche bleiben davon unberührt. Erforderliche eingeschränkte Nachweise dürfen nach den vorgesehenen Fristen fortbestehen und berechtigen nicht zu weiterer Werbung.

4. **Kommunikation**

- Versand notwendiger Reservierungs-E-Mails über Resend (Plus Five Five, Inc., USA), insbesondere Bestätigungen, Änderungen, Stornierungen und Erinnerungen, gegebenenfalls mit ICS-Kalenderdatei, sowie Übermittlung individueller reservierungsbezogener Nachrichten und Empfang zugehöriger E-Mail-Antworten.
- Benachrichtigungen an den Verantwortlichen (z. B. neue Reservierung, neue Reservierungsanfrage, Stornierungen) sowie eine tägliche Zusammenfassung ungelesener Gastnachrichten.

  Das reservierungsbezogene Nachrichtencenter umfasst individuelle ausgehende Nachrichten, eingehende E-Mail-Antworten und gespeicherte Kopien automatischer Reservierungsnachrichten. Es verarbeitet Nachrichtentext und gegebenenfalls Betreff/HTML-Darstellung, Absender und Empfänger, Zeitpunkte, technische Nachrichten- und Antwortzuordnungen, Zustellstatus, Anzahl eingegangener Anhänge, gemeinsame Gelesen- und Sternmarkierungen sowie erforderliche Bearbeiterkennung und Namen. Der Reservierungsverlauf kann frühere und geänderte Kontakt- und Reservierungsangaben enthalten. Eine gemeinsame Gelesen-Markierung ist keine individuelle Lesebestätigung.

Allergien und andere gesundheitsbezogene Angaben gehören nicht in allgemeine Buchungsnotizen, Reservierungsnachrichten oder deren Anhänge. Für einen tatsächlich erforderlichen gesundheitlich bedingten besonderen Bedarf ist mit dem Restaurant vorab ein geeigneter Kontaktweg und eine zulässige Verarbeitung festzulegen. Die bloße Eingabe in ein Freitextfeld ersetzt keine erforderliche ausdrückliche Einwilligung oder andere einschlägige Ausnahme nach Art. 9 DSGVO. Unerwartete sensible Inhalte werden unverzüglich geprüft; soweit sie unzulässig oder nicht mehr erforderlich sind, veranlasst das Restaurant ihre Löschung oder Einschränkung nach Ziffer 13 Absatz 9. Eine Weiterleitung des sensiblen Inhalts an den Support ist dafür nicht erforderlich.

Reservierungsnachrichten einschließlich ihrer Inhalte und daraus abgeleiteter Tags oder Gruppen dürfen nicht für die werbliche Auswahl verwendet werden. Sie werden nicht als Eingaben für die optionale Kampagnen-KI beauftragt. Die bloße Nutzung des Nachrichtencenters, eine Antwort oder eine Kontozuordnung erweitert keine Werbeeinwilligung.

Eine freiwillige Notiz aus dem Onlinebuchungsformular wird zusätzlich als erste Gastnachricht im Nachrichtencenter gespeichert. Es handelt sich um eine eigenständige Kopie; eine spätere Änderung oder Löschung der Reservierungsnotiz entfernt diese Chatnachricht nicht automatisch. Automatische Reservierungs-E-Mails werden mit ihrem vollständigen erzeugten Inhalt einschließlich HTML als Kopie gespeichert.

Antworten an die individuelle Antwortadresse des Nachrichtencenters werden der Reservierung im Dashboard zugeordnet und nicht automatisch an das allgemeine E-Mail-Postfach des Restaurants weitergeleitet. Das Restaurant erhält einmal täglich eine E-Mail an seine hinterlegte Kontaktadresse mit der Anzahl ungelesener Gastnachrichten, ohne Gastnamen oder Nachrichteninhalte. Die Zusammenfassung ist standardmäßig aktiv und in den Einstellungen abschaltbar. Eine Benachrichtigung je einzelner Nachricht gibt es nicht. Nur wenn eine automatische Buchungsmail aus technischen Gründen mit der allgemeinen Restaurantadresse als Antwortadresse versandt wurde, gelangt eine Antwort stattdessen dorthin. Maßgeblich ist die Antwortadresse der konkreten Nachricht.

Resend (Plus Five Five, Inc., USA) empfängt und speichert die eingehende E-Mail einschließlich Inhalt und mitgesendeter Anhänge in den USA. Für den eingesetzten Pro-Tarif beträgt die reguläre laufende Aufbewahrung 30 Tage ab Eingang; Sicherungskopien beim Anbieter folgen dessen eigenem Sicherungszyklus. Im Reservly-Nachrichtencenter werden der aufbereitete Antworttext, Absenderadresse, Betreff, Empfangszeit und Anzahl der Anhänge sowie die erforderlichen Zuordnungsdaten gespeichert. Die vollständigen E-Mail-Anhänge werden dort nicht als Chatdateien angezeigt. Die 30-Tage-Frist beim Empfangsdienstleister ist von der Löschfrist des Chatverlaufs nach Ziffer 13 Absatz 5 zu unterscheiden. Berechtigte frühere Löschungen werden über den Support veranlasst.

Zusätzlich kann das Restaurant aus einem Gästeprofil des Gästebuchs einen direkten Chat mit dem Gast führen (Direktchat), auch ohne Bezug zu einer bestimmten Reservierung. Je Restaurant und Gästeprofil besteht höchstens ein Direktchat. Er setzt eine hinterlegte E-Mail-Adresse voraus und ist nur Nutzern mit Rechten für Nachrichten und Gästebuch zugänglich. Verarbeitet werden dieselben Daten wie im Reservierungschat sowie Name und E-Mail-Adresse des Gasts als Kontaktkopie und die Zuordnung zum Gästeprofil. Antworten werden über eine eigene Antwortadresse über Resend empfangen und dem Direktchat zugeordnet; ist das Gästeprofil im Gästebuch nicht mehr sichtbar, werden eingehende Antworten verworfen. Direktchats dienen der individuellen Kommunikation mit dem Gast. Werbung darf darüber nur unter den Voraussetzungen des § 174 TKG 2021 versandt

werden, insbesondere mit einer passenden Einwilligung; das gilt auch für manuell angelegte oder per CSV importierte Kontakte. Inhalte von Direktchats werden wie Reservierungsnachrichten weder für die werbliche Auswahl noch als Eingaben für die Kampagnen-KI verwendet. Die Löschfrist richtet sich nach Ziffer 13 Absatz 5.

- Feedback (optional): Eine E-Mail mit Bitte um eine Bewertung, gegebenenfalls 48 Stunden nach dem Reservierungstermin, darf nur auf dokumentierte Weisung und bei nachgewiesener Zulässigkeit nach § 174 TKG 2021 sowie der DSGVO versendet werden. Eine Reservierung allein ist keine Werbeeinwilligung. Ohne gültige Grundlage bleibt der Versand deaktiviert. Verarbeitet werden Bewertung, freiwilliger Freitext, technische Zuordnung und Versandstatus; eine Weiterleitung erfolgt nur an berechtigte Restaurantadressen. Eine Veröffentlichung ist nicht beauftragt.

5. **Konfiguration & Administration**
   - Verwaltung von Restaurant-Stammdaten
   - Konfiguration von Öffnungszeiten, Pacing, Tischlogik und sonstigen Systemeinstellungen.
6. **Sicherheit, Stabilität und Missbrauchsschutz**
   - Einsatz von Rate-Limiting-Mechanismen (z. B. Upstash Redis) zur Vermeidung von Missbrauch (z. B. automatisierte Reservierungsversuche), u. a. durch Speicherung einer pseudonymisierten Kennung (Hash einer IP-Adresse mit geheimem Schlüssel) mit kurzer Speicherfrist (max. 1 Stunde).
   - Logging und Monitoring zum Zweck der Störungsanalyse, Fehlerbehebung und Sicherstellung der Verfügbarkeit und Integrität des Systems.
7. **Statistik und Systemoptimierung**
   - Erstellung technischer und betrieblicher Auswertungen (z. B. Auslastung, Anzahl Reservierungen) in aggregierter, pseudonymisierter oder anonymisierter Form, ohne Bezug auf identifizierte natürliche Personen.

4.2 Rechtsgrundlagen

(1) Die Bestimmung einer geeigneten Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Gästen (z. B. Art. 6 Abs. 1 lit. b DSGVO – Vertragserfüllung Bewirtungsvertrag, ggf. lit. f DSGVO – berechtigtes Interesse an effizienter Reservierungsverwaltung) obliegt dem Verantwortlichen.

(2) Gastdaten und Daten zu Mitarbeiterhandlungen, die Reservly ausschließlich für die Reservierungs- und Betriebszwecke des Restaurants verarbeitet, unterliegen dessen Weisungen und Rechtsgrundlagen. Eigene Reservly-Vertrags-, Konto-, Abrechnungs- und Sicherheitszwecke bleiben davon getrennt und werden in den B2B-Datenschutzhinweisen erläutert. Der Restaurantzugang macht nicht sämtliche Daten der handelnden Person zu Auftragsdaten.

(3) Die Verarbeitung technischer Daten zu Zwecken der Sicherheit und Stabilität (insbesondere Rate Limiting mit pseudonymisierten IP-Hashes mit kurzer Speicherfrist) ist notwendige Nebenverarbeitung im Rahmen der Erfüllung des Auftrags zur sicheren Bereitstellung des Systems; sie erfolgt auf Grundlage der vom Verantwortlichen gewählten Rechtsgrundlage und dient zugleich dem berechtigten Interesse an der Gewährleistung der Sicherheit und Verfügbarkeit der Dienste.

5. Kategorien von Daten und betroffenen Personen

5.1 Kategorien personenbezogener Daten

Die Verarbeitung umfasst insbesondere folgende Datenkategorien:

1. **Gäste des Verantwortlichen (Reservierende):**

- Basis- und Kontaktdaten: Name, E-Mail-Adresse, Telefonnummer;
- Reservierungsdaten: Datum, Uhrzeit, Anzahl der Personen, ggf. Tischzuordnung, Reservierungsstatus (z. B. angefragt, bestätigt, abgelehnt, abgelaufen, storniert, no-show); bei Reservierungsanfragen zusätzlich Bearbeiterkennung und eine optionale Nachricht des Restaurants zur Entscheidung;
- Optionale Notizen dienen erforderlichen organisatorischen Angaben wie Sitzwünschen oder Anlass. Gesundheitsdaten, insbesondere Allergien, und andere besondere Datenkategorien werden nicht gezielt abgefragt. Werden solche Angaben dennoch übermittelt, prüft das Restaurant unverzüglich ihre Zulässigkeit. Soweit die erforderliche Grundlage nach Art. 6 und Ausnahme nach Art. 9 DSGVO fehlen, veranlasst es unverzüglich die Löschung oder Einschränkung über support@reservly.at nach Ziffer 13 Absatz 9; eine zugängliche Originalnotiz wird zusätzlich bereinigt. Deren Änderung allein löscht die eigenständige Chatkopie nicht.
- Feedbackdaten (sofern Funktion aktiviert): Bewertung (z. B. 1–5 Sterne), Freitext-Feedback, Zeitpunkt der Abgabe, technische Metadaten (z. B. Link-/Token-ID), Zuordnung zur Reservierung.
- technische Daten: Zeitstempel, pseudonymisierte IP-Information (IP-Hash) und ähnliche Protokolldaten, soweit für Sicherheits- und Rate-Limiting-Zwecke erforderlich.

  Verarbeitet werden erforderliche Absender- und Empfängeradressen, Anzeigenamen, Betreff und Inhalt einschließlich HTML-Darstellung, Zeitpunkte, Nachrichten- und Anbieterkennungen, Zustell- und Fehlerstatus sowie notwendige Daten zu Abmeldungen, Beschwerden und Empfängersperren. Geschützte Vergleichswerte von E-Mail-Adressen für Sperrlisten bleiben pseudonyme personenbezogene Daten.

Gästebuchdaten: zusätzlich Firma, Sprachen, Tags, manuelle Gruppen und Filterregeln, Notiztitel und -text, Erinnerungsdatum, Dateiinhalte und -metadaten, Ersteller- und Bearbeitungskennungen sowie dokumentierte manuelle Änderungen des Marketingstatus. Betroffen sind auch vom Restaurant selbst erfasste Kontaktpersonen ohne Reservierung oder Rewards-Mitgliedschaft.

CSV-Import und -Export: Berechtigte Restaurantnutzer können eigene Gästekontakte importieren und Gästebuchdaten exportieren. Importiert werden Name, E-Mail, optional Telefonnummer und Geburtsdatum sowie ein angegebener Marketingstatus; der Abgleich erfolgt anhand der E-Mail-Adresse innerhalb desselben Restaurants. Ein Export kann zusätzlich Firma, Sprachen, Tags, Gruppen, Mitgliedschaftsstatus, Reservierungs- und Besuchszähler, Kontaktzeitpunkte und Einwilligungsstatus enthalten. Notizinhalte, Notizdateien, einzelne Reservierungsdetails und individuelle Punktebuchungen sind nicht Bestandteil dieses CSV-Exports. Der Export kann auch Kontakte ohne Marketingeinwilligung enthalten und ist deshalb keine Versandfreigabe.

2. **Nutzer des Backoffice (Mitarbeitende / Beauftragte des Verantwortlichen):**
   - Teamdaten umfassen Vor- und Nachname, E-Mail-Adresse, optionale Telefonnummer und Funktion, Restaurant- und Standortzuordnung, Rolle und einzelne Berechtigungen, Einladungs-, Annahme- und Statuszeitpunkte sowie erforderliche Authentifizierungs- und Bearbeiterkennungen. Persönliche vierstellige Teamcodes werden in geschützter Prüfform verarbeitet; sie sind von einer gegebenenfalls weiter genutzten gemeinsamen vierstelligen Loyalty-Admin-PIN zu unterscheiden.
   - Authentifizierungsdaten: Login-Informationen (z. B. Supabase Auth)
   - Protokolldaten: durchgeführte Aktionen im System (z. B. Anlegen, Ändern, Stornieren von Reservierungen). Dazu gehören erforderliche Zuordnungen beim Lesen, Senden und Bearbeiten reservierungsbezogener Nachrichten sowie Änderungen von Reservierungsdaten; nicht jede Anzeige wird personenbezogen protokolliert.

3. **Besucher der öffentlichen Restaurant-Unterseiten:** technische Zugriffsdaten (z. B. IP-Adresse, Zeitstempel, User-Agent, Request-IDs/Logdaten), soweit zur Bereitstellung, Sicherheit und Fehleranalyse erforderlich.

Das manuelle Setzen eines Marketingstatus dokumentiert lediglich die Erklärung durch das Restaurant; es ersetzt keine tatsächlich erteilte, nachweisbare Einwilligung der betroffenen Person. Das Restaurant hält Herkunft, Zeitpunkt, Inhalt und Umfang der Erklärung nachweisbar fest und erfüllt bei nicht unmittelbar erhobenen Angaben die Informationspflichten nach Art. 14 DSGVO. Für besondere Datenkategorien, insbesondere Gesundheitsdaten, ist das allgemeine Gästebuch nicht vorgesehen; diese dürfen nicht in Notizen, Dateien, Tags oder Filterregeln aufgenommen werden, solange keine gesondert geprüfte zulässige Verarbeitung eingerichtet ist. Für importierte Angaben prüft das Restaurant Quelle, Richtigkeit, Rechtsgrundlage und Informationspflichten nach Art. 14 DSGVO. Ein „Ja“ in einer Datei oder eine Bestätigung durch Mitarbeitende ersetzt keine Erklärung des Gastes und keinen Nachweis ihres Textes, Datums, Restaurants, Kanals und Umfangs. Ein früherer Widerruf oder Widerspruch darf durch eine alte Importdatei nicht aufgehoben werden; dazu bedarf es einer nachfolgenden wirksamen neuen Erklärung. Exportdateien dürfen nur zweckgebunden, zugriffsgeschützt und so lange wie erforderlich gespeichert und weitergegeben werden. Das Restaurant bezieht diese Kopien in Auskunft, Berichtigung, Widerrufsabgleich und Löschung ein.

5.2 Kategorien betroffener Personen

- Gäste / Kund:innen des Verantwortlichen,
- Mitarbeiter:innen und sonstige vom Verantwortlichen benannte Nutzer des Reservierungssystems.
- Besucher der vom Auftragsverarbeiter im Auftrag bereitgestellten öffentlichen Restaurant-Unterseiten (Websitebesucher).

Der Verantwortliche stellt sicher, dass keine besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO in das System eingegeben werden, sofern hierfür keine geeignete Rechtsgrundlage besteht.

6. Pflichten des Verantwortlichen

(1) Der Verantwortliche ist im Verhältnis der Parteien allein dafür verantwortlich, dass:

- die Verarbeitung der personenbezogenen Daten (einschließlich der Übermittlung an den Auftragsverarbeiter) auf einer geeigneten Rechtsgrundlage nach Art. 6 und ggf. Art. 9 DSGVO basiert;
- er seine Informationspflichten gegenüber den betroffenen Personen nach Art. 13 und 14 DSGVO erfüllt (insbesondere durch geeignete Datenschutzhinweise zum Online-Reservierungssystem);
- er die Rechte der betroffenen Personen (Kapitel III DSGVO) gegenüber den betroffenen Personen wahrnimmt;
- er ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO führt, in das die Nutzung des Reservierungssystems als Verarbeitungstätigkeit aufgenommen wird.

(2) Der Verantwortliche erteilt dem Auftragsverarbeiter alle Weisungen in Bezug auf Art, Umfang und Zwecke der Verarbeitung (siehe Ziffer 7).

(3) Der Verantwortliche teilt dem Auftragsverarbeiter unverzüglich mit, wenn er Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen in den Auftragsergebnissen feststellt.

7. Weisungsgebundenheit

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer darüberhinausgehenden Verarbeitung verpflichtet ist (Art. 28 Abs. 3 lit. a DSGVO). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen werden zunächst durch diesen Vertrag und den Hauptvertrag festgelegt und können vom Verantwortlichen danach in Textform (z. B. per E-Mail oder über das Kundenkonto) geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und ist berechtigt, die Umsetzung der Weisung bis zur Bestätigung oder Anpassung der Weisung auszusetzen.

8. Vertraulichkeit (personenbezogene Daten)

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

(2) Personenbezogene Auftragsdaten dürfen nicht für eigene Zwecke, insbesondere eigene Werbung von Reservly gegenüber Gästen, verwendet werden. Eine Verarbeitung außerhalb des Auftrags benötigt eine eigenständige Rechtsgrundlage, transparente Information und die Einhaltung des Telekommunikationsrechts; eine Vereinbarung mit dem Restaurant allein genügt dafür nicht.

9. Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter ergreift alle erforderlichen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen sind in **Anlage 2 (TOMs)** beschrieben und umfassen u. a.:

- Nutzung sicherer Hosting- und Datenbank-Infrastruktur (z. B. Vercel für Next.js-Deployment, Supabase/PostgreSQL mit Standort in der EU, Netlify für öffentliche Restaurant-Unterseiten);
- mandantenfähige Architektur mit strikter Mandantentrennung durch serverseitige Autorisierungsprüfungen (z. B. tenant-ID-Filter in allen relevanten Abfragen);
- Authentifizierung für Restaurant-Nutzer mittels individueller Benutzerkonten (z. B. über Supabase Auth) und Zugriffsbeschränkung auf den jeweiligen Restaurant-Mandanten;
- Schutz der Übertragung durch TLS/HTTPS;
- Schutz der Integrität durch
- serverseitige Validierung von Eingaben und wohldefinierte Statuslogik für Reservierungen;
- Rate Limiting und Missbrauchsschutz mittels pseudonymisiertem IP-Hash (Speicherfrist max. 1 Stunde) in einem In-Memory-Store (z. B. Upstash Redis);
- regelmäßige Backups der Datenbank mit angemessener Aufbewahrungsdauer und turnusmäßiger Überschreibung älterer Backups;
- Monitoring, Logging und Incident-Response-Prozesse.

