GAESTRO

Data Processing Agreement

Pursuant to Article 28 of the General Data Protection Regulation (EU) 2016/679

Version 1.0 — Effective 25 April 2026

1. Parties

This Data Processing Agreement ("DPA") is entered into between:

Data Controller ("Controller"): The entity that has entered into a service agreement with Gaestro for the use of the Gaestro platform, as identified in the applicable service agreement.

Data Processor ("Processor"): Gaestro, operated by Clinton Asonze, CVR pending registration, Denmark. Contact: privacy@gaestro.io

This DPA forms an integral part of the service agreement between the parties and supplements it with regard to the processing of personal data.

2. Definitions

Terms used in this DPA have the meanings given to them in Regulation (EU) 2016/679 ("GDPR") and the Danish Data Protection Act (Databeskyttelsesloven, Act No. 502 of 23 May 2018). In addition:

- **"Platform"** means the Gaestro guest feedback SaaS application.
- **"Personal Data"** means any information relating to an identified or identifiable natural person processed through the Platform.
- **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller.
- **"Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

3. Subject Matter and Duration

The Processor processes Personal Data on behalf of the Controller for the purpose of providing the Gaestro platform, which enables hotels to collect, store, analyze, and report on guest feedback through surveys distributed via email and QR codes.

Page 1 of 11

The duration of processing corresponds to the term of the service agreement between the parties. Upon termination, the provisions of Section 11 (Deletion and Return of Data) apply.

4. Nature and Purpose of Processing

The processing includes the following operations:

- Collection of survey responