Vertrag über Auftragsverarbeitung nach Art. 28 DSGVO

(„Auftragsverarbeitungsvertrag“ / „Data Processing Agreement“)

Produkt: Reservly Rewards / Loyalty-Bonussystem

Stand: 15.10.2026 Version: 4.4

zwischen

Lukas Gerber, Einzelunternehmer, handelnd unter der Marke „Reservly“

Wassergasse 32, 1030 Wien, Österreich

GISA-Zahl: 40050812

E-Mail: support@reservly.at

Kontakt für Datenschutzanfragen: support@reservly.at

– nachfolgend „Auftragsverarbeiter“ oder „Reservly“ –

und

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

– nachfolgend „Verantwortlicher“ oder „Restaurant“ –

gemeinsam auch die „Parteien“.

Hinweis zur elektronischen Form: Dieser Vertrag wird elektronisch im Rahmen des Loyalty-Onboardings abgeschlossen. Mit der gesonderten AVV-Checkbox akzeptiert der Verantwortliche diesen Vertrag in der jeweils angezeigten Version. Reservly protokolliert Restaurant, handelnden Benutzer, Version, Dokumentpfad, Zeitpunkt und Annahmekanal. Diese elektronische Form genügt Art. 28 Abs. 9 DSGVO.

1. Gegenstand und Geltungsbereich

(1) Dieser AVV gilt ausschließlich für Verarbeitungen personenbezogener Daten, die Reservly beim Betrieb von Reservly Rewards im Auftrag des Restaurants gemäß Art. 28 DSGVO durchführt.

(2) Erfasst sind – soweit vom Restaurant aktiviert – insbesondere Punkteprogramme, digitale Stempelkarten, Prämien und Gutscheine, Mitgliedschaften, QR- und Scanvorgänge, administrative Freigaben, manuelle Korrekturen, Kampagnen über E-Mail, Push oder In-App, zeit-, wetter-, geburtstags- oder standortbezogene Auslöser, Wallet-Pässe, Statistiken, Missbrauchsprotokolle und optionale Minigames. Erfasst sind außerdem das restaurantbezogene Gästebuch, manuelle Kontakte, Notizen und Dateien, manuelle Gruppen und Smartgruppen, Kampagnendesign und optionale KI-Unterstützung. CSV-Import und -Export eigener Gästebuchdaten sowie bewusst gewählte KI-Dateieingaben sind nach Maßgabe der Anlagen erfasst.

(3) Nicht erfasst sind das Reservierungssystem oder andere separat gebuchte Reservly-Produkte. Hierfür gelten gegebenenfalls eigene Vereinbarungen. Ebenfalls nicht erfasst sind Verarbeitungen, für die Reservly nach § 4.3 selbst Verantwortlicher ist. Die Anzeige rechtmäßig zugeordneter Reservierungsbezüge desselben Restaurants im Gästebuch ist als Schnittstelle erfasst; die eigentliche Reservierungsabwicklung bleibt dem gesonderten AVV zugeordnet. Das Nachrichtencenter einschließlich der Reservierungschats und der Direktchats mit Gästebuchkontakten bleibt dem AVV Reservierungssystem zugeordnet.

(4) Der konkrete Umfang richtet sich nach den aktivierten Funktionen, den Einstellungen des Restaurants, dessen dokumentierten Weisungen sowie Anlage 1.

2. Begriffsbestimmungen

(1) Es gelten die Begriffe der DSGVO, insbesondere „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „Unterauftragsverarbeiter“, „betroffene Person“ und „Verletzung des Schutzes personenbezogener Daten“.

(2) „Mitglied“ bezeichnet eine Endkundin oder einen Endkunden, die oder der einem vom Restaurant betriebenen Rewards-Programm beigetreten ist. „Restaurantpersonal“ umfasst Beschäftigte und sonstige vom Restaurant autorisierte Personen mit Dashboard-, Scanner-, Kiosk- oder Freigabezugriff.

(3) „Programm“ umfasst die vom Restaurant festgelegten Regeln, Punkte, Stempel, Prämien, Gutscheine, Aktionen, Inhalte und zugeordneten Standorte. Ein standortübergreifendes Programm darf nur Standorte derselben Rechtsperson umfassen, sofern keine gesonderte rechtliche und vertragliche Regelung getroffen wird.

3. Dauer der Verarbeitung

(1) Dieser AVV beginnt mit seiner elektronischen Annahme und gilt, solange Reservly im Auftrag des Restaurants personenbezogene Daten für Reservly Rewards verarbeitet.

(2) Die Verarbeitung endet grundsätzlich mit Beendigung des Rewards-Moduls und Abschluss einer vorgesehenen Abwicklungsphase. Soweit die Hauptvereinbarung eine 90-tägige Abwicklungsphase vorsieht, darf Reservly die hierfür erforderlichen Daten bis zu deren Ende verarbeiten; währenddessen können bestehende Ansprüche eingelöst und Mitglieder informiert werden.

(3) Gesetzliche Aufbewahrungspflichten, berechtigte Sicherheits- oder Missbrauchsnachweise und technisch unvermeidbare Sicherungskopien bleiben nach Maßgabe von § 13 und Anlage 1 unberührt.

4. Rollenverteilung und Weisungsrahmen

(1) Das Restaurant ist Verantwortlicher für die Zwecke und wesentlichen Mittel seines Programms. Dies betrifft insbesondere Programmbedingungen, Punkte- und Stempelvergabe, Prämien und Gutscheine, Freigaben und Korrekturen durch Restaurantpersonal, restaurantbezogene Mitgliederverwaltung, Kampagnen und Zielgruppen sowie die hierfür erforderlichen Rechtsgrundlagen und Informationspflichten.

(2) Reservly verarbeitet diese Daten als Auftragsverarbeiter ausschließlich auf dokumentierte Weisung des Restaurants, soweit nicht Unionsrecht oder österreichisches Recht eine Verarbeitung verlangt. In diesem Fall informiert Reservly das Restaurant vor der Verarbeitung, sofern das Recht dies nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

(3) Außerhalb dieses AVV kann Reservly für klar abgegrenzte Plattformzwecke selbst Verantwortlicher sein, insbesondere für das zentrale Reservly-Konto und Login, Kontosicherheit, die vom Endkunden selbst gesteuerte zentrale Verwaltung seiner Mitgliedschaften, zwingende technische Plattformkommunikation sowie notwendige plattformweite Sicherheits- und Missbrauchsprävention. Diese Verarbeitungen richten sich nach der Reservly-Datenschutzerklärung und dürfen nicht auf Weisung des Restaurants für andere Zwecke umgewidmet werden.

(4) Soweit sich die tatsächlichen Zwecke und Mittel künftig ändern oder eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO entsteht, werden die Parteien vor Aktivierung der betreffenden Funktion eine gesonderte Vereinbarung schließen. Dieser AVV begründet für sich allein keine gemeinsame Verantwortlichkeit.

5. Art, Zweck und Umfang der Auftragsverarbeitung

(1) Reservly erhebt, erfasst, ordnet, speichert, aktualisiert, gleicht ab, übermittelt, stellt bereit, protokolliert, schränkt ein, anonymisiert und löscht personenbezogene Daten, soweit dies zur Bereitstellung und Absicherung der vom Restaurant gewählten Rewards-Funktionen erforderlich ist.

(2) Die Verarbeitung dient ausschließlich dem technischen Betrieb des restaurantbezogenen Programms, der Erfassung und Einlösung von Punkten, Stempeln, Prämien und Gutscheinen, der Mitglieder- und Statusverwaltung, der Kampagnenzustellung, der optionalen Standort- und Wallet-Funktionen, der Nachvollziehbarkeit von Freigaben und Korrekturen, der Fehlerbehebung, der Sicherheit sowie der vom Restaurant beauftragten Auswertung.

(3) Kategorien betroffener Personen und personenbezogener Daten sind in Anlage 1 abschließend nach Funktionsgruppen beschrieben. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht vorgesehen. Das Restaurant darf keine sensiblen Zielgruppen, diskriminierenden Kriterien oder Eingaben verlangen und hat Freitextfelder entsprechend zu verwenden.

6. Pflichten des Verantwortlichen

(1) Das Restaurant ist für die Rechtmäßigkeit der Verarbeitung, die Zulässigkeit seiner Weisungen, die Richtigkeit seiner Programmregeln und die Erfüllung der Betroffeneninformationen verantwortlich.

(2) Das Restaurant stellt die erforderlichen Einwilligungen für Werbeversand und personenbezogene Angebotsauswahl sicher. Maßgeblich sind Restaurant, Kanal, Zweck und einbezogene Datenarten; ein allgemeiner Marketingstatus ersetzt diesen Umfangsnachweis nicht. Push benötigt zusätzlich die Gerätefreigabe, Geofence-Marketing eine gesonderte Einwilligung. Ein Widerruf muss ebenso einfach möglich sein wie die Erteilung. Die Programmteilnahme darf nicht von nicht erforderlicher Werbung abhängen.

(3) Das Restaurant legt Inhalte, Zielgruppen, Zeitpunkt, Kanal und Frequenz von Kampagnen fest und beachtet insbesondere DSGVO, TKG 2021 und wettbewerbsrechtliche Vorgaben. Öffnungs- oder Klicktracking ist nicht Bestandteil der beauftragten Funktion; verarbeitet werden nur technische Zustell-, Fehler-, Bounce-, Abmelde- und Einlösedaten.