(2) Die zum Zeitpunkt des Vertragsschlusses bestehenden Maßnahmen sind in Anlage 2 dokumentiert. Sie können unter Berücksichtigung des technischen Fortschritts angepasst werden,

sofern das Schutzniveau nicht abgesenkt wird. Wesentliche Änderungen werden dokumentiert und dem Verantwortlichen auf Anfrage mitgeteilt.

10. Unterstützung bei Betroffenenrechten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen, unter Berücksichtigung von Art und Umfang der Verarbeitung, nach Möglichkeit bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III DSGVO (Art. 12–23), insbesondere:

- Auskunft (Art. 15),
- Berichtigung (Art. 16),
- Löschung (Art. 17),
- Einschränkung (Art. 18),
- Datenübertragbarkeit (Art. 20),
- Widerspruch (Art. 21).

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, verweist dieser sie – soweit möglich – an den Verantwortlichen und leitet die Anfrage unverzüglich an den Verantwortlichen weiter.

(3) Reservly unterstützt die Erfüllung von Betroffenenrechten mit den verfügbaren Such-, Berichtigungs-, Sperr- und Löschmöglichkeiten sowie erforderlichen manuellen Auskünften und Exporten. Das Fehlen einer Export-Schaltfläche beschränkt diese Pflicht nicht. Zusatzleistungen über die gesetzlich und vertraglich geschuldete Unterstützung hinaus können nach vorheriger transparenter Vereinbarung vergütet werden; notwendige Unterstützung darf nicht durch unverhältnismäßige Kosten verhindert werden.

Die Unterstützung umfasst noch rechtmäßig vorhandene Nachrichten, automatische HTML-Kopien, frühere Kontaktangaben im Verlauf, Bearbeiterdaten, technische E-Mail-Bestände und einschlägige Daten bei Unterauftragsverarbeitern. Eine Berichtigung des aktuellen Gastfelds ersetzt nicht die Prüfung früherer Kopien. Erforderliche historische Nachweise werden gekennzeichnet, eingeschränkt oder zusammen mit einer Berichtigung aufbewahrt. Eine rechtmäßig geschuldete Löschung oder Einschränkung wird nicht allein bis zum regulären Löschlauf aufgeschoben.

11. Unterstützung bei Sicherheit, DPIA und Meldungen

Der Auftragsverarbeiter unterstützt den Verantwortlichen, soweit möglich und unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO), insbesondere:

- bei der Sicherstellung angemessener technischer und organisatorischer Maßnahmen (Art. 32);
- bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden (Art. 33) und an betroffene Personen (Art. 34) im jeweils erforderlichen Umfang;
- bei der Durchführung von Datenschutz-Folgenabschätzungen (Art. 35) und ggf. Konsultationen der Aufsichtsbehörde (Art. 36), sofern die im Rahmen der Verarbeitung durch den Auftragsverarbeiter bereitgestellten Informationen hierfür benötigt werden.

12. Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich und ohne schuldhaftes Zögern über ihm bekannt gewordene Verletzungen des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betreffen (Art. 33 Abs. 2 DSGVO).

(2) Die Mitteilung enthält, soweit möglich, die in Art. 33 Abs. 3 DSGVO genannten Informationen, insbesondere:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten;
- Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Der Auftragsverarbeiter trifft unverzüglich geeignete Maßnahmen zur Sicherung der Daten und zur Minderung möglicher Nachteile für betroffene Personen und stimmt sich hierzu mit dem Verantwortlichen ab.

13. Löschung, Anonymisierung und Backups

(1) Personenbezogene Felder einzelner Reservierungen einschließlich Name, E-Mail, Telefon und Notizen werden nach Ablauf der vom Restaurant gewählten Reservierungsfrist nach dem Reservierungsdatum gelöscht oder wirksam anonymisiert. Standard sind 30 Tage. Als dokumentierte Weisung kann der Inhaber in den Einstellungen für Reservierungen 7, 14, 30, 60, 90 oder 180 Tage oder 1, 3 oder 7 Jahre und für Direktchats 7, 14, 30, 60, 90 oder 180 Tage oder 1 Jahr wählen. Jede Abweichung vom Standard begründet das Restaurant in eigenen Worten; Erforderlichkeit und Rechtsgrundlage der gewählten Frist verantwortet das Restaurant. Eine Reservierungsfrist über einem Jahr setzt voraus, dass das Restaurant eine gesetzliche Aufbewahrungspflicht bestätigt; dann bleiben bis zum Fristende nur Name, E-Mail-Adresse, Termin, Personenanzahl und Status erhalten, während Telefonnummer, Notizen, Stornotexte und der Reservierungschat weiterhin nach 30 Tagen gelöscht werden. Eine geänderte Frist gilt ab dem nächsten Löschlauf für alle bestehenden Daten; vor einer Verkürzung bestätigt das Restaurant den Umfang der dadurch zusätzlich gelöschten Daten. Bei einer Verlängerung werden bereits gelöschte Daten nicht wiederhergestellt. Eine vom Standard abweichende Frist wird samt Begründung in den Datenschutzhinweisen für Gäste beim jeweiligen Restaurant angezeigt. Für restaurantbezogene Gastprofile ohne aktive oder gesperrte Mitgliedschaft ist eine Bereinigung nach zwei Jahren ohne relevante Aktivität vorgesehen. Technisch werden hierzu insbesondere letzter Besuch, letzte Aktualisierung und erster Kontakt beziehungsweise Anlagezeitpunkt herangezogen. Eine innerhalb der letzten drei Jahre beendete Mitgliedschaft desselben Restaurants kann eine gesonderte, erforderliche Aufbewahrung für Nachweise begründen; für Mitgliedschaften gelten die gesonderten Rewards-Fristen. Eine bloße technische Aktualisierung begründet keinen neuen Speicherzweck. Entfällt der zulässige Zweck früher, werden die Daten früher gelöscht oder auf erforderliche, zugriffsbeschränkte Nachweise reduziert. Diese Frist löscht weder automatisch das zentrale Konto noch Profile anderer Restaurants. Die Entfernung einzelner Reservierungsfelder allein gewährleistet keine Anonymität, wenn Personen über Gastprofile oder Verknüpfungen bestimmbar bleiben. Einzelne Reservierungs-Besuchsereignisse mit Reservierungskennung, Zeitpunkt und Personenanzahl werden mit Ablauf der Reservierungsfrist des Restaurants (Standard 30 Tage) nach dem Termin gelöscht. Rechtmäßig weiter benötigte Reservierungszähler und der letzte Aktivitätszeitpunkt können im Gastprofil verbleiben und bleiben personenbezogen; Loyalty-Besuchsereignisse unterliegen ihren eigenen Fristen. Notizen, Erinnerungen, Gruppenzuordnungen und Dateianhänge dürfen nur für ihren jeweiligen Zweck gespeichert werden. Bei Zweckfortfall oder Profillöschung sind auch gespeicherte Dateiobjekte und Verknüpfungen zu entfernen; eine bloße Löschung des Datenbankverweises genügt nicht. Auch Freitext-Stornogründe sind von der Anonymisierung einzelner Reservierungen erfasst.

(2) Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses Vertrags und auf Weisung des Verantwortlichen löscht der Auftragsverarbeiter alle personenbezogenen Daten oder gibt sie dem Verantwortlichen zurück und löscht vorhandene Kopien, sofern nicht eine gesetzliche Aufbewahrungspflicht besteht (Art. 28 Abs. 3 lit. g DSGVO).

(3) Sicherungskopien sind gegen reguläre Nutzung und unberechtigten Zugriff zu schützen. Gelöschte Auftragsdaten dürfen darin nur bis zur erforderlichen planmäßigen Rotation verbleiben und ausschließlich zur Wiederherstellung verwendet werden. Reservly dokumentiert je eingesetztem System den konkreten Sicherungszyklus und die maximale Aufbewahrungsdauer und stellt diese Angaben dem Restaurant vor Beginn der Verarbeitung sowie bei wesentlichen Änderungen bereit. Nach einer Wiederherstellung sind zwischenzeitliche Löschungen und Einschränkungen erneut anzuwenden, bevor Daten wieder produktiv genutzt werden. Gesetzlich gebotene Löschungen dürfen nicht durch eine unbegrenzte Backup-Aufbewahrung umgangen werden.

(4) Für Feedback werden spätestens 30 Tage nach dem Reservierungstermin sowohl die Reservierungszuordnung als auch identifizierende Angaben im Freitext und in verbleibenden Verknüpfungen entfernt. Nur tatsächlich anonyme Bewertungen dürfen für die Qualitätsauswertung fortbestehen. Die bloße Entfernung einer Reservierungs-ID genügt nicht. Erforderliche, konkret begründete Nachweise zu offenen Beschwerden werden davon getrennt und zugriffsbeschränkt nur bis zur Erledigung und einer notwendigen Nachweisfrist aufbewahrt.

(5) Ein Reservierungschat wird einschließlich automatischer Inhaltskopien, Bearbeiterangaben und zugehöriger Reservierungsänderungen zum späteren von zwei Zeitpunkten gelöscht: mit Ablauf der Reservierungsfrist des Restaurants nach dem Reservierungstermin (Absatz 1; Standard 30 Tage, für den Chat höchstens ein Jahr, bei einer längeren Reservierungsfrist 30 Tage) oder sieben Tage nach der letzten persönlichen Nachricht von Gast oder Restaurant. Automatische E-Mails, Systemereignisse sowie Gelesen- und Sternmarkierungen verlängern die Frist nicht; bei einer tatsächlichen Terminverschiebung ist der geänderte Termin maßgeblich. Nach Fristablauf werden keine Antworten mehr angenommen. Läuft ein Chat länger als die übrigen Reservierungsdaten, bleiben Name und E-Mail-Adresse des Gasts bis zur Löschung des Chats als dessen Kontakt erhalten. Bei frühzeitiger Buchung können Nachrichten länger als 30 Tage ab Versand gespeichert bleiben. Ein Direktchat wird gelöscht, wenn während der vom Restaurant gewählten Frist für Direktchats (Standard 30 Tage) keine persönliche Nachricht von Gast oder Restaurant eingegangen ist; jede persönliche Nachricht verlängert die Frist für den gesamten Verlauf, ein leerer Direktchat läuft ab seiner Erstellung. Mit dem Direktchat werden seine Nachrichten, die Kontaktkopie und die Antwortadresse gelöscht; das Gästeprofil bleibt bestehen. Frühere berechtigte Löschanfragen bleiben möglich. Erforderliche Nachweise zu einem konkreten offenen Anspruch werden nur gesondert, zugriffsbeschränkt und für dessen erforderliche Dauer aufbewahrt.

(6) Versandprotokolle in Reservlys zentraler E-Mail-Verarbeitung werden einschließlich der Schlüssel gegen doppelten Versand 30 Tage nach dem Versand vollständig gelöscht; zugehörige Ereignisse des E-Mail-Dienstleisters werden ebenfalls gelöscht. Nur vorübergehend benötigte Versandinhalte werden bereits nach erfolgreicher Übergabe entfernt, soweit sie nicht für zulässige Fehlerbehebung oder Wiederholung erforderlich sind. Inhaltliche Kopien im Nachrichtencenter und erforderliche Kampagnen- oder Einwilligungsnachweise folgen ihren gesonderten Fristen. Nach einer Abmeldung, einer Spam-Beschwerde oder einer dauerhaft gescheiterten Zustellung wird ein Sperrvermerk mit einem geschützten Vergleichswert der E-Mail-Adresse und dem Anlass gespeichert. Er dient nur dazu, keine weiteren unerwünschten oder unzulässigen E-Mails an diese Adresse zu senden, und wird gelöscht, sobald er dafür nicht mehr erforderlich ist.

(7) Die Aufbewahrung beim E-Mail-Dienstleister ist von der Speicherung bei Reservly getrennt. Für den eingesetzten Tarif Resend Pro nennt der Anbieter 30 Tage laufende Datenaufbewahrung; Sicherungskopien beim Anbieter folgen dessen eigenem Sicherungszyklus. Dies ist keine einheitliche Frist für alle bei Reservly geführten Datenbestände. Nach Ende des Resend-Vertrags sieht das DPA die Löschung verbleibender Daten innerhalb von 90 Tagen vor. Diese Abwicklungsfrist verlängert weder die laufenden Fristen bei Reservly noch rechtmäßig geschuldete frühere Einzelfalllöschungen. Auskunft zu den betroffenen Datenarten und Unterstützung bei einer früher erforderlichen Löschung sind über support@reservly.at erhältlich.

(8) Einladungslinks gelten sieben Tage. Nicht angenommene Einladungsprofile werden spätestens 30 Tage nach Ablauf oder Widerruf der Einladung gelöscht, sofern nicht ein konkret dokumentierter Nachweisfall eine eingeschränkte Aufbewahrung erfordert. Bei Entfernung eines Teammitglieds wird

dessen Zugang entzogen; dies ist noch keine vollständige Löschung aller personenbezogenen Daten. Nicht mehr erforderliche Kontakt- und Zusatzangaben des restaurantbezogenen Profils werden spätestens innerhalb von 30 Tagen entfernt. Eine minimale Bearbeiterzuordnung bleibt nur so lange erhalten, wie sie für den jeweiligen rechtmäßig aufbewahrten Vorgang erforderlich ist; sie unterliegt dessen Frist und darf keine dauerhafte Personalakte bilden. Andere berechtigte Restaurantzugänge eines zentralen Kontos bleiben davon getrennt.

(9) Supportgestützte Löschung und Einschränkung einzelner sensibler Nachrichten

Für einzelne Nachrichten besteht im Restaurant-Dashboard derzeit keine Löschfunktion. Das Restaurant veranlasst die erforderliche Löschung oder Einschränkung über support@reservly.at. Bei unerwarteten Gesundheitsdaten oder anderen unzulässigen sensiblen Inhalten erfolgt die Meldung unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis. Sie bezeichnet Restaurant, Reservierungskennung und betroffene Nachricht beziehungsweise Zeitpunkt; sensible Inhalte und Anhänge dürfen nicht nochmals ungeschützt mitgesendet werden. Das Restaurant beendet unzulässige weitere Nutzung und beschränkt die Weitergabe unverzüglich. Eine zugängliche Originalnotiz wird zusätzlich bereinigt; dies ersetzt die Löschung ihrer Chatkopie nicht.

Reservly bestätigt und prüft eine solche Meldung unverzüglich, spätestens innerhalb von 24 Stunden nach Eingang. Erforderliche vorläufige Zugriffsbeschränkungen in den eigenen Systemen werden innerhalb dieser Frist veranlasst und umgesetzt. Fehlende Angaben oder Zweifel an der Weisungsberechtigung werden ebenfalls innerhalb dieser Frist konkret zurückgemeldet; bereits mögliche Schutzmaßnahmen bleiben geschuldet. Eine hinreichend zuordenbare und berechtigte Löschweisung setzt Reservly in seinen aktiven Systemen unverzüglich, spätestens innerhalb von 72 Stunden nach Eingang, um und bestätigt das Ergebnis. Bei der Fristberechnung zählen auch Wochenenden und Feiertage; die Höchstfristen erlauben bei höherer Dringlichkeit keinen Aufschub.

Die Prüfung erfasst die ursprüngliche Reservierungsnotiz, ihre eigenständig gespeicherte erste Chatnachricht, weitere Nachrichten und Antwortzitate, vollständige automatische E-Mail-Kopien einschließlich HTML, gegebenenfalls vorhandene frühere Werte im Änderungsverlauf sowie einschlägige technische E-Mail- und Supportkopien. Es wird nicht nur der sichtbare aktuelle Notiztext entfernt. Gesetzlich erforderliche oder anderweitig rechtmäßig aufzubewahrende Nachweise bleiben ausschließlich im notwendigen Umfang getrennt und zugriffsbeschränkt erhalten; Reservly teilt Grund, Umfang und weitere Frist mit. Sicherungskopien werden nach dem dokumentierten Sicherungszyklus bereinigt und dürfen gelöschte Inhalte bei einer Wiederherstellung nicht erneut in den normalen Betrieb bringen.

Soweit die erforderliche Löschung Daten bei Resend oder anderen Unterauftragsverarbeitern betrifft, veranlasst Reservly sie unverzüglich, spätestens innerhalb von 24 Stunden nach Eingang der zuordenbaren und berechtigten Weisung, und verfolgt den Abschluss nach. Die 72-Stunden-Frist für Reservlys aktive Systeme ist keine Zusage einer entsprechenden Resend-Frist. Spätestens innerhalb dieser 72 Stunden informiert Reservly das Restaurant über noch ausstehende Providermaßnahmen, bereits ergriffene Schutzmaßnahmen und den nächsten Bearbeitungsschritt; offene Fälle werden bis zum bestätigten Abschluss weiterverfolgt. Eine gebotene frühere Löschung darf nicht allein auf die reguläre 30-Tage-Frist verwiesen werden.

14. Unterauftragsverarbeiter

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter („Unterauftragsverarbeiter“) im Sinne des Art. 28 Abs. 2 und 4 DSGVO hinzuziehen. Eine aktuelle Liste der Unterauftragsverarbeiter mit Angaben zu Leistung, Standort und Verarbeitungsumfang ist in **Anlage 3** enthalten.

(2) Der Auftragsverarbeiter erhält vom Verantwortlichen eine **allgemeine Genehmigung** zum Einsatz der in Anlage 3 aufgeführten Unterauftragsverarbeiter und zur Hinzufügung oder Ersetzung von Unterauftragsverarbeitern, sofern:

- Reservly informiert das Restaurant aktiv in Textform mindestens 14 Tage vor dem vorgesehenen Einsatz eines hinzugefügten oder ersetzenden Unterauftragsverarbeiters; die

Mitteilung nennt Anbieter, Aufgabe, Datenkategorien, Verarbeitungsorte, Transfergarantien, vorgesehenen Beginn und Widerspruchsweg. Die aktuelle Liste wird dauerhaft zugänglich gehalten. Eine stille Änderung der Liste ersetzt die Mitteilung nicht. Das Restaurant kann innerhalb von 14 Tagen nach Zugang aus wichtigem datenschutzrechtlichem Grund widersprechen. Dies gilt auch für einschlägige Änderungen in nachgelagerten Lieferantenketten. Erhält Reservly selbst eine kurzfristige Anbieterinformation, informiert Reservly unverzüglich; der zugesagte Vorlauf wird dadurch nicht verkürzt. Ist dieser nicht einzuhalten, beginnt die betroffene geänderte Verarbeitung erst nach rechtzeitiger wirksamer Autorisierung oder bleibt bis dahin ausgesetzt. Eine vorherige gesonderte ausdrückliche Genehmigung der konkret bezeichneten Änderung bleibt möglich.

- Kann ein berechtigter Widerspruch nicht durch eine zumutbare Alternative geklärt werden, wird die betroffene Verarbeitung nicht mit dem widersprochenen neuen Anbieter aufgenommen beziehungsweise zum Änderungszeitpunkt ausgesetzt. Das Restaurant kann die konkret betroffene Funktion zum Änderungszeitpunkt außerordentlich beenden. Zwingende Rechte und die datenschutzrechtliche Rückgabe-/Löschpflicht bleiben unberührt.

(3) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich mindestens zu denselben datenschutzrechtlichen Pflichten, zu denen der Auftragsverarbeiter gegenüber dem Verantwortlichen verpflichtet ist (Art. 28 Abs. 4 DSGVO). Der Auftragsverarbeiter bleibt für die Handlungen des Unterauftragsverarbeiters gegenüber dem Verantwortlichen verantwortlich.

15. Internationale Datenübermittlungen

(1) Für Kernsysteme werden soweit möglich europäische Regionen verwendet. Der beauftragte E-Mail-Versand und -Empfang über Resend umfasst hingegen reguläre Verarbeitung und Speicherung in den USA; dies ist nicht nur ein möglicher gelegentlicher Supportzugriff.

(2) Soweit Daten in einem Drittland verarbeitet werden oder von dort zugegriffen wird, stellt der Auftragsverarbeiter sicher, dass die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. durch einen Angemessenheitsbeschluss nach Art. 45 DSGVO oder geeignete Garantien nach Art. 46 DSGVO, insbesondere Standarddatenschutzklauseln) und führt eine entsprechende Bewertung des Datenschutzniveaus („Transfer Impact Assessment“) durch.

(3) Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen Informationen über die eingesetzten Übermittlungsmechanismen (z. B. Standarddatenschutzklauseln) zur Verfügung.

Resend wird von Plus Five Five, Inc., USA, betrieben. E-Mail-Daten werden auch in den USA verarbeitet und gespeichert; eine europäische Versandregion begründet keine ausschließliche EU-Speicherung. Für die Auftragsverarbeitung werden die einschlägigen EU-Standardvertragsklauseln nach Beschluss (EU) 2021/914 und erforderliche ergänzende Maßnahmen zugrunde gelegt. Bei Reservly als Auftragsverarbeiter des Restaurants gilt Modul 3, bei Reservly als Verantwortlichem und Resend als Auftragsverarbeiter Modul 2. Für die im Resend-DPA gesondert geregelte eigene Verantwortlichkeit für Account- und Nutzungsdaten gilt bei entsprechender Übermittlung Modul 1. Informationen und eine Kopie der einschlägigen Garantien sind über support@reservly.at erhältlich; schutzbedürftige Angaben können geschwärzt werden.

Für die beauftragte E-Mail-Verarbeitung handelt Resend als Auftragsverarbeiter beziehungsweise Unterauftragsverarbeiter. Davon abgegrenzt verarbeitet Resend bestimmte Daten zur Verwaltung seines Kundenkontos und zur Sicherheit und Nutzung seines Dienstes in eigener Verantwortlichkeit. Nutzungsdaten können technische Protokolle und Angaben zu Quelle und Ziel einer Kommunikation umfassen. Restaurant-Teammitglieder erhalten durch ihren Reservly-Zugang nicht automatisch ein eigenes Resend-Konto. Informationen zur eigenen Verarbeitung durch Resend stehen unter https://resend.com/legal/privacy-policy. Diese Abgrenzung erlaubt keine zusätzliche Restaurantwerbung oder freie Nutzung von Nachrichteninhalten. Resend setzt weitere Anbieter für Infrastruktur, Sicherheit und Zustellung ein; die aktuelle nachgelagerte Liste steht unter https://resend.com/legal/subprocessors. Deren Einsatz unterliegt den einschlägigen vertraglichen Schutz- und Änderungsregeln.

16. Kontrollen und Audits

(1) Der Verantwortliche ist berechtigt, die Einhaltung dieses Vertrags und der datenschutzrechtlichen Vorgaben im erforderlichen und angemessenen Umfang zu kontrollieren.

(2) Der Auftragsverarbeiter kann zum Nachweis geeignete Dokumente (z. B. technische und organisatorische Maßnahmen, Zertifizierungen, Auditberichte unabhängiger Stellen) zur Verfügung stellen. Die Parteien sind sich einig, dass solche „remote-Nachweise“ vorrangig zu nutzen sind, bevor weitergehende Vor-Ort-Inspektionen erfolgen.

(3) Soweit darüber hinaus eine Inspektion beim Auftragsverarbeiter erforderlich ist, findet diese:

- höchstens einmal pro Kalenderjahr,
- mit einer Ankündigungsfrist von mindestens 14 Tagen,
- während der üblichen Geschäftszeiten und
- unter Wahrung der Vertraulichkeit anderer Kunden und der Sicherheit der Systeme

statt. Die Parteien können im Einzelfall eine abweichende Regelung treffen (z. B. bei konkretem Verdacht auf schwerwiegende Verstöße).

(4) Führt eine Prüfung nicht zu einem erheblichen Verstoß des Auftragsverarbeiters gegen datenschutzrechtliche Pflichten, trägt der Verantwortliche die angemessenen, nachzuweisenden Aufwände des Auftragsverarbeiters für die Unterstützung der Prüfung.

16a. Anlassbezogene Kontrollen

Die Beschränkung regulärer Inspektionen auf einmal jährlich und die Ankündigungsfrist gelten nicht bei konkreten Anhaltspunkten für Datenschutzverstöße, einem Sicherheitsvorfall, einer behördlichen Anforderung oder sonstigem begründetem zusätzlichem Prüfbedarf. In dringenden Fällen ist eine kurzfristige Prüfung zu ermöglichen. Nachweise ersetzen eine erforderliche Inspektion nicht. Kostenregelungen dürfen die gesetzlich geschuldete Kontrolle und Unterstützung nicht verhindern oder unverhältnismäßig erschweren; durch einen Verstoß von Reservly verursachte zusätzliche Prüfkosten trägt Reservly.

17. Dokumentation und Accountability

(1) Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.

(2) Der Auftragsverarbeiter dokumentiert den Abschluss dieses Auftragsverarbeitungsvertrags im Rahmen des elektronischen Onboardings, insbesondere durch Protokollierung der jeweils akzeptierten Version, des Zeitpunkts der Zustimmung und der Zuordnung zur Restaurant-/Tenant-ID sowie zur Nutzer-ID des bestätigenden Accounts. Der Nachweis bezeichnet zusätzlich den Pfad der unveränderlich archivierten Dokumentfassung sowie den Annahmekanal. Historische Annahmen werden nicht rückwirkend auf diese neue Fassung umgestellt.

(3) Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesem Vertrag niedergelegten Pflichten nachzuweisen (Art. 28 Abs. 3 lit. h DSGVO).

18. Laufzeit, Rangfolge und Kündigung

(1) Dieser Vertrag tritt mit Abschluss des Hauptvertrags in Kraft und gilt für dessen Dauer.

(2) Eine isolierte Kündigung dieses Vertrags ohne Kündigung des Hauptvertrags ist grundsätzlich ausgeschlossen. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt, insbesondere bei schwerwiegenden oder wiederholten Verstößen gegen datenschutzrechtliche Pflichten.

(3) Im Falle von Widersprüchen zwischen Regelungen dieses Vertrags und Regelungen des Hauptvertrags gehen die Bestimmungen dieses Vertrags zur Auftragsverarbeitung den Regelungen des Hauptvertrags vor, soweit sie die Verarbeitung personenbezogener Daten betreffen.

19. Geheimhaltung (Betriebs- und Geschäftsgeheimnisse)

(1) Die Parteien behandeln alle ihnen im Zusammenhang mit diesem Vertrag bekannt werdenden Geschäfts- und Betriebsgeheimnisse der jeweils anderen Partei vertraulich. Dieses Geheimhaltungsgebot gilt über die Laufzeit des Vertrags hinaus.

(2) Die Vertraulichkeitsverpflichtung gilt nicht für Informationen, die:

- bereits allgemein bekannt waren oder ohne Verstoß gegen diesen Vertrag allgemein bekannt werden oder
- von der empfangenden Partei unabhängig und ohne Rückgriff auf vertrauliche Informationen entwickelt wurden.

(3) Die Parteien verpflichten ihre Mitarbeitenden und ggf. beauftragte Dritte entsprechend.

20. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schrift- oder Textform. Dies gilt auch für einen Verzicht auf dieses Formerfordernis. Die elektronische Form (einschließlich Bestätigung durch Checkbox im Onboarding unter Protokollierung von Version und Zeitstempel) genügt dem Schriftformerfordernis im Sinne von Art. 28 Abs. 9 DSGVO.

(2) Sollte eine Bestimmung dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung treten die gesetzlichen Vorschriften.

(3) Es gilt das Recht der Republik Österreich unter Ausschluss des UN-Kaufrechts. Gerichtsstand ist – soweit gesetzlich zulässig – der Sitz des Auftragsverarbeiters.

Anlage 1 – Beschreibung der Verarbeitung

1. System / Komponenten

Reservly ist ein webbasiertes Online-Reservierungssystem (SaaS) für Restaurants mit folgenden Komponenten:

- **Reservierungs-Widget** (Next.js/React), Einbindung per **iFrame** auf Websites/Online-Auftritten des Verantwortlichen oder auf öffentlichen Restaurant-Unterseiten (z. B. reservly.at/restaurant/…).
- **Backend/API** (Next.js/Node.js) zur Verarbeitung der Reservierungslogik.
- **Datenbank & Auth:** Supabase/PostgreSQL (EU-Region), **Supabase Auth** für Dashboard-Logins.
- **Dashboard/Backoffice** (Next.js, Multi-Tenant) zur Verwaltung von Reservierungen und Einstellungen. Das Gästebuch umfasst auch manuelle Kontakte, Notizen und private Dateianhänge sowie manuelle und dynamische Gruppen.
- **Öffentliche Restaurant-Unterseiten** (z. B. reservly.at/restaurant/…), bereitgestellt über ein Hosting und CDN (Netlify), inkl. Einbindung des Reservierungs-Widgets per iFrame.
- Transaktionaler E-Mail-Versand und Empfang reservierungsbezogener Antworten über Resend (Plus Five Five, Inc., USA); Nachrichtencenter mit individuellen Nachrichten, automatischen Kopien und Reservierungsänderungsverlauf sowie Direktchats mit Gästebuchkontakten; tägliche Zusammenfassung ungelesener Nachrichten an das Restaurant.

