Data processing agreement (DPA)

2026-11-12-r2-EN

Partner means the business identified in the signed Agreement or accepted self-service order. The same DPA applies to all three contracting routes for entrusted personal data.

1 Parties, scope and instructions

The Partner is controller and RESTOBOT Yaroslav Baran is processor for personal data entrusted to operate the Partner's venue services. Processing comprises collection, recording, storage, organisation, retrieval, transmission to authorised recipients, correction, restriction, return and deletion for orders, delivery coordination, reservations, payments, loyalty, authorised messages, support and venue reporting. It lasts for the service term and the controlled return/deletion period. The Agreement, enabled lawful configurations and subsequent written or recorded electronic instructions constitute the documented instructions, including for transfers.

RESTOBOT processes entrusted data only on those instructions unless EU or Member-State law requires otherwise; in that case it informs the Partner of the requirement before processing unless the law prohibits this. RESTOBOT immediately informs the Partner if an instruction infringes applicable data-protection law and suspends the affected instruction while the parties resolve it. RESTOBOT does not sell entrusted data or independently use it for advertising.

2 People and data categories

Data subjects: guests/customers, reservation and waitlist participants, loyalty members, persons placing or receiving orders, and Partner personnel whose details are entrusted for venue operations. Independent worker profiles and RESTOBOT's own business-contact processing are outside this processor scope to the extent RESTOBOT determines their purposes.

- Identity/contact and delivery data: names, email, telephone, delivery address and necessary delivery instructions; Telegram identifiers and relevant profile information where that channel is used.

- Orders and loyalty: purchased items, amounts, discounts, transaction and refund history, loyalty identifiers, balances, stamps, rewards and relevant communication history.

- Reservations: venue/location, date, time, time zone, party size, duration, notes, waitlist, cancellations, attendance and no-show history; status changes, timestamps, reasons, relevant actor identifiers, venue-specific allow/block entries and their review history where recorded.

- Payment metadata: provider/account identifiers, Customer ID, PaymentMethod ID or equivalent token, PaymentIntent/SetupIntent identifiers, amounts, currency, payment/charge/refund/dispute status and reconciliation references. These linked tokens are personal data; RESTOBOT does not store full card numbers or CVC for these integrations.

- Authorisation and security evidence: payment-authorisation text/version, acceptance time, IP address where recorded, necessary technical logs and access/change records. The authorisation is limited to its stated payment purpose.

The service does not require special-category or criminal-conviction data. The Partner must avoid entering such data in free text; any necessary exceptional processing requires a separately established legal basis, instructions and appropriate safeguards. Dietary notes can reveal health or religious information and must be minimised.

3 Controller duties and assistance

The Partner determines lawful purposes, legal bases, notices, permitted recipients and proportionate retention instructions; provides Articles 13/14 information; verifies payment authority; and handles data-subject requests. Starting a bot, making a reservation or accepting service terms is not automatically marketing consent. The Partner assesses legitimate interests for no-show records and any automated decisions, and conducts a DPIA where required.

RESTOBOT assists with rights requests, security, breach notifications, DPIAs and prior consultation under Articles 32-36, taking account of the processing and available information. It promptly forwards requests and does not independently reject them on the Partner's behalf. Both parties cooperate so the controller can meet statutory deadlines. Additional charges must not prevent mandatory assistance.

4 Confidentiality, security and assurance

Access is limited to authorised persons bound by confidentiality. RESTOBOT must implement and maintain risk-appropriate Article 32 measures, including access separation between venues, least privilege, secure transport, appropriate protection of stored data and tokens, backup/restoration, vulnerability management, incident handling and periodic effectiveness testing. The specific implemented measures and relevant exceptions must be documented and supplied to the Partner before processing; these obligations are subject to verification under this DPA.

RESTOBOT supplies information needed to demonstrate compliance and permits audits and inspections by the Partner or its mandated auditor. Reasonable scheduling, confidentiality and proportionate costs must not frustrate an urgent incident investigation, a supervisory authority or a statutory audit right.

5 Providers, subprocessors and transfers

The initial list of actual subprocessors must be supplied to and approved by the Partner before their processing begins. It must identify the contracting legal entity, service, data categories, processing/access countries and transfer safeguard. A vendor logo, brand or an 'EEA' label alone is insufficient. Provider roles are determined by their actual functions and agreements.

General authorisation for subsequent additions or replacements is conditional on at least 30 days' advance notice with the above information and a meaningful opportunity to object on data-protection grounds before access begins. If no safe alternative resolves an objection, the affected service may be ended without an early-termination penalty and unused prepaid fees for it are returned. RESTOBOT imposes equivalent Article 28 obligations on subprocessors and remains responsible for their performance.

Stripe or another payment provider may be an independent controller for regulated payment, fraud-prevention and identity-verification purposes. Telegram and other independently selected channels may have their own controller purposes. Roles are assessed by function and the actual contracts; no provider is automatically a processor for all activities. The Partner's own direct provider contracts are distinguished from RESTOBOT's subprocessing.

Transfers, including access from outside the EEA, require documented instructions and a valid GDPR Chapter V mechanism. Where standard contractual clauses are used, the parties assess the transfer circumstances and any needed supplementary measures. Copies or a meaningful description of the safeguards must be available. Processing locations and applicable transfer mechanisms are specified in the provider register supplied to the Partner.

6 Breaches

RESTOBOT notifies the Partner without undue delay after becoming aware of a personal-data breach, with an operational target of an initial notice within 24 hours. It must not wait to complete an investigation or use the controller's 72-hour regulatory deadline as its own waiting period. The notice contains known facts about the nature and scope, affected people/data, contact point, likely consequences and measures, with prompt phased updates when necessary. RESTOBOT preserves relevant evidence and assists the Partner's legally required notifications; the Partner makes its own controller notification decisions.

7 Retention, return and deletion

The Partner's documented schedule must set review/deletion triggers for each category, including no-show records, block-list entries, payment tokens, authorisation evidence and backups. Tokenisation does not make indefinite retention lawful. RESTOBOT must support deletion or disabling of saved-payment credentials when their authorised purpose ends, coordinated with the provider, while segregating only evidence still needed for a documented lawful claim or obligation. A controller instruction does not override the provider's separate statutory retention duties.

After the processing services end, RESTOBOT, at the Partner’s choice, returns or deletes all entrusted personal data and deletes existing copies under GDPR Article 28(3)(g). The exception covers only data whose storage is required by EU or Member-State law applicable to RESTOBOT. Only the legally required scope is retained for the required period, with purpose and access restrictions. A requirement to retain accounting documents does not justify retaining the entire guest database. When the storage obligation ends, the data are deleted. Return, deletion and treatment of backups take place without undue delay under a documented procedure; a technical schedule does not authorise indefinite retention. Completion is documented to the Partner, and protection duties continue until processing ends.

8 Independent purposes and priority

RESTOBOT separately determines necessary processing for its own billing, business contacts, account security and independent worker/tipping services as described in the applicable privacy notices and on an appropriate legal basis. The Partner cannot grant blanket GDPR consent on behalf of guests. Truly anonymous statistics are outside GDPR only after effective anonymisation; pseudonymous identifiers and linked payment tokens are not anonymous. Processor data may not be repurposed merely by calling it analytics.

This DPA does not restrict data-subject rights or supervisory powers. Any inter-party liability allocation remains subject to GDPR Articles 28 and 82 and other mandatory law.