(4) Das Restaurant verwaltet die Zugriffe seines Personals nach dem Need-to-know-Prinzip.

Administrative Loyalty-Funktionen werden dem verfügbaren authentifizierten Restaurantkonto beziehungsweise einem persönlich freigegebenen Teammitglied zugeordnet. Persönliche vierstellige Teamcodes und die weiterhin mögliche gemeinsame vierstellige Admin-PIN sind getrennte Verfahren. Bei gemeinsamer PIN ist eine eindeutige Zuordnung zur tatsächlich handelnden natürlichen Person nicht allein durch die PIN gewährleistet. Individuelle Zugänge und Codes sind nicht weiterzugeben; gemeinsame Codes sind auf berechtigte Personen zu beschränken und bei Personalwechsel oder Verdacht unverzüglich zu ändern.

(5) Das Restaurant informiert Reservly unverzüglich über fehlerhafte Daten, unrechtmäßige Weisungen, Sicherheitsereignisse in seiner Sphäre und Umstände, die eine Datenschutz-Folgenabschätzung erfordern könnten.

(6) 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. 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.

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.

7. Weisungen

(1) Die Hauptvereinbarung, dieser AVV, die im Dashboard vorgenommenen Einstellungen, Funktionsaktivierungen, Kampagnenaufträge und berechtigten Supportanfragen bilden die dokumentierten Weisungen des Restaurants.

(2) Einzelweisungen können in Textform an support@reservly.at erteilt werden. Sie müssen eindeutig, rechtmäßig, technisch umsetzbar und auf die Auftragsverarbeitung beschränkt sein. Reservly dokumentiert wesentliche Einzelweisungen und deren Umsetzung.

(3) Hält Reservly eine Weisung für datenschutzrechtswidrig, informiert Reservly das Restaurant unverzüglich und darf die Ausführung bis zur Bestätigung, Änderung oder Klärung aussetzen. Offenkundig rechtswidrige Weisungen werden nicht ausgeführt.

(4) Änderungen, die erhebliche Zusatzleistungen oder eine wesentliche Systemanpassung erfordern, werden vor Umsetzung hinsichtlich Aufwand, Zeitplan und gegebenenfalls Vergütung abgestimmt.

8. Vertraulichkeit und eingesetzte Personen

(1) Reservly setzt nur Personen ein, die auf Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind und nur im erforderlichen Umfang Zugriff erhalten.

(2) Die Verpflichtung besteht nach Ende der Tätigkeit fort. Reservly schult berechtigte Personen regelmäßig zu Datenschutz, Informationssicherheit, Mandantentrennung und sicherem Umgang mit Support- und Produktionszugriffen.

(3) Zugriffe auf Produktionsdaten erfolgen nur für Betrieb, Wartung, Support, Fehleranalyse, Sicherheit oder aufgrund einer dokumentierten Weisung und werden nach Maßgabe der TOMs kontrolliert.

9. Technische und organisatorische Maßnahmen

(1) Reservly trifft und erhält die in Anlage 2 beschriebenen Maßnahmen nach Art. 32 DSGVO. Maßgeblich sind Risiko, Stand der Technik, Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung.

(2) Reservly darf Maßnahmen weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und dem Restaurant auf Anfrage mitgeteilt.

(3) Das Restaurant ist für die Sicherheit seiner Endgeräte, Netzwerke, E-Mail-Konten, Scanner- und Kioskgeräte, Zugangsdaten sowie für die interne Rollenvergabe verantwortlich. Reservlys TOMs entbinden das Restaurant nicht von eigenen Maßnahmen nach Art. 24 und 32 DSGVO.

10. Unterstützung bei Betroffenenrechten

(1) Reservly unterstützt das Restaurant unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei Anträgen nach Art. 12 bis 23 DSGVO, insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Widerruf.

(2) Erhält Reservly einen Antrag, der erkennbar Daten des Restaurants betrifft, leitet Reservly ihn ohne unangemessene Verzögerung an das Restaurant weiter und beantwortet ihn nicht eigenständig, außer auf dokumentierte Weisung oder soweit Reservly für den betreffenden Verarbeitungsteil selbst Verantwortlicher ist.

(3) Das Restaurant bleibt für Prüfung, Identitätsfeststellung, inhaltliche Entscheidung und fristgerechte Antwort verantwortlich. Reservly stellt vorhandene Export-, Sperr-, Berichtigungs- und Löschfunktionen bereit oder unterstützt angemessen über den Support.

Die Unterstützung umfasst auch rechtmäßig vorhandene E-Mail-Inhalte und Metadaten, Sperrlisten und einschlägige Providerbestände. Früheres Löschen oder Einschränken bei einer berechtigten Anfrage bleibt unabhängig vom regulären Bereinigungszyklus geschuldet. Daten eines anderen Restaurants und eigenverantwortliche zentrale Kontodaten werden nur im jeweils zulässigen Umfang einbezogen.

11. Unterstützung bei Sicherheit, Folgenabschätzung und Behörden

(1) Reservly unterstützt das Restaurant angemessen bei Pflichten nach Art. 32 bis 36 DSGVO, soweit die Unterstützung die Auftragsverarbeitung betrifft und die erforderlichen Informationen Reservly vorliegen.

(2) Dies umfasst Informationen zu Sicherheitsmaßnahmen, Risikobewertungen, Datenschutz-Folgenabschätzungen, Konsultationen der Aufsichtsbehörde und Nachweise zur Verarbeitung. Das Restaurant stellt Reservly die für eine konkrete Unterstützung erforderlichen Angaben rechtzeitig bereit.

(3) Zusatzaufwand, der über die gesetzlich geschuldete und im üblichen Leistungsumfang enthaltene Unterstützung hinausgeht, kann nach vorheriger Abstimmung angemessen verrechnet werden.

12. Verletzungen des Schutzes personenbezogener Daten

(1) Reservly meldet dem Restaurant eine Verletzung des Schutzes personenbezogener Daten im Verantwortungsbereich von Reservly unverzüglich nach Bekanntwerden, soweit Daten des Restaurants betroffen sind.

(2) Die Meldung enthält, soweit verfügbar, Art des Vorfalls, betroffene Daten und Personengruppen, ungefähres Ausmaß, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Abhilfemaßnahmen sowie eine Kontaktstelle. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

(3) Reservly dokumentiert Vorfälle und unterstützt das Restaurant bei dessen Bewertung sowie bei Meldungen nach Art. 33 und 34 DSGVO. Die Verantwortung für Meldungen an Behörde und Betroffene bleibt beim Restaurant, soweit dieses Verantwortlicher ist.

(4) Das Restaurant meldet Reservly unverzüglich Vorfälle in seiner Sphäre, die die Plattform oder Daten anderer Mandanten gefährden könnten, und wirkt an Eindämmung und Aufklärung mit.

13. Berichtigung, Löschung, Rückgabe und Aufbewahrung

(1) Reservly berichtigt, sperrt, exportiert, anonymisiert oder löscht Daten nach dokumentierter Weisung und gemäß Anlage 1, soweit keine vorrangige gesetzliche Pflicht oder ein zulässiger, klar abgegrenzter eigener Verarbeitungszweck entgegensteht.

(2) Nach Ende der Auftragsverarbeitung löscht oder gibt Reservly auf Wahl des Restaurants die noch vorhandenen Auftragsdaten zurück und löscht vorhandene Kopien, soweit nicht Unionsrecht oder österreichisches Recht eine weitere Speicherung verlangt. Die Wahl ist vor Vertragsende mitzuteilen; andernfalls erfolgt die Löschung nach dem Standard- Löschkonzept.

(3) Daten in Sicherungskopien werden nicht für operative Zwecke wiederhergestellt, außer zur Wiederherstellung des Systems, und mit den regulären Backup-Zyklen überschrieben oder gelöscht. Bis dahin bleiben sie geschützt und zugriffsbeschränkt.

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.

(4) Die beauftragte Belegprüfung umfasst das Auslesen und Validieren strukturierter RKSV-QR-Daten, die Berechnung der Punkte oder Stempel, die Prüfung wiederholter Verwendung und die erforderliche Nachweisführung. Das Restaurant kann für die Vergabe von Punkten oder Stempeln einen Rechnungsscan als regulären Nachweis voraussetzen. Dies ist vor der Teilnahme zusammen mit Umrechnung, Rundung, Mindestbetrag, zulässigem Belegalter und sonstigen Teilnahmegrenzen verständlich mitzuteilen. Beim Mitarbeitenden-Scan werden die Werte aus dem RKSV-QR-Code berechnet und von berechtigtem Personal bestätigt. Ein Gast-Selbstscan mit automatischer Gutschrift ist nur verfügbar, soweit dieses Verfahren für das betreffende Programm tatsächlich freigeschaltet ist. Eine Vorschau oder Testanzeige ist keine verbuchte Gutschrift. Ohne erforderlichen gültigen Nachweis erfolgt grundsätzlich keine Vergabe über den Scanweg; eine begründete manuelle Prüfung oder Korrektur durch das Restaurant bleibt möglich.