- **Rate Limiting/Missbrauchsschutz** über **Upstash Redis** (Speicherung eines **IP-Hashes** mit TTL max. 1 Stunde).

2. Art der Verarbeitung (Vorgänge)

Erheben, Erfassen, Speichern, Auslesen, Ändern, Stornieren, Übermitteln (E-Mail), Protokollieren, Einschränken sowie Löschen/Anonymisieren sowie Bewerten und Weiterleiten von Feedback an den Verantwortlichen. Hinzu kommen Empfang und Zuordnung von E-Mail-Antworten sowie die erforderliche Speicherung und Bereinigung von Nachrichtenkopien und Bearbeitungsverläufen.

Bereitstellung/Hosting der öffentlichen Restaurant-Unterseiten inkl. technisch notwendiger Verarbeitung von Zugriffsdaten (Server-/CDN-Logs) zur Auslieferung, Sicherheit und Fehleranalyse.

3. Zwecke der Verarbeitung im Auftrag

- Abwicklung und Verwaltung von **Online-Reservierungen** (inkl. Slot-/Verfügbarkeitsberechnung und Bearbeitung von Reservierungsanfragen).
- Betrieb des **Dashboards** (Planung/Verwaltung; manuelle Reservierungen).
- Versand transaktionaler Kommunikation an Gäste und Benachrichtigungen an das Restaurant. Dazu gehören reservierungsbezogene individuelle Kommunikation, Direktchats mit Gästebuchkontakten und der Empfang von Antworten.
- **Sicherheit/Stabilität** des Systems (Rate Limiting, Logging/Monitoring, Fehleranalyse).
- **Aggregierte/anonymisierte Auswertungen** ohne Personenbezug (System/Business-Optimierung).
- Einholung und Weiterleitung von internem Service-Feedback der Gäste an den Verantwortlichen (Bewertung und optionaler Freitext).

4. Betroffene Personen

- Gäste/Kund:innen des Verantwortlichen (Reservierende sowie Gästebuchkontakte, mit denen das Restaurant Nachrichten austauscht).
- Mitarbeiter:innen/Beauftragte des Verantwortlichen (Dashboard-Nutzer).
- Besucher der öffentlichen Restaurant-Unterseiten (Websitebesucher).

5. Kategorien personenbezogener Daten

Gäste: Name, E-Mail, Telefonnummer; Reservierungsdetails (Datum/Uhrzeit/Personenanzahl/Status, ggf. Tisch); optionale Notizen (Freitext); technische Daten (Zeitstempel, IP-Hash, erforderliche Logs).

Das reservierungsbezogene Nachrichtencenter umfasst individuelle ausgehende Nachrichten, eingehende E-Mail-Antworten und gespeicherte Kopien automatischer Reservierungsnachrichten. Es verarbeitet Nachrichtentext und gegebenenfalls Betreff/HTML-Darstellung, Absender und Empfänger, Zeitpunkte, technische Nachrichten- und Antwortzuordnungen, Zustellstatus, Anzahl eingegangener Anhänge, gemeinsame Gelesen- und Sternmarkierungen sowie erforderliche Bearbeiterkennung und Namen. Der Reservierungsverlauf kann frühere und geänderte Kontakt- und Reservierungsangaben enthalten. Eine gemeinsame Gelesen-Markierung ist keine individuelle Lesebestätigung. Für Direktchats gelten dieselben Datenkategorien; hinzu kommen Name und E-Mail-Adresse des Gasts als Kontaktkopie und die Zuordnung zum Gästeprofil. Bei Reservierungsanfragen kommen Anfragestatus, Bearbeiterkennung und eine optionale Nachricht des Restaurants zur Entscheidung hinzu.

Verarbeitet werden erforderliche Absender- und Empfängeradressen, Anzeigenamen, Betreff und Inhalt einschließlich HTML-Darstellung, Zeitpunkte, Nachrichten- und Anbieterkennungen, Zustell- und Fehlerstatus sowie notwendige Daten zu Abmeldungen, Beschwerden und Empfängersperren. Geschützte Vergleichswerte von E-Mail-Adressen für Sperrlisten bleiben pseudonyme personenbezogene Daten.

Eine freiwillige Notiz aus dem Onlinebuchungsformular wird zusätzlich als erste Gastnachricht im Nachrichtencenter gespeichert. Es handelt sich um eine eigenständige Kopie; eine spätere Änderung oder Löschung der Reservierungsnotiz entfernt diese Chatnachricht nicht automatisch. Automatische Reservierungs-E-Mails werden mit ihrem vollständigen erzeugten Inhalt einschließlich HTML als Kopie gespeichert.

Resend (Plus Five Five, Inc., USA) empfängt und speichert die eingehende E-Mail einschließlich Inhalt und mitgesendeter Anhänge in den USA. Für den eingesetzten Pro-Tarif beträgt die reguläre laufende Aufbewahrung 30 Tage ab Eingang; Sicherungskopien beim Anbieter folgen dessen eigenem Sicherungszyklus. Im Reservly-Nachrichtencenter werden der aufbereitete Antworttext, Absenderadresse, Betreff, Empfangszeit und Anzahl der Anhänge sowie die erforderlichen Zuordnungsdaten gespeichert. Die vollständigen E-Mail-Anhänge werden dort nicht als Chatdateien angezeigt. Die 30-Tage-Frist beim Empfangsdienstleister ist von der Löschfrist des Chatverlaufs nach Ziffer 13 Absatz 5 zu unterscheiden. Berechtigte frühere Löschungen werden über den Support veranlasst.

Dashboard-Nutzer: Teamdaten umfassen Vor- und Nachname, E-Mail-Adresse, optionale Telefonnummer und Funktion, Restaurant- und Standortzuordnung, Rolle und einzelne Berechtigungen, Einladungs-, Annahme- und Statuszeitpunkte sowie erforderliche Authentifizierungs- und Bearbeiterkennungen. Persönliche vierstellige Teamcodes werden in geschützter Prüfform verarbeitet; sie sind von einer gegebenenfalls weiter genutzten gemeinsamen vierstelligen Loyalty-Admin-PIN zu unterscheiden. Erforderliche Aktions- und Bearbeiterdaten nach Ziffer 5 und Anlage 2.

Besucher der öffentlichen Restaurant-Unterseiten: technische Zugriffsdaten (z. B. IP-Adresse, Zeitstempel, User-Agent, Request-IDs/Logdaten), soweit zur Bereitstellung und Sicherheit erforderlich.

Hinweis: Freitext-Feedback kann im Einzelfall besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO enthalten.

Hinweis: Freitextnotizen können im Einzelfall besondere Kategorien i. S. d. Art. 9 DSGVO enthalten; der Verantwortliche instruiert seine Nutzer, solche Daten nur bei geeigneter Rechtsgrundlage einzugeben. Die Bearbeitung unerwarteter sensibler Inhalte und ihrer Kopien erfolgt nach Ziffer 13 Absatz 9 über support@reservly.at.

6. Ort der Verarbeitung / Drittland

Kernsysteme in den vereinbarten EU/EWR-Regionen; E-Mail-Versand und -Empfang über Resend einschließlich Verarbeitung und Speicherung in den USA. Weitere internationale Zugriffe nach Anlage 3 und Ziffer 15. Eine ausschließliche EU-Verarbeitung sämtlicher Auftragsdaten wird nicht zugesagt.

7. Löschung / Anonymisierung / Backups

- Löschung oder wirksame Anonymisierung personenbezogener Reservierungsfelder nach Ablauf der Reservierungsfrist des Restaurants (Standard 30 Tage nach Reservierungsdatum; Einzelheiten in Ziffer 13 Absatz 1). Für rechtmäßig getrennt geführte Gastprofile und erforderliche Historien gelten die besonderen, zweckgebundenen Fristen in Ziffer 13 Absatz 1. Statistiken dürfen nur bei tatsächlich aufgehobenem Personenbezug dauerhaft anonym gespeichert werden.
- Backups: Sicherungskopien sind gegen reguläre Nutzung und unberechtigten Zugriff zu schützen. Gelöschte Auftragsdaten dürfen darin nur bis zur erforderlichen planmäßigen Rotation verbleiben und ausschließlich zur Wiederherstellung verwendet werden. Reservly dokumentiert je eingesetztem System den konkreten Sicherungszyklus und die maximale Aufbewahrungsdauer und stellt diese Angaben dem Restaurant vor Beginn der Verarbeitung sowie bei wesentlichen Änderungen bereit. Nach einer Wiederherstellung sind zwischenzeitliche Löschungen und Einschränkungen erneut anzuwenden, bevor Daten

wieder produktiv genutzt werden. Gesetzlich gebotene Löschungen dürfen nicht durch eine unbegrenzte Backup-Aufbewahrung umgangen werden.

- Nach Vertragsende: Rückgabe/Löschung nach Weisung, soweit keine Aufbewahrungspflichten entgegenstehen.
- Feedbackdaten werden spätestens 30 Tage nach dem Reservierungsdatum von der Reservierung entkoppelt. Freitext und sonstige identifizierende Angaben sind zusätzlich zu löschen oder so zu bearbeiten, dass eine Identifizierung auch aus dem Inhalt und verbleibenden Verknüpfungen nicht mehr möglich ist. Das Entfernen der reservation_id allein ist keine Anonymisierung. In Postfächern des Restaurants weiterverarbeitete Kopien unterliegen dessen eigenem Löschkonzept; Reservly weist bei der Weiterleitung darauf hin.