Der QR-Rohinhalt wird ausschließlich flüchtig zur Validierung verarbeitet und unmittelbar nach deren Abschluss verworfen; er darf weder in Datenbanken noch in Protokollen, Analysediensten oder dauerhaften Gerätespeichern abgelegt werden. Für den Duplikatsschutz wird ein kryptografischer Hash des QR-Codes verwendet. Gespeichert werden nur erforderliche strukturierte Nachweisdaten: Hash, Restaurant- und Programmzuordnung, Belegkennung und erforderliche Kassenkennung, Belegbetrag und -zeitpunkt, Scanzeitpunkt, Prüfergebnis, Mitgliedschafts- und Buchungszuordnung, gutgeschriebene Punkte oder Stempel sowie die angewandte Berechnungsregel. Beim Personalverfahren können die erforderliche Mitarbeiterkennung und begründete Korrekturen hinzukommen. Der mit einer Mitgliedschaft verknüpfte Hash ist pseudonym und nicht anonym. Rechnungsbilder werden nicht gespeichert; eine Bildarchivierung oder OCR-Auswertung gehört nicht zu diesem Verfahren.

Das Restaurant ist Verantwortlicher für Programmbedingungen, Rechtsgrundlagen und erforderliche Speicherfristen; Reservly handelt bei der Durchführung dieser Scan- und Buchungsvorgänge als Auftragsverarbeiter. Betroffen sind teilnehmende Gäste und handelnde Mitarbeitende. Ein Selbstscan erfordert keine Kenntnisgabe fremder Gäste- oder Belegdaten. Die Einbindung eines neuen Dienstes zur Bild- oder OCR-Verarbeitung bedarf vor Einsatz einer gesonderten Beauftragung und Prüfung nach diesem AVV.

14. Unterauftragsverarbeiter

(1) Das Restaurant erteilt Reservly eine allgemeine Genehmigung, die in Anlage 3 genannten Unterauftragsverarbeiter einzusetzen. Reservly schließt mit ihnen Verträge, die im Wesentlichen gleichwertige Datenschutzpflichten vorsehen, soweit Art. 28 DSGVO anwendbar ist.

(2) 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.

(3) Können die Parteien einen berechtigten Widerspruch nicht durch eine zumutbare Alternative lösen, darf das Restaurant die konkret betroffene Funktion zum Änderungszeitpunkt außerordentlich beenden. Ein Widerspruch darf nicht allein auf sachfremden oder wettbewerblichen Gründen beruhen. Bis zur Klärung wird die konkret betroffene geänderte Verarbeitung ausgesetzt oder über eine bereits zulässige Alternative erbracht.

(4) Reservly bleibt gegenüber dem Restaurant für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich, soweit dies gesetzlich vorgesehen ist.

15. Verarbeitungsorte und Drittlandübermittlungen

(1) Reservly bevorzugt für Kernverarbeitung und Speicherung europäische Regionen. Einzelne technische Anbieter können Daten in Drittländern verarbeiten oder von dort zugreifen, insbesondere bei Push-, Wallet-, Support-, Sicherheits- oder globalen Infrastrukturleistungen. Der E-Mail-Einsatz von Resend umfasst reguläre Verarbeitung und Speicherung in den USA.

(2) Eine Übermittlung in ein Drittland erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage eines Angemessenheitsbeschlusses, einer gültigen Zertifizierung nach dem EU–US Data Privacy Framework, geeigneter Standardvertragsklauseln einschließlich erforderlicher Zusatzmaßnahmen oder einer anderen zulässigen Grundlage.

(3) Reservly stellt dem Restaurant auf Anfrage Informationen zur einschlägigen Übermittlungsgrundlage zur Verfügung. Optionale Dienste, die der Endkunde selbst aktiviert und für die Apple, Google oder ein anderer Anbieter eigenständig verantwortlich ist, fallen nur insoweit unter diesen AVV, als Reservly darin tatsächlich im Auftrag des Restaurants handelt.

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. Nachweise und Kontrollen

(1) Reservly stellt alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art.

28 DSGVO erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen durch das Restaurant oder einen von diesem beauftragten, fachkundigen und zur Verschwiegenheit verpflichteten Prüfer.

(2) Vorrangig werden aktuelle Dokumentationen, TOM-Beschreibungen, Zertifikate, Prüfberichte oder schriftliche Auskünfte verwendet. Vor-Ort-Prüfungen sind mit angemessener Frist abzustimmen, dürfen den Betrieb und Rechte anderer Kunden nicht beeinträchtigen und finden grundsätzlich während üblicher Geschäftszeiten statt.

(3) Eine Beschränkung auf eine Prüfung pro Kalenderjahr gilt nicht bei konkretem Verdacht, Sicherheitsvorfall, behördlicher Anordnung oder wesentlicher Änderung der Verarbeitung. Eigene Kosten trägt grundsätzlich jede Partei; außergewöhnlicher Zusatzaufwand kann bei unbegründeten oder unverhältnismäßigen Prüfungen nach Vorabinformation verrechnet werden.

17. Dokumentation und Mitwirkung

(1) Reservly führt die gesetzlich erforderlichen Verzeichnisse und stellt dem Restaurant die für dessen Verzeichnis der Verarbeitungstätigkeiten erforderlichen Informationen zur Auftragsverarbeitung bereit.

(2) Die Parteien arbeiten mit der zuständigen Datenschutzbehörde zusammen. Reservly informiert das Restaurant über behördliche Anfragen zu dessen Auftragsdaten, soweit dies rechtlich zulässig ist.

(3) Das Restaurant hält seine Stammdaten, Ansprechpartner, Rollen, Standorte und Weisungen aktuell. Es dokumentiert insbesondere Kampagnenentscheidungen, Einwilligungstexte, Zielgruppenregeln und Berechtigungen des Restaurantpersonals.

Dokumentierter Abschlussnachweis

Der Abschlussnachweis bezeichnet das Restaurant und die handelnde berechtigte Person, die angenommene AVV-Version loyalty-4.4, die unveränderbar zugeordnete Dokumentfassung, Datum, Uhrzeit und Annahmekanal. Historische angenommene Fassungen bleiben unverändert erhalten; eine neue Version wird gesondert zugeordnet. Eine technische Freischaltung ersetzt nicht die erforderliche dokumentierte Beauftragung.

18. Rangfolge, Änderungen und Beendigung

(1) Bei Widersprüchen zu datenschutzrechtlichen Fragen geht dieser AVV der Hauptvereinbarung und den Allgemeinen Geschäftsbedingungen vor. Im Übrigen bleiben die Hauptvereinbarung und die AGB unberührt.

(2) Reservly kann diesen AVV an geänderte Rechtslage, Behördenpraxis, Produktfunktionen oder Unterauftragsverhältnisse anpassen. Wesentliche Änderungen werden rechtzeitig mitgeteilt und erfordern, soweit rechtlich oder vertraglich notwendig, eine erneute elektronische Zustimmung.

(3) Die Beendigung des Rewards-Moduls beendet diesen AVV nach Abschluss der zulässigen Abwicklung, ohne dass es einer gesonderten Kündigung bedarf. Fortwirkende Pflichten, insbesondere Vertraulichkeit, Nachweis, Löschung und gesetzliche Aufbewahrung, bleiben bestehen.

19. Geschäftsgeheimnisse und Rechte Dritter

(1) Beide Parteien behandeln im Rahmen dieses AVV bekannt werdende Geschäfts- und Betriebsgeheimnisse sowie Sicherheitsinformationen vertraulich.

(2) Prüfungen und Auskünfte sind so durchzuführen, dass Quellcode, Sicherheitsarchitektur, Daten anderer Restaurants und Rechte von Unterauftragsverarbeitern nur im erforderlichen Umfang offengelegt werden. Gleichwertige Nachweise können eine direkte Offenlegung ersetzen, soweit der gesetzliche Kontrollzweck erreicht wird.

20. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses AVV bedürfen zumindest der Textform; elektronische Zustimmung und systemseitige Protokollierung genügen, soweit gesetzlich zulässig.

(2) Sollten einzelne Bestimmungen unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle einer unwirksamen Bestimmung treten die gesetzlichen Vorschriften.

(3) Es gilt österreichisches Recht unter Ausschluss seiner Verweisungsnormen, soweit zwingendes Datenschutzrecht nicht entgegensteht. Gerichtsstand und Streitbeilegung richten sich nach der Hauptvereinbarung und zwingendem Recht.

(4) Die Anlagen 1 bis 3 sind Bestandteil dieses AVV.

Anlage 1 – Beschreibung der Verarbeitung

1. System / Komponenten

Reservly Rewards ist ein webbasiertes und appgestütztes Loyalty-Bonussystem (SaaS) für Restaurants mit folgenden Komponenten:

- Mitgliederkonto im Programm: Beitritt, Status, Zuordnung zum Restaurant/Standort, Punkte- und Stempelsaldo, Historie, Austritt und Sperren.
- Punkte, Stempel, Prämien und Gutscheine: Gutschrift, Einlösung, Korrektur, Storno, Ablauf nach Programmende und Nachweis der Transaktion.
- QR, Scanner und Kiosk: Erzeugung und Prüfung zufälliger bzw. gehashter Mitgliedschafts- und Sitzungstokens; Scan- und Freigabevorgänge; Synchronisation und Missbrauchsschutz.
- Administrative Freigaben: Individuelle Restaurantzugänge und persönliche vierstellige Teamcodes sowie weiterhin mögliche gemeinsame vierstellige Admin-PIN; erforderliche Zuordnung und Protokollierung gemäß Ziffer 6. Keine stets persönliche Identifizierung allein durch die gemeinsame PIN.
- Kampagnen: Technischer Versand von E-Mail, Push und In-App-Nachrichten im nachgewiesenen restaurant-, kanal- und zweckbezogenen Einwilligungsumfang; Geofence-Marketing benötigt einen gesonderten Nachweis, Push zusätzlich die Geräteberechtigung. Zustell- und Fehlerstatus ohne Öffnungs-/Klicktracking.
- Automationen: Zeit-, Wetter-, Geburtstag-, Welcome- und standortbezogene Auslöser; ein Geofence je Kampagne und technisch bis zu 20 gleichzeitig aktive Regionen auf dem Endgerät.
- Wallet: Optionale Apple- oder Google-Wallet-Pässe, Serien-/Objektkennungen, QR/Barcode, Saldo-/Statusupdates und technische Registrierungen.
- Minigames: Teilnahme, zufälliges Ergebnis, Gewinnzuordnung, Frequenzbegrenzung und Missbrauchsschutz; kein Einsatz gegen Entgelt ohne gesonderte Prüfung.
- Dashboard, API und Support: Mandantenbezogene Verwaltung, Statistiken, Exporte, Fehleranalyse, Rechteverwaltung, Protokollierung und Support.

2. Art der Verarbeitung (Vorgänge)

Erheben, Erfassen, Ordnen, Speichern, Auslesen, Aktualisieren, Abgleichen, Übermitteln, Bereitstellen, Protokollieren, Einschränken, Exportieren, Anonymisieren und Löschen personenbezogener Daten, soweit dies für die aktivierten Rewards-Funktionen erforderlich ist.

3. Zwecke der Verarbeitung im Auftrag

- Bereitstellung und Durchführung des vom Restaurant konfigurierten Bonusprogramms einschließlich Nachweis von Gutschriften, Einlösungen, Korrekturen und Mitgliedschaftsstatus.
- Zustellung rechtmäßig beauftragter Werbekampagnen und Auswahl ihrer Empfänger innerhalb des jeweils nachgewiesenen Einwilligungsumfangs. Davon getrennt erfolgt die Zustellung notwendiger transaktionaler Programmnachrichten auf deren eigener Rechtsgrundlage.
- Betrieb optionaler QR-, Scanner-, Kiosk-, Wallet-, Standort-, Wetter-, Geburtstags- und Minigame-Funktionen.
- Mandantentrennung, Zugriffskontrolle, Verfügbarkeit, Fehlerbehebung, Synchronisation, Rate-Limits für ausgewählte Authentifizierungs- und Provider-Schnittstellen, Sicherheits- und Missbrauchserkennung sowie Unterstützung bei Betroffenenanfragen.
- Vom Restaurant beauftragte Statistiken und Auswertungen, soweit möglich aggregiert oder anonymisiert.

4. Betroffene Personen

- Mitglieder / Endkunden: Personen, die einem Rewards-Programm beitreten, teilnehmen, austreten, gesperrt oder entfernt werden oder Wallet- /Kommunikationsfunktionen nutzen.
- Interessenten / Empfänger: Personen mit dokumentiertem restaurantbezogenem Marketing-Opt-in, gesondertem Geofence-Nachweis oder einem technischen Zustellvorgang.
- Restaurantpersonal: Inhaber, Administratoren, Beschäftigte und sonstige autorisierte Personen mit Dashboard-, Scanner-, Kiosk-, Kampagnen-, Freigabe- oder Supportbezug.
- Sonstige Kontaktpersonen: Vom Restaurant benannte Ansprechpartner für Vertrag, Datenschutz, Support oder Sicherheit.

5. Kategorien personenbezogener Daten

- Stamm- und Kontaktdaten: Name/Anzeigename, E-Mail-Adresse, Telefonnummer, Nutzer- und Mitgliedskennung sowie – soweit vom Mitglied angegeben und für aktivierte Funktionen erforderlich – das vollständige Geburtsdatum. Das vollständige Geburtsdatum kann technisch im restaurantbezogenen Gastprofil gespeichert sein. In den Restaurantansichten werden daraus nur Tag und Monat ausgegeben; das Geburtsjahr und das vollständige Geburtsdatum werden dort nicht angezeigt. Tag und Monat bleiben bei Zuordnung zu einem Mitglied personenbezogene Daten. Zugriff und Verarbeitung des vollständigen Datums sind auf erforderliche interne Funktionen und berechtigte technische Administration beschränkt; eine Nutzung durch das Restaurant zur individuellen Altersauswertung wird nicht beauftragt. Für manuell angelegte Kontakte ohne übernommenes Rewards-Profil kann das Restaurant ein selbst erhobenes vollständiges Geburtsdatum im Gästebuch erfassen und bearbeiten; es muss hierfür die Erforderlichkeit und Rechtsgrundlage gesondert prüfen. Die beschränkte Anzeige übernommener Rewards-Geburtsdaten bleibt bestehen.
- Mitgliedschaft und Status: Restaurant, Standort, Programm, aktiv/gesperrt/ausgetreten/entfernt/inaktiv, Beitritts- und Austrittszeitpunkt, Statusereignisse, Grund, Notiz, handelnde Person und Metadaten.
- Loyalty- und Transaktionsdaten: Punkte/Stempel verdient und eingelöst, aktueller Saldo, Verlauf, Prämien, Gutscheine, Einlösungen, Besuche, Zeitpunkte, Scan-, Freigabe-, Storno- und Korrekturvorgänge sowie der jeweilige Änderungsbetrag (Delta).

- Einwilligungs- und Kampagnendaten: Restaurantbezogenes Marketing-Opt-in/Opt-out, gesonderter Geofence-Nachweis, Text-/Versionsnachweis, Zeitpunkt, Quelle, technischer User-Agent, Zielgruppenzuordnung, Empfänger-Snapshot, Versand-, Fehler-, Bounce-, Abmelde-, Widerrufs- und Einlösestatus sowie technische Push-Berechtigung; keine Öffnungs- oder Klickmessung.
- Geräte-, Push- und Walletdaten: Gerätekennung, Expo-Push-Token, Plattform, Berechtigungsstatus, Aktivierungs-/Deaktivierungszeitpunkt, Wallet-Seriennummer, Pass-/Objekt-ID, Apple-Push-Token, Registrierungs- und Synchronisationsdaten.
- Standort- und Kontextdaten: Kein serverseitiger Verlauf exakter GPS-Koordinaten.

Für Geofence-Auslösung höchstens Nutzer, Restaurant, Kampagne, Zeitpunkt und Ergebnis; zusätzlich restaurantbezogene Standort-, Zeit- und Wetterparameter.

- Technische und Sicherheitsdaten: IP-Adresse, Browser, Betriebssystem, App-Version, Sprache, Zugriffs-, Login-, Session-, Fehler- und Sicherheitsprotokolle, QR-Token/Hash, Rate-Limit- und Missbrauchssignale.
- Personal- und Berechtigungsdaten: 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. Hinzu kommen erforderliche Freigabe-, Änderungs- und Tätigkeitsnachweise.
- Kommunikations- und Supportdaten: Anfragen, Nachrichten, Anhänge und technische Diagnosedaten, soweit zur Bearbeitung 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.

  Reservierungs- und Direktchatnachrichten 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.
- Freitextdaten: Notizen, Tags, Präferenzen oder Korrekturgründe, die das Restaurant eingibt. Besondere Kategorien sind nicht vorgesehen und dürfen nicht zielgerichtet erfasst werden.

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.

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.

Gruppen- und Auswahldaten: manuelle Mitgliedszuordnungen, gespeicherte Smartgruppenregeln und die daraus berechnete Zugehörigkeit; ergänzend Kampagnendesign, Medienadressen, Testempfänger und erforderliche technische KI-Nutzungsdaten.

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht vorgesehen. Das Restaurant darf keine sensiblen Zielgruppen, diskriminierenden Kriterien oder entsprechenden Freitexteingaben verlangen.

6. Rollenabgrenzung nach Funktion

- Programmregeln, Punkte, Stempel, Prämien, Gutscheine: Verantwortlicher – Restaurant; Einordnung – Reservly als Auftragsverarbeiter.
- Restaurantbezogene Mitglieder-, Status- und Mitarbeiterprotokolle: Verantwortlicher – Restaurant; Einordnung – Reservly als Auftragsverarbeiter.
- Restaurantkampagnen und deren Zielgruppen: Verantwortlicher – Restaurant; Einordnung – Reservly als technischer Auftragsverarbeiter.
- Zentrales Reservly-Konto, Login, Kontosicherheit und Alterskontrolle (Kontonutzung grundsätzlich ab 14 Jahren): Verantwortlicher – Reservly; Einordnung – Außerhalb dieses AVV.
- Vom Endkunden gesteuerte zentrale Mitgliedschaftsübersicht: Verantwortlicher – Reservly, soweit Zwecke/Mittel eigenständig festgelegt; Einordnung – Außerhalb dieses AVV; Schnittstelle zum restaurantbezogenen Programm bleibt auftragsbezogen.
- Plattformweite zwingende Sicherheit/Missbrauchsprävention: Verantwortlicher – Reservly, soweit eigenständiger Zweck; Einordnung – Außerhalb dieses AVV; restaurantbezogene Nachweise können zugleich Auftragsdaten sein.
- Gemeinsam bestimmte neue Zwecke/Mittel: Verantwortlicher – Erst nach gesonderter Prüfung; Einordnung – Gegebenenfalls Art.-26-Vereinbarung vor Aktivierung.