  Ein Reservierungschat wird einschließlich automatischer Inhaltskopien, Bearbeiterangaben und zugehöriger Reservierungsänderungen zum späteren von zwei Zeitpunkten gelöscht: mit Ablauf der Reservierungsfrist des Restaurants nach dem Reservierungstermin (Ziffer 13 Absatz 1; Standard 30 Tage, für den Chat höchstens ein Jahr, bei einer längeren Reservierungsfrist 30 Tage) oder sieben Tage nach der letzten persönlichen Nachricht von Gast oder Restaurant. Automatische E-Mails, Systemereignisse sowie Gelesen- und Sternmarkierungen verlängern die Frist nicht; bei einer tatsächlichen Terminverschiebung ist der geänderte Termin maßgeblich. Nach Fristablauf werden keine Antworten mehr angenommen. Läuft ein Chat länger als die übrigen Reservierungsdaten, bleiben Name und E-Mail-Adresse des Gasts bis zur Löschung des Chats als dessen Kontakt erhalten. Bei frühzeitiger Buchung können Nachrichten länger als 30 Tage ab Versand gespeichert bleiben. Ein Direktchat wird gelöscht, wenn während der vom Restaurant gewählten Frist für Direktchats (Standard 30 Tage) keine persönliche Nachricht von Gast oder Restaurant eingegangen ist; jede persönliche Nachricht verlängert die Frist für den gesamten Verlauf, ein leerer Direktchat läuft ab seiner Erstellung. Mit dem Direktchat werden seine Nachrichten, die Kontaktkopie und die Antwortadresse gelöscht; das Gästeprofil bleibt bestehen. Frühere berechtigte Löschanfragen bleiben möglich. Erforderliche Nachweise zu einem konkreten offenen Anspruch werden nur gesondert, zugriffsbeschränkt und für dessen erforderliche Dauer aufbewahrt.

  Versandprotokolle in Reservlys zentraler E-Mail-Verarbeitung werden einschließlich der Schlüssel gegen doppelten Versand 30 Tage nach dem Versand vollständig gelöscht; zugehörige Ereignisse des E-Mail-Dienstleisters werden ebenfalls gelöscht. Nur vorübergehend benötigte Versandinhalte werden bereits nach erfolgreicher Übergabe entfernt, soweit sie nicht für zulässige Fehlerbehebung oder Wiederholung erforderlich sind. Inhaltliche Kopien im Nachrichtencenter und erforderliche Kampagnen- oder Einwilligungsnachweise folgen ihren gesonderten Fristen. Nach einer Abmeldung, einer Spam-Beschwerde oder einer dauerhaft gescheiterten Zustellung wird ein Sperrvermerk mit einem geschützten Vergleichswert der E-Mail-Adresse und dem Anlass gespeichert. Er dient nur dazu, keine weiteren unerwünschten oder unzulässigen E-Mails an diese Adresse zu senden, und wird gelöscht, sobald er dafür nicht mehr erforderlich ist.

  Die Aufbewahrung beim E-Mail-Dienstleister ist von der Speicherung bei Reservly getrennt. Für den eingesetzten Tarif Resend Pro nennt der Anbieter 30 Tage laufende Datenaufbewahrung; Sicherungskopien beim Anbieter folgen dessen eigenem Sicherungszyklus. Dies ist keine einheitliche Frist für alle bei Reservly geführten Datenbestände. Nach Ende des Resend-Vertrags sieht das DPA die Löschung verbleibender Daten innerhalb von 90 Tagen vor. Diese Abwicklungsfrist verlängert weder die laufenden Fristen bei Reservly noch rechtmäßig geschuldete frühere Einzelfalllöschungen. Auskunft zu den betroffenen Datenarten und Unterstützung bei einer früher erforderlichen Löschung sind über support@reservly.at erhältlich.

  Einladungslinks gelten sieben Tage. Nicht angenommene Einladungsprofile werden spätestens 30 Tage nach Ablauf oder Widerruf der Einladung gelöscht, sofern nicht ein

konkret dokumentierter Nachweisfall eine eingeschränkte Aufbewahrung erfordert. Bei Entfernung eines Teammitglieds wird dessen Zugang entzogen; dies ist noch keine vollständige Löschung aller personenbezogenen Daten. Nicht mehr erforderliche Kontakt- und Zusatzangaben des restaurantbezogenen Profils werden spätestens innerhalb von 30 Tagen entfernt. Eine minimale Bearbeiterzuordnung bleibt nur so lange erhalten, wie sie für den jeweiligen rechtmäßig aufbewahrten Vorgang erforderlich ist; sie unterliegt dessen Frist und darf keine dauerhafte Personalakte bilden. Andere berechtigte Restaurantzugänge eines zentralen Kontos bleiben davon getrennt.

8. Weisungen / Kontakt

Weisungen über AVV/Hauptvertrag sowie in Textform (z. B. E-Mail).

Kontakt für Datenschutz/AVV, Support sowie Security/Incidents: support@reservly.at

9. Datenweitergabe und Marketing

Eine gesonderte Vereinbarung mit dem Restaurant allein erlaubt Reservly keine eigene Werbung gegenüber Gästen. Eine Verarbeitung für eigene Zwecke setzt eine eigenständige Rechtsgrundlage, transparente Information und die Einhaltung des Telekommunikationsrechts voraus; sie ist nicht Gegenstand dieses AVV.

Betroffenenanfragen sind unabhängig vom Vorhandensein einer Export-Schaltfläche fristgerecht zu unterstützen. Die gesetzlich erforderliche Bereitstellung von Informationen und Unterstützung darf nicht an unverhältnismäßigen Zusatzentgelten scheitern.

Werden rechtmäßig vorhandene Reservierungskontakte in gesondert gebuchten Restaurantkampagnen verwendet, bleiben Einwilligung, Zweckbindung und Mandantentrennung maßgeblich. Für Kampagnendesign und optionale KI-Unterstützung gelten die ergänzenden Verarbeitungsvorgaben des Loyalty-/Rewards-AVV, soweit diese Funktionen beauftragt sind. Eine bloße Reservierung, Gruppenzuordnung oder Verknüpfung erlaubt weder Direktwerbung noch die Übermittlung von Gastdaten an einen KI-Dienst. Vor einer solchen Beauftragung muss der einschlägige AVV einschließlich des konkreten KI-Unterauftragsverarbeiters wirksam einbezogen sein.

Bei SMS-Versand oder zusätzlichen Medien- und Übersetzungsdiensten muss Reservly den konkreten Unterauftragsverarbeiter samt Leistung, Datenkategorien, Verarbeitungsort und Übermittlungsmechanismus vor seinem Einsatz nach Ziffer 14 mitteilen. Eine bloße Funktionsbeschreibung ersetzt diese Mitteilung und die erforderliche vertragliche Bindung nicht.

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)

1. Ziel und Schutzniveau

Der Auftragsverarbeiter setzt technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau nach Art. 32 DSGVO sicherzustellen. Dies umfasst insbesondere die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste, die Fähigkeit zur Wiederherstellung nach Zwischenfällen sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen.

2. Organisation, Rollen und Verantwortlichkeiten

Alle mit der Verarbeitung befassten Personen sind auf Vertraulichkeit verpflichtet bzw. unterliegen einer gesetzlichen Verschwiegenheitspflicht. Zugriffe auf Produktivdaten erfolgen nach dem Need-to-know-Prinzip; administrative Berechtigungen sind auf wenige Personen beschränkt. Weisungen, Datenschutzanfragen und Sicherheitsmeldungen werden über eine zentrale Kontaktadresse (z. B. support@reservly.at) entgegengenommen und intern klar zugeordnet bzw. eskaliert. Änderungen am System werden über einen nachvollziehbaren Entwicklungs- und Releaseprozess gesteuert; der Quellcode ist versioniert (z. B. GitHub) und Deployments sind nachvollziehbar (z. B. CI/CD über Vercel). Zugriffe auf das CMS/Hosting der öffentlichen Restaurant-Unterseiten sind rollenbasiert

beschränkt (Need-to-know). Veröffentlichungsrechte (Publish) sind auf berechtigte Personen begrenzt. Konten und Zugriffsdaten werden regelmäßig überprüft.

3. Zutritts- und Zugangskontrolle

Die physische Sicherheit der Rechenzentrumsinfrastruktur liegt im Verantwortungsbereich der eingesetzten Cloud-Dienstleister (z. B. Vercel, Supabase, Upstash, Resend, Netlify) und deren organisatorischen und technischen Sicherheitsmaßnahmen. Der Systemzugang zum Restaurant-Dashboard erfolgt ausschließlich über individuelle Benutzerkonten mittels Supabase Auth. Für Konten gelten Passwortrichtlinien nach Stand der Technik; Schutzmechanismen gegen Brute-Force und missbräuchliche Anmeldeversuche werden durch Provider- und Systemmechanismen unterstützt. Zugriffe auf Cloud-Konten, Repositories und Secrets sind auf berechtigte Personen beschränkt und werden regelmäßig überprüft.

4. Zugriffskontrolle und Mandantentrennung (Multi-Tenant)

Reservly ist mandantenfähig aufgebaut. Der Zugriff auf Daten und Funktionen ist technisch so gestaltet, dass Restaurant-Nutzer ausschließlich auf den eigenen Restaurant-Mandanten zugreifen können. Dies erfolgt insbesondere durch serverseitige Autorisierungsprüfungen im Backend, die tenant-ID-basiert sämtliche relevanten Lese- und Schreibzugriffe absichern. Inhaber haben den vorgesehenen vollständigen restaurantbezogenen Zugriff; Teammitglieder erhalten nur zugewiesene Rollen und einzelne Rechte, insbesondere getrennte Rechte für Nachrichten lesen/senden, Gästeverwaltung, Export, Marketing und Administration. Standortzuordnungen dienen im Teammodell der organisatorischen beziehungsweise statistischen Zuordnung und sind keine eigenständige technische Standort-Zugriffsgrenze. Berechtigungen werden serverseitig geprüft; bei Personalwechsel sind Zugang und Sitzungen zeitnah zu entziehen. Ein direkter Datenbankzugriff aus dem Browser für Gast- Funktionen erfolgt nicht; Interaktionen laufen über abgesicherte API-Endpunkte. Öffentliche Aktionen wie Stornieren oder Ändern durch Gäste erfolgen ausschließlich über nicht erratbare Tokens/Links. Dateianhänge des Gästebuchs liegen im privaten Supabase-Objektspeicher. Nach Prüfung der Restaurantzugehörigkeit werden zeitlich begrenzte signierte Anzeige- oder Downloadlinks erzeugt; diese dürfen nicht an unberechtigte Personen weitergegeben werden. Nicht-Bilder werden als Download ausgeliefert.