7. Löschung / Anonymisierung / Aufbewahrung

- Aktive restaurantbezogene Mitgliedschaft: Für die Dauer der Mitgliedschaft und soweit zur Programmdurchführung erforderlich.
- Gastprofile: 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. Beendete Mitgliedschaften und dazu noch erforderliche Gastprofilbezüge werden nach den gesonderten Mitgliedschaftsfristen grundsätzlich bis zu drei Jahre eingeschränkt aufbewahrt, soweit Nachweise, Missbrauchsabwehr oder Ansprüche dies erfordern.
- Loyalty-Ledger, gewöhnliche Mitgliedskarten-Scans, Gutschein- und Prämieneinlösungen: Bis zu 3 Jahre ab Ereignis, soweit erforderlich und kein längerer gesetzlicher Nachweis nötig ist. Für erfolgreiche Rechnungsscans und deren zugehörige Buchungsnachweise sowie erfolglose Rechnungsscanversuche gelten vorrangig die folgenden besonderen Regeln.
- Erfolgreiche Rechnungsscans: Für einen Scan, der zu einer Punkte- oder Stempelgutschrift führt, ist der reduzierte Nachweis aus Hash und zugehöriger Scan-/Punktebuchung grundsätzlich sieben Jahre ab Ende des maßgeblichen Kalenderjahres aufzubewahren. Soweit die Unterlagen

tatsächlich abgaben- oder rechnungslegungsrechtlich aufbewahrungspflichtig sind, beruht dies auf Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 132 BAO beziehungsweise, soweit anwendbar, § 212 UGB. Eine Punktegutschrift begründet für sich allein keine solche gesetzliche Pflicht. Außerhalb einer gesetzlichen Pflicht setzt die siebenjährige Nachweisaufbewahrung ein dokumentiertes, erforderliches und überwiegendes Interesse an der Nachvollziehbarkeit von Gutschriften und der Bearbeitung von Reklamationen nach Art. 6 Abs. 1 lit. f DSGVO voraus; entfällt die Erforderlichkeit früher, werden die Daten früher gelöscht oder wirksam anonymisiert. Während der Nachweisaufbewahrung ist die Nutzung auf diesen Zweck beschränkt; sie berechtigt nicht zur Werbung oder zu neuen Gastprofilen. Nach Fristablauf erfolgt die automatische Löschung oder wirksame Anonymisierung. Nur für konkrete noch offene Verfahren dürfen die dafür erforderlichen Daten gesondert und zugriffsbeschränkt länger aufbewahrt werden.

- Erfolglose Rechnungsscans: Abgelehnte, ungültige oder abgebrochene Scanversuche ohne Gutschrift werden nicht dauerhaft gespeichert. Soweit für Missbrauchsschutz oder technische Fehleranalyse erforderlich, werden minimale Versuchsmetadaten höchstens 30 Tage ab dem Versuch gespeichert und danach automatisch gelöscht; ohne solchen Bedarf erfolgt keine Speicherung. QR-Rohinhalt und Rechnungsbilder sind auch von diesen Protokollen ausgeschlossen. Die bloße Ablehnung verlängert die Frist nicht. Ein bereits vorhandener Nachweis einer früheren erfolgreichen Gutschrift folgt weiterhin seiner eigenen Frist.
- Umsetzung und Vertragsende: Die besonderen Scanfristen gehen allgemeineren Protokoll-, Konto-, Mitgliedschafts- und Programmfristen vor, soweit die jeweilige Aufbewahrung rechtmäßig erforderlich ist. Erforderliche reduzierte Nachweise sind gegen vorzeitige Löschung durch verknüpfte Datensätze zu schützen. Das Ende des AVV begründet keine eigenmächtige Fortsetzung der Verarbeitung: Nachweise werden nach Wahl und Weisung des Verantwortlichen zurückgegeben oder gelöscht; eine weitere Archivierung im Auftrag setzt eine fortbestehende dokumentierte Vereinbarung voraus. Vor Aktivierung sind Löschläufe, Zugriffsrechte, Backups und das Verwerfen der Rohdaten entsprechend einzurichten und zu prüfen.
- Scanner- und Kiosk-Betriebsprotokolle: Regelmäßig bis zu 90 Tage; für erfolglose Rechnungsscanversuche gilt vorrangig die Höchstfrist von 30 Tagen. QR-Rohdaten und Rechnungsbilder dürfen nicht in Betriebs-, Fehler- oder Sicherheitsprotokollen enthalten sein.
- Geofence-Ereignisse: 30 Tage; keine dauerhafte Speicherung exakter GPS- Verläufe.
- Kampagnen-Zustelldaten: Personenbezogen 12 Monate, danach Löschung oder Anonymisierung, sofern kein konkreter Nachweisfall fortbesteht.
- Einwilligungsnachweise: Für die aktive Nutzung und bis zu 3 Jahre nach Widerruf oder letzter Nutzung, soweit zur Rechtsverteidigung erforderlich.
- Technische, Fehler- und Sicherheitsprotokolle: Regelmäßig 30 bis 90 Tage; im Sicherheitsfall eingeschränkt bis zum Abschluss der Untersuchung und zulässiger Nachweisfristen.

  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.

- Wallet- und Push-Daten: Solange Gerät/Pass aktiv oder die Mitgliedschaft besteht; danach Deaktivierung und Löschung im regulären Bereinigungszyklus.
- Geburtstagsdaten: Bis Löschung des Kontos bzw. Gastprofils, Deaktivierung der Funktion oder Wegfall des Verarbeitungszwecks; im restaurantbezogenen Gastprofil nach den hierfür geltenden Mitgliedschafts- und Gastprofilfristen.
- Gesperrte Mitgliedschaft: Bis zu 3 Jahre; anschließend Überführung in den Status entfernt nach dokumentierter Prüfung, wobei ein minimaler Entfernt-/Sperrnachweis bis zu weiteren 3 Jahren fortbestehen kann, wenn dies zur Missbrauchsabwehr erforderlich ist.
- Abrechnungs- und steuerrelevante Daten: Bis zu 7 Jahre oder nach der jeweils zwingenden gesetzlichen Frist; Zugriff auf den gesetzlichen Zweck beschränkt.
- Kontolöschung: Reservly-eigene Kontodaten grundsätzlich binnen 30 Tagen; Auftragsdaten werden entsprechend Mitgliedschafts-, Nachweis- und gesetzlichen Fristen behandelt.
- Programmende: Während einer vorgesehenen 90-tägigen Abwicklungsphase; danach Löschung, Anonymisierung oder zulässige eingeschränkte Aufbewahrung gemäß dieser Matrix.

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.

KI-Verarbeitung: Der Gesprächsverlauf verbleibt während der Bearbeitung im Browserzustand; übernommene Ergebnisse werden als Kampagneninhalt gespeichert. Für Kontingentkontrolle und Fehlerklärung werden Restaurant-, Kampagnen-, Benutzer- und Anfragekennung, Zeitpunkte, Modell- und Promptversion, Tokenverbrauch, Kostenwerte, Status und Anbieter-Antwortkennung gespeichert, nicht die Prompt- oder Antworttexte in dieser Nutzungsbuchung. Die deaktivierte Speicherung von API-Antworten (store: false) schließt anbieterseitige Sicherheitsprotokolle und zeitweilige technische Zwischenspeicherung nicht aus. Nach den Anbieterangaben können Sicherheitsprotokolle grundsätzlich bis zu 30 Tage, bei gesetzlichen Pflichten oder notwendiger Gefahrenabwehr auch länger, sowie modellabhängige Prompt-Zwischenspeicher bis zu 24 Stunden bestehen. API-Inhalte werden standardmäßig nicht zum Modelltraining genutzt; eine Freigabe von Auftragsdaten zum Training ist nicht beauftragt. Für erforderliche eigene Nutzungsnachweise gilt eine zweckgebundene Aufbewahrung; spätestens nach Abschluss der Abrechnung und einer

erforderlichen Nachweisfrist von grundsätzlich bis zu drei Jahren sind personenbeziehbare Nutzungsbuchungen zu löschen oder zu anonymisieren, sofern keine konkrete gesetzliche Pflicht oder ein offener Nachweisfall entgegensteht. KI-Anhänge werden für die konkrete Anfrage übertragen und nicht als eigene dauerhafte Dateien bei Reservly gespeichert. Ein technischer Reparaturversuch kann dieselben Anhänge erneut übermitteln. Im weiteren Gespräch können Dateinamen und bereits erzeugte Antworten fortbestehen; übernommene Inhalte bleiben im Kampagnenentwurf. Die abgeschaltete Speicherung eines abrufbaren API-Antwortverlaufs bedeutet keine vollständige Speicherfreiheit beim Anbieter. Für Bilder und Dateien gelten auch dessen Sicherheitsprüfungen; auffällige Bilder können zur manuellen Sicherheitsprüfung zurückbehalten werden.

8. Verarbeitungshäufigkeit, Datenquellen und Kontakt

Die Verarbeitung erfolgt fortlaufend oder ereignisbezogen während der Nutzung. Daten stammen von Mitgliedern, vom Restaurant und seinem Personal, aus dem zentralen Reservly-Konto, aus Scanner-, Kiosk-, Wallet- und Push-Schnittstellen sowie aus technisch erzeugten Protokollen. Wetterdaten werden ohne Übermittlung personenbezogener Kundendaten abgefragt; Geofence-Ergebnisse werden auf den erforderlichen Ereignisnachweis reduziert.

Die Datenquellen umfassen ergänzend die manuellen Eingaben und Dateien berechtigter Restaurantnutzer sowie rechtmäßig verknüpfte Reservierungs- und Rewards-Daten desselben Restaurants. Es werden keine Gästedaten anderer Restaurants zur Zielgruppenbildung herangezogen. Weitere Quellen sind vom Restaurant rechtmäßig geführte CSV-Kontaktlisten.

Weisungen erfolgen über AVV/Hauptvertrag, Dashboard-Einstellungen und Textform. Kontakt für Datenschutz/AVV, Support sowie Security/Incidents: support@reservly.at

9. Ergänzung zur Verarbeitung von Freundeseinladungen

Die Beschreibung dieser Anlage umfasst auch die vom Restaurant aktivierte Funktion „Freunde einladen“. Betroffen sind einladende Mitglieder, Personen, die über einen Einladungslink beitreten, sowie berechtigte Restaurantnutzer bei der Konfiguration der Aktion. Nicht teilnehmende Freunde werden nicht durch einen Adressbuchimport erfasst.

Art und Zweck der Verarbeitung: Erzeugen und Zuordnen persönlicher Einladungslinks, Prüfen der Teilnahmevoraussetzungen und Limits, Zuordnen der neu beigetretenen Person zum einladenden Mitglied, Erfassen des Beitritts und der qualifizierenden Besuchsvergabe, Berechnen und Ausgeben der Bonuspunkte/-stempel oder Gutscheine, Anzeigen der Einladungsübersicht sowie Bearbeiten erforderlicher Nachweis- und Missbrauchsfälle.

Datenkategorien: Restaurant- und Programmkennung, Einladungskennung und -code, Nutzer- und Mitgliedschaftskennungen beider Beteiligten, Vorname aus dem Profilnamen für die Übersicht, Status, Annahme- und Belohnungszeitpunkt, festgehaltene Angebotsbedingungen (Auslöser, Art, Empfänger, Höhe und gegebenenfalls Gutscheinlaufzeit), Verknüpfungen zu Bonusbuchungen und Gutscheinen sowie die zur Auslösung erforderliche Besuchsvergabe. Die für den Beitritt ohnehin erforderlichen Konto-, Profil- und Teilnahme-/Einwilligungsnachweise bleiben nach den übrigen Regelungen verarbeitet.

Rollen und Offenlegung: Das Restaurant bestimmt die Empfehlungsaktion und ist für deren Programmdaten verantwortlich; Reservly verarbeitet sie insoweit im Auftrag. Die einladende Person erhält in ihrer eigenen Übersicht ausschließlich Vorname, Annahmedatum und Annahme-/Belohnungsstatus der ihr zugeordneten Einladungen. Beim Besuchsauslöser kann daraus die erfolgte erste qualifizierende Vergabe erkennbar sein. Ein Zugriff auf fremde Kontakt-, Kauf- oder Besuchsdetails wird dadurch nicht eingeräumt. Zentrales Konto und eigenständige Plattform-Sicherheitszwecke bleiben nach Ziffer 6 abgegrenzt.

Datenquellen sind die Eingaben der Beteiligten, das bestehende Profil, die vom Restaurant eingestellte Aktion und die systemseitig erfasste Teilnahme und Bonusvergabe. Die lokale Zwischenspeicherung eines begonnenen Einladungsbeitritts dient der Fortsetzung des Vorgangs.

Beim Teilen wählt das Mitglied einen externen Kommunikationsdienst selbst; dieser wird nicht allein dadurch zum Unterauftragsverarbeiter des Restaurants. Es wird keine automatische Einladung an von Reservly ausgewählte Freunde versandt.

Speicherkriterien ergänzend zu Ziffer 7: Der persönliche Code wird für die aktive Einladungsfunktion vorgehalten. Angenommene Einladungen und Zuordnungen werden für offene Bonusansprüche sowie das mitgliedschaftsbezogene Einladungslimit benötigt. Nach Wegfall dieser Zwecke werden nur erforderliche Bonus- und Missbrauchsnachweise eingeschränkt aufbewahrt, grundsätzlich höchstens drei Jahre ab Erledigung der Einladung beziehungsweise Ende des noch erforderlichen Mitgliedschaftsbezugs. Ohne weiteren Nachweisbedarf ist früher zu löschen oder wirksam zu anonymisieren. Bei konkreten offenen Ansprüchen oder zwingenden gesetzlichen Pflichten gelten nur die dafür erforderlichen längeren Fristen und Zugriffsbeschränkungen. Verknüpfte Codes, Beteiligtenkennungen und Bonusdaten sind in den Löschprozess einzubeziehen.

10. Angebotsreservierungen

Bei einer Angebotsreservierung werden Angebots-, Restaurant-, Nutzer-, Mitgliedschafts- und Gutscheinzuordnung, zugeteilte Kontingenteinheit, Status sowie Reservierungs-, Rückgabe-, Einlöse- und Ablaufzeitpunkte verarbeitet. Dies dient der Zuteilung begrenzter Vorteile, der Prüfung von Kontingent und Mehrfachbeanspruchung, der Rückgabe, Einlösung und Bearbeitung von Ansprüchen. Das jeweilige Restaurant ist hierfür Verantwortlicher; Reservly verarbeitet die Programmdaten in dessen Auftrag. Andere Mitglieder sehen keine personenbezogene Liste der Reservierenden. Für die gewünschte Teilnahme und Abwicklung ist Art. 6 Abs. 1 lit. b DSGVO maßgeblich; erforderliche Missbrauchs- und Anspruchsnachweise beruhen auf Art. 6 Abs. 1 lit. f DSGVO mit dem Interesse an einer ordnungsgemäßen und überprüfbaren Abwicklung.

Personenbeziehbare Angebotszuteilungen werden bis zur Einlösung, wirksamen Rückgabe oder zum Ablauf und zur Erledigung offener Ansprüche benötigt. Danach werden nur erforderliche Nachweise zugriffsbeschränkt für höchstens drei Jahre ab Erledigung aufbewahrt; ohne Nachweisbedarf erfolgt die Löschung oder wirksame Anonymisierung früher. Konkrete offene Rechtsstreitigkeiten oder zwingende gesetzliche Pflichten können eine längere zweckgebundene Aufbewahrung erfordern. Die Löschung muss auch Zuordnungen zwischen Angebot, Zuteilung, Mitgliedschaft und Gutschein erfassen; das Entfernen des Namens aus einem Gutschein allein genügt nicht.

11. Ergänzende Weisungen zur Datenminimierung

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.

Der Marketingwiderruf beendet die werbliche Verwendung von Tag und Monat. Eine für Konto-, Alterskontrolle oder erforderliche Anspruchsnachweise noch zulässige interne Verarbeitung wird dadurch nicht zu einer Werbeverarbeitung. Das Restaurant erteilt keine Weisung zur werblichen Verwendung nach Widerruf.

Vor einer Entfernung nach Ablauf einer Sperre prüft das Restaurant, ob Grund, Dauer und Folgen weiterhin verhältnismäßig sind. Ein technischer Statuswechsel ersetzt diese Prüfung nicht. Minimalnachweise dürfen nur solange bestehen, wie der konkrete Nachweis- oder Missbrauchsschutzzweck dies erfordert.

12. Aktionscodes und einmalige Geräteboni

Für restaurantbezogene Aktionscodes werden Kampagnen-, Code-, Programm- und Mitgliedschaftszuordnung, ein geschützter Codewert, Gültigkeits- und Nutzungslimits, Beanspruchungszeitpunkte sowie zugeordnete Bonus- und Gutscheinbuchungen verarbeitet. Für einmalige Startvorteile können Gerätekennungen in einen kryptografisch geschützten Vergleichswert umgewandelt und mit Programm, Bonustyp, Schlüsselversion, Beanspruchungszeitpunkt und gegebenenfalls Mitgliedschaft gespeichert werden. Der Vergleichswert bleibt personenbezogen beziehungsweise personenbeziehbar; er ist keine Anonymisierung.

Restaurantbezogene Bonusabwicklung erfolgt im Auftrag. Soweit Reservly eine davon abgegrenzte zwingende Plattform-Sicherheitsverarbeitung für eigene Zwecke vornimmt, gelten die Verantwortlichkeitsregeln in Ziffer 4 und die Datenschutzerklärung. Ein gerätebezogener Treffer darf bei gemeinsam genutzten Geräten nicht ohne Prüfung als persönlicher Missbrauchsnachweis behandelt werden. Erforderliche Vergleichswerte werden nur für die Dauer der tatsächlich noch zu prüfenden einmaligen Berechtigung aufbewahrt, mindestens jährlich auf Erforderlichkeit geprüft und bei Zweckfortfall gelöscht. Erledigte einzelne Anspruchsnachweise werden grundsätzlich höchstens drei Jahre zugriffsbeschränkt gespeichert, soweit erforderlich. Eine unbefristete Speicherung allein wegen technischer Verfügbarkeit ist nicht beauftragt.