5. Weitergabekontrolle und Übertragungssicherheit

Die Kommunikation zwischen Widget, Dashboard, Backend und Provider erfolgt über verschlüsselte Schnittstellen (TLS/HTTPS). Schlüssel, Tokens und Zugangsdaten werden geschützt außerhalb des Quellcodes verwaltet. Resend übernimmt den Versand und den Empfang zugehöriger Reservierungsantworten; übertragen werden nur erforderliche Inhalte und Metadaten. Eingehende Webhooks werden auf Echtheit geprüft und Antworten anhand geschützter Zuordnungen dem richtigen Restaurant und Vorgang zugewiesen. Nicht erforderliche Inhalte gehören nicht in Betriebs- und Fehlerprotokolle.

6. Integrität, Eingabekontrolle und Nachvollziehbarkeit

Reservierungen werden über definierte serverseitige API-Routen erstellt, geändert oder storniert. Eingaben werden serverseitig validiert; Statusübergänge folgen einer kontrollierten Logik, um inkonsistente oder manipulierte Zustände zu verhindern. Sicherheits- und betriebsrelevante Ereignisse (z. B. Authentifizierungsereignisse, fehlgeschlagene Logins, kritische Änderungen wie Storno/Umbuchung) werden in angemessenem Umfang protokolliert. Der Zugriff auf Protokolle ist beschränkt; Logdaten werden nur so lange gespeichert, wie es für Sicherheit und Betrieb erforderlich ist (regelmäßig höchstens 30 bis 90 Tage ab Ereignis, abhängig von notwendigem Betriebs- oder Sicherheitszweck; frühere Löschung bei Wegfall des Zwecks), sofern keine längeren gesetzlichen Pflichten bestehen. Soweit Protokollierung durch Unterauftragsverarbeiter erfolgt (z. B. Hosting/CDN), gelten ergänzend deren Aufbewahrungsfristen; der Auftragsverarbeiter nutzt solche Logs nur, soweit erforderlich (z. B. Störungsanalyse/Sicherheit). Das Nachrichtencenter kann Bearbeitername/-kennung, Änderungszeitpunkte und frühere beziehungsweise neue Reservierungsangaben enthalten. Gemeinsame Gelesen- und Sternmarkierungen sind keine

personenbezogenen Lesebestätigungen. Der Verlauf unterliegt der Chatfrist; andere Protokolle folgen ihrem eigenen erforderlichen Zweck.

7. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

Der Betrieb erfolgt auf skalierbarer Cloud-Infrastruktur (z. B. Vercel für Deployment/Hosting, Supabase für Datenbank und Auth in EU-Region). Es werden regelmäßige Backups der Datenbank erstellt; die konkreten Sicherungszyklen und maximalen Aufbewahrungsfristen werden nach Ziffer 13 dokumentiert und mitgeteilt. Für Störungen und Ausfälle bestehen Wiederherstellungsverfahren; nach Wiederherstellungen werden Lösch- und Anonymisierungsprozesse erneut angewandt. Monitoring und Fehleranalyse unterstützen die Sicherstellung der Verfügbarkeit und Stabilität des Systems.

8. Datenminimierung, Pseudonymisierung und Speicherbegrenzung

Im Reservierungsprozess werden nur die für die Reservierungsabwicklung erforderlichen Daten erhoben (Name, E-Mail-Adresse, Telefonnummer; Notizfeld optional). Zur Missbrauchsprävention wird Rate Limiting eingesetzt; hierbei wird ausschließlich eine pseudonymisierte Kennung (Hash der IP-Adresse mit geheimem Schlüssel) in Upstash Redis gespeichert und nach spätestens einer Stunde automatisch gelöscht. Zur Speicherbegrenzung werden personenbezogene Reservierungsdaten (Name, E-Mail, Telefon, Notizen) automatisiert nach Ablauf der Reservierungsfrist des Restaurants (Standard 30 Tage nach dem Reservierungsdatum, Ziffer 13 Absatz 1) anonymisiert (Entfernung/Nullsetzung der personenbezogenen Felder), wobei verbleibende Gastprofil-Verknüpfungen gesondert nach Ziffer 13 zu behandeln sind und nur tatsächlich anonyme Metadaten unbefristet für Statistiken verbleiben dürfen. Produktions- und Entwicklungsumgebungen sind getrennt; Live-Daten werden in Entwicklungs-/Testumgebungen nicht eingesetzt oder nur nach Anonymisierung/Pseudonymisierung. Nachrichtenkopien, Providerereignisse, Teamprofile und identifizierender Feedbacktext werden nach Ziffer 13 einbezogen. Löschläufe werden überwacht und Fehler nachbearbeitet; nach Wiederherstellung sind Löschungen erneut anzuwenden.

9. Unterauftragsverarbeiter und internationale Übermittlungen

Unterauftragsverarbeiter werden nach geeigneten Datenschutz- und Sicherheitskriterien ausgewählt und vertraglich nach Art. 28 DSGVO eingebunden. Änderungen bei Unterauftragsverarbeitern erfolgen gemäß den Informations- und Widerspruchsregelungen des AVV. Sofern Drittlandzugriffe nicht sicher ausgeschlossen werden können, werden Übermittlungen nur unter Einhaltung der Vorgaben der Art. 44 ff. DSGVO vorgenommen (z. B. Standarddatenschutzklauseln und Transfer Impact Assessment, soweit erforderlich).

10. Incident Response und Datenschutzverletzungen

Für Sicherheitsvorfälle besteht ein dokumentierter Prozess zur Erkennung, Eindämmung, Bewertung, Behebung und Dokumentation. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über bekannt gewordene Verletzungen des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betreffen, und stellt die verfügbaren Informationen zur Unterstützung der Pflichten des Verantwortlichen nach Art. 33 und 34 DSGVO bereit.

11. Regelmäßige Überprüfung und Verbesserung

Die TOMs werden regelmäßig überprüft und bei wesentlichen Änderungen der Verarbeitung, des Systems, der Architektur oder der eingesetzten Unterauftragsverarbeiter angepasst, ohne das Schutzniveau abzusenken. Berechtigungen (Zugänge, Rollen, administrative Rechte) werden mindestens 1-mal pro Jahr überprüft. Sicherheitsupdates und Abhängigkeiten werden im Rahmen des Entwicklungs- und Deployment-Prozesses gepflegt.

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung / Rolle	Ort/Region / Drittlandhinweis

Unterauftragsverarbeiter	Leistung / Rolle	Ort/Region / Drittlandhinweis
Supabase	Datenbank (PostgreSQL), Auth (Supabase Auth), ggf. Realtime sowie privater Objektspeicher für Gästebuch-Dateianhänge	EU/EWR (AWS eu-central-1, Frankfurt); Art. 44 ff. DSGVO ggf. relevant.
Vercel	Hosting/Deployment (Widget, API, Dashboard)	Globales CDN/Edge; Verarbeitung ggf. EU/EWR und Drittländer (insb. USA). Drittlandübermittlungen möglich → Art. 44 ff. DSGVO (z. B. SCC).
Upstash	Redis Rate Limiting (IP-Hash, TTL max. 1h)	EU/EWR – Region gemäß Projektkonfiguration (z. B. Frankfurt). Drittlandzugriffe nicht vollständig ausgeschlossen → Art. 44 ff. DSGVO (SCC).
Resend / Plus Five Five, Inc., USA	Versand transaktionaler und zulässig beauftragter E-Mails, Empfang von Reservierungsantworten, technische Zustell- und Sperrdaten; erforderliche Kontaktangaben, Inhalte und Metadaten	USA; keine Zusage ausschließlicher EU-Speicherung. DPA und EU-Standardvertragsklauseln Modul 3 für Unterauftragsverarbeitung; ergänzende Maßnahmen nach Ziffer 15. Eigene Account-/Nutzungszwecke des Anbieters sind gesondert nach Ziffer 15 abgegrenzt; insoweit keine pauschale Unterauftragsverarbeiterrolle.
Netlify, Inc., USA	Hosting und CDN der öffentlichen Restaurant-Unterseiten (reservly.at/restaurant/…).	Globale Infrastruktur, Verarbeitung auch in den USA. Netlify-DPA; EU-US Data Privacy Framework, soweit anwendbar, andernfalls EU-Standardvertragsklauseln (Modul 3) samt ergänzenden Maßnahmen.

Änderungen und Widerspruch: Es gilt Ziffer 14 mit aktiver Mitteilung, mindestens 14 Tagen Vorlauf und Widerspruchsmöglichkeit. Verspätete Informationen eines vorgelagerten Dienstleisters verkürzen diese Zusage nicht.

Soweit vor der Umstellung rechtmäßig an Brevo beziehungsweise die Sendinblue-Unternehmensgruppe übermittelte Daten noch zur erforderlichen Abwicklung, Löschung oder Erfüllung konkreter Nachweispflichten vorhanden sind, bleibt Brevo hierfür Empfänger. Nach der Umstellung werden darüber keine neuen Nachrichten im umgestellten Bereich versandt. Restbestände werden zweckgebunden bereinigt; die Mitteilung zum Wechsel bezeichnet den betroffenen Umfang und den Übergang. Eine Übernahme alter Sperr- oder Abmeldedaten begründet keine neue Werbeerlaubnis.