13. Optionale KI-Unterstützung für Kampagnen

Bei einer KI-Anfrage werden die Eingabe, das aktuelle E-Mail-Design einschließlich Texten, Bildadressen und Gutscheinentwurf, bis zu sechs vorangegangene Gesprächsrunden sowie ausgewählte Restaurant- und Kampagneninformationen an OpenAI übermittelt. Zum Kontext gehören insbesondere Restaurantkontakt und -adresse, sichtbare Speisekarteninhalte, Öffnungs- und Schließzeiten, Programmeinstellungen, Kampagnennotizen, Zielgruppennamen und Filterbeschreibungen sowie Betreff und Vorschautext ausgewählter früherer Kampagnen. Gästelisten, einzelne Gastprofile, Notizdateien und individuelle Besuchs- oder Kontaktdaten werden nicht automatisch als Gästedatensätze geladen. Personenbezug kann dennoch durch Freitexte, Gruppennamen, Filterwerte oder Kampagneninhalte entstehen; eine automatische Anonymisierung dieser Inhalte findet nicht statt.

Zusätzlich kann der Restaurantnutzer bewusst ausgewählte Bilder, Dokumente und Tabellen an eine KI-Anfrage anhängen. Deren Inhalt, Dateityp und gegebenenfalls Dateiname werden an OpenAI übermittelt; auch enthaltene personenbezogene Angaben oder Metadaten können mitübermittelt werden. Die Auswahl lädt keine Dateien automatisch aus dem Gästebuch nach. Vor dem Absenden sind nicht erforderliche Personenangaben und vertrauliche oder besonders geschützte Inhalte auch aus Dateien und Metadaten zu entfernen; eine automatische Anonymisierung wird nicht vorgenommen.

Die Verarbeitung dient ausschließlich der angeforderten Erstellung oder Bearbeitung des Entwurfs. Betroffen können Restaurantnutzer, Ansprechpartner und in rechtmäßig übermittelten Inhalten genannte Personen sein. Reservly veranlasst keine eigene Nutzung dieser Auftragsinhalte für Modelltraining. Gästeeinzeldaten und sensible Inhalte dürfen nicht allein wegen ihrer technischen Eingabemöglichkeit übermittelt werden. Vor Einsatz gelten die Anbieter-, Informations- und Drittlandvoraussetzungen nach Ziffern 14 und 15.

Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)

1. Ziel und Schutzniveau

Reservly setzt technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau nach Art. 32 DSGVO sicherzustellen. Sie gewährleisten insbesondere Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, Wiederherstellbarkeit sowie die regelmäßige Prüfung der Wirksamkeit. Gleichwertige oder bessere Maßnahmen dürfen die beschriebenen Maßnahmen ersetzen.

2. Organisation, Rollen und Verantwortlichkeiten

- Festgelegte Verantwortlichkeiten für Datenschutz, Informationssicherheit, Betrieb und Vorfallbehandlung; dokumentierte Vertraulichkeitsverpflichtungen.
- Regelmäßige Sensibilisierung und bedarfsbezogene Schulungen; Zugriff auf Produktionssysteme nur für autorisierte Personen.
- Dokumentierte Prozesse für Berechtigungen, Änderungen, Support, Sicherheitsvorfälle, Betroffenenrechte, Aufbewahrung und Löschung.
- Auswahl und regelmäßige Überprüfung von Unterauftragsverarbeitern anhand von Sicherheit, Vertragslage und Verarbeitungsort.

3. Zutritts- und Systemzugangskontrolle

- Betrieb in professionell gesicherten Rechenzentren der Infrastrukturprovider; kein eigener frei zugänglicher Serverbetrieb in Restaurantstandorten.
- Authentifizierung über zentralen Authentifizierungsdienst, sichere Sitzungen, rollenbasierte Zugriffe und Schutz administrativer Funktionen.
- Geheimnisse, API-Schlüssel und Service-Rollen werden außerhalb des Quellcodes in geschützten Umgebungs- bzw. Secret-Systemen verwaltet und bei Bedarf rotiert.
- Rate-Limiting und Wiederholungsschutz für ausgewählte Vorgänge, insbesondere Passwort-Reset, erneute Bestätigungsmails und einzelne externe Provider- bzw. öffentliche Schnittstellen; weitere Vorgänge werden durch Authentifizierung, Sitzungsprüfung, Datenbankregeln und atomare Transaktionen geschützt.

4. Zugriffs-, Berechtigungs- und Mandantentrennung

- Mandantenbezogene Datenmodelle mit Restaurant- und Standortzuordnung; serverseitige Autorisierungsprüfungen vor Zugriff oder Änderung.
- Row Level Security und ergänzende serverseitige Autorisierungsprüfungen sichern die Mandantentrennung. Inhaberzugriff und einzelne Teamrechte werden unterschieden. Die Standortzuordnung eines Teamprofils ist eine organisatorische beziehungsweise statistische Zuordnung und keine gesonderte technische Standort-Zugriffsgrenze.
- Administrative Service-Rollen werden nur serverseitig und für definierte Funktionen verwendet; Client-Anwendungen erhalten keine unbeschränkten Schlüssel.
- Rollen und einzelne Rechte für Team, Gäste, Exporte, Marketing und Administration; individuelle Zugänge, persönliche Teamcodes und gemeinsame Admin-PIN gemäß Ziffer 6. Gemeinsame PIN-Freigaben erlauben nicht stets eine Zuordnung zur tatsächlich handelnden natürlichen Person.

5. Übertragungs- und Speicherschutz

- Verschlüsselte Übertragung über TLS/HTTPS für Web-, App-, API- und Provider-Kommunikation.
- Verschlüsselung ruhender Daten nach den Sicherheitsmechanismen der eingesetzten Infrastrukturprovider; Zugriffsbeschränkung auf Datenbanken und Speicher.
- Mitgliedschafts-QR- und Realtime-Sitzungstokens werden zufällig, gehasht oder zeitlich bzw. kontextuell begrenzt eingesetzt. Die optionale vierstellige Admin-PIN ist davon getrennt und nur im zugriffsbeschränkten Restaurantkontext vorgesehen. Persönliche vierstellige Teamcodes werden in geschützter Prüfform gespeichert und bei Entzug der Berechtigung deaktiviert; sie dürfen nicht in Protokollen erscheinen.
- Push-, Wallet- und Providerkennungen werden ausschließlich für die jeweilige technische Zustellung bzw. Aktualisierung verwendet.

6. Eingabe-, Änderungs- und Nachvollziehbarkeitskontrolle

- Protokollierung wesentlicher Mitgliedschafts-, Scan-, Einlöse-, Freigabe-, Sperr- und Korrekturereignisse mit Zeit, handelnder Restaurantbenutzer-ID und verfügbarem Kontext; ein gesonderter Rollensnapshot wird nicht für jedes Ereignis gespeichert.
- Manuelle Punkteänderungen enthalten Änderungsbetrag (Delta), Grund, Zeitstempel und handelnde Restaurantbenutzer-ID; der aktuelle Saldo wird in der Mitgliedschaft geführt.
- Restaurantbezogenes Marketing-Opt-in und gesondertes Geofence-Marketing werden protokolliert; Öffnungs- und Klicktracking ist für diese beauftragten Kampagnen nicht zulässig und muss deaktiviert bleiben.
- Änderungen an Datenbank und Anwendung werden versioniert, geprüft und kontrolliert ausgerollt; Produktions- und Entwicklungsumgebungen werden getrennt behandelt.

Ergänzende Maßnahmen für Gästebuch und KI: Notizdateien werden in privatem Objektspeicher abgelegt und nach Restaurantprüfung über befristete signierte Links bereitgestellt; Nicht-Bilder werden als Download ausgeliefert. Kampagnenbilder und Tablet-Videos sind hiervon getrennte, öffentlich abrufbare Medien. KI-Aufrufe werden serverseitig autorisiert, auf ausgewählte Kontextdaten begrenzt und die Ausgaben strukturell geprüft; diese Prüfung ersetzt keine Inhaltskontrolle oder Anonymisierung durch den Verantwortlichen. Bei CSV-Transfer sind Restaurantberechtigung und Datenumfang zu prüfen. KI-Dateien werden auf zulässigen Typ und Umfang geprüft; diese technische Prüfung anonymisiert keine Inhalte.

7. Verfügbarkeit, Wiederherstellung und Belastbarkeit

- Redundante Cloud-Infrastruktur und von den Providern bereitgestellte Sicherungs- und Wiederherstellungsmechanismen; regelmäßige Überprüfung kritischer Wiederanlaufpfade.
- Überwachung technischer Fehler, API-Ausfälle, Zustellprobleme und ungewöhnlicher Nutzung; definierte Eskalation bei sicherheitsrelevanten Ereignissen.
- Daten in Backups bleiben während des Backup-Zyklus geschützt und werden mit der regulären Rotation überschrieben; operative Wiederverwendung ist auf Wiederherstellung beschränkt.
- Fail-safe Behandlung fehlerhafter Zustellungen und Synchronisation; wiederholbare Transaktionen und Schutz vor unbeabsichtigter Doppelvergabe, soweit technisch vorgesehen.

8. Datenminimierung und Löschung

- Erhebung und Anzeige nur der für die jeweilige Funktion erforderlichen Daten; Restaurantzugriff grundsätzlich nur auf eigene Mitglieder und Programme.
- Keine serverseitige Speicherung exakter GPS-Verläufe; Geofence-Daten werden auf Ereignis und Ergebnis reduziert und nach 30 Tagen gelöscht.
- Technisch bereitgestellte Lösch- und Anonymisierungsfunktionen für Kontolöschung, inaktive Mitgliedschaften, Gastprofile, Einwilligungs-, Kampagnen-, Geräte-, Ledger- und Protokolldaten; Ausführung über einen authentifizierten betrieblichen Löschlauf. Dies umfasst auch technische E-Mail-Bestände, einschlägige Providerdaten und Teamdaten nach Anlage 1; ausgeführte Bereinigungen und Fehler werden nachvollziehbar kontrolliert.
- Anonymisierung aggregierter Statistiken, wenn ein Personenbezug nicht mehr erforderlich ist.

9. App-, Scanner-, Kiosk- und Gerätesicherheit

- Trennung von Endkunden-App, Restaurant-Dashboard und Scanner- /Kioskfunktionen mit funktionsbezogenen Berechtigungen.
- Geräte- und Pushregistrierungen werden eindeutig zugeordnet und können deaktiviert oder widerrufen werden; Berechtigungsstatus wird beachtet.

- Kiosk- und Scannerprotokolle werden zeitlich begrenzt; sensible Administrationsfunktionen erfordern erhöhte Berechtigung bzw. geschützte PIN-/Code-Prüfung.
- Das Restaurant schützt physische Geräte, Bildschirmsperren, lokale Konten und Netzwerke und meldet Verlust oder Kompromittierung unverzüglich.

10. Kampagnen-, Einwilligungs- und Profilingschutz

- Werbliche Gruppierung und Versand sind auf das ausgewählte Restaurant und den nachgewiesenen Kanal-, Zweck- und Datenumfang zu begrenzen. Ein allgemeiner Marketingstatus allein belegt keine Einwilligung in jede Datenquelle. Abmeldungen und Widerrufe sind auch für vorbereitete Kampagnen umzusetzen.
- Keine Öffnungs- oder Klickmessung; Speicherung nur technischer Zustell-, Fehler-, Bounce-, Abmelde- und Einlösedaten.
- Sperre oder Einschränkung offensichtlich rechtswidriger, sensibler, diskriminierender oder missbräuchlicher Zielgruppen und Inhalte.
- Keine ausschließlich automatisierte Entscheidung mit rechtlicher oder ähnlich erheblicher Wirkung; zufällige Minigame-Ergebnisse dienen nur der vom Restaurant festgelegten Bonusvergabe.

11. Prüfung, Bewertung und Verbesserung

- Regelmäßige Überprüfung der Wirksamkeit wesentlicher Maßnahmen, insbesondere Authentifizierung, Autorisierung, Mandantentrennung, Löschprozesse und Vorfallbehandlung.
- Sicherheitsupdates und Abhängigkeitsaktualisierungen nach Risiko und Verfügbarkeit; Behandlung bekannt gewordener Schwachstellen nach Priorität.
- Dokumentation wesentlicher Änderungen, Vorfälle und Korrekturmaßnahmen; Anpassung des Sicherheitsniveaus bei neuen Funktionen oder veränderter Risikolage.

Anlage 3 – Unterauftragsverarbeiter

Die Liste gibt den für Reservly Rewards vorgesehenen technischen Stand wieder. Dienste werden nur eingesetzt, soweit die jeweilige Funktion aktiviert und die erforderliche Anbietervereinbarung abgeschlossen ist.

Unterauftragsverarbeiter	Leistung / Rolle	Ort/Region / Drittlandhinweis
Supabase, Inc. / vertraglich zuständige Supabase-Einheit	Datenbank, Authentifizierung, Realtime, Objektspeicher und Backend-Funktionen	EU-Region, derzeit Frankfurt (AWS eu-central-1), soweit konfiguriert. AVV/DPA; bei Drittlandzugriff DPF und/oder SCC samt Zusatzmaßnahmen.
Vercel Inc.	Hosting, API-Ausführung, Deployment, CDN/Edge und technische Protokolle	EU und globale Infrastruktur; möglicher Zugriff/Verarbeitung in den USA. DPA; DPF und/oder SCC samt Zusatzmaßnahmen.
Resend / Plus Five Five, Inc., USA	Transaktionale und vom Restaurant zulässig beauftragte E-Mail-Zustellung; Kontaktangaben, Inhalte, technische Versand-, Zustell- und Sperrdaten	USA; DPA und EU-Standardvertragsklauseln Modul 3 für Unterauftragsverarbeitung sowie erforderliche Zusatzmaßnahmen. Eigene Anbieterzwecke nach Ziffer 15 gesondert; keine pauschale EU-Speicherung.
Upstash, Inc.	Redis-basierte Rate-Limits, Kontingente und kurzlebige technische Zustände	EU-Region, derzeit Frankfurt, soweit konfiguriert; möglicher US-Bezug. DPA; DPF und/oder SCC samt Zusatzmaßnahmen.
650 Industries, Inc. (Expo)	Technische Zustellung mobiler Push-Nachrichten über den Expo Push Service	USA / globale Push-Infrastruktur. DPA bzw. geeignete vertragliche Einbindung; DPF und/oder SCC samt Zusatzmaßnahmen.

OpenAI Ireland Ltd. (EWR-Vertragspartner; gegebenenfalls mit OpenAI OpCo, LLC und weiteren Unterauftragnehmern) – optionale Kampagnen-KI über die API. Daten: Eingaben, Entwürfe, begrenzter Gesprächsverlauf, Restaurant- und Kampagnenkontext nach Anlage 1. Rolle:

Unterauftragsverarbeiter für im Auftrag übermittelte personenbezogene Inhalte. Verarbeitung und Zugriffe können auch außerhalb des EWR, insbesondere in den USA, stattfinden; eine ausschließliche EU-Verarbeitung wird nicht zugesagt. Vor Einsatz sind der konkrete Anbieter-Vertrag, DPA, Verarbeitungsorte, Aufbewahrungseinstellungen und die einschlägigen Garantien nach Art. 44 ff. DSGVO zu dokumentieren. Die Informations- und Widerspruchsfrist nach Ziffer 14 bleibt einzuhalten. Die übermittelten Inhalte umfassen auch die vom Nutzer bewusst ausgewählten KI-Anhänge und erforderlichen Dateimetadaten nach Anlage 1 Ziffer 13.

Optionale Plattform- und Empfängerdienste

Die folgenden Dienste sind nicht in jedem Fall Unterauftragsverarbeiter des Restaurants. Ihre Rolle hängt von der konkreten Aktivierung, der Auswahl durch den Endkunden und der tatsächlichen Datenübermittlung ab:

- Apple Inc. / Apple-Konzerngesellschaften: Apple Wallet, Apple Push Notification Service und optional Apple-Anmeldung. Nutzergewählter Wallet-/Kontodienst; technische Pass-Updates können einen auftragsbezogenen Anteil haben.
- Google LLC / Google-Konzerngesellschaften: Google Wallet, optional Google-Anmeldung, Google Places zur Geokodierung und eingebettete Google-Maps-Karten. Wallet und Anmeldung sind nutzergewählte Dienste; bei Places- und Kartenabrufen können Restaurant-/Standortangaben sowie technische Verbindungsdaten übermittelt werden.
- Open-Meteo: Wetterdaten für wetterbezogene Automationen. Es werden nach aktuellem Design keine personenbezogenen Kundendaten übermittelt; Anfrage bezieht sich auf Ort/Wetter.
- OpenStreetMap/Nominatim und CARTO: Geokodierung und Kartendarstellung im Restaurant-Dashboard. Primär Restaurant-/Standortdaten; bei direktem Browserabruf können technische Verbindungsdaten des Restaurantnutzers anfallen.
- Cloudflare, Inc. / Cloudflare-Konzerngesellschaften: Optionaler Objektspeicher und Auslieferung von Restaurant- bzw. Menümedien über Cloudflare R2. Soweit die Medienfunktion im Loyalty-Angebot verwendet wird; bei direktem Abruf können technische Verbindungsdaten anfallen. Die Cloudflare-R2-Medienfunktion umfasst auch das optionale Startbildschirmvideo am Loyalty-Tablet; dessen Abruf kann technische Verbindungsdaten erzeugen. Vertrauliche Gästedaten dürfen nicht als öffentliches Video bereitgestellt werden.

Änderungen und Widerspruch: Es gilt Ziffer 14 mit aktiver Mitteilung, mindestens 14 Tagen Vorlauf und Widerspruchsmöglichkeit. Die aktuelle Liste bleibt im Dashboard oder auf einer mitgeteilten Datenschutzseite zugänglich. Verspätete Anbieterinformationen verkürzen den zugesagten Vorlauf 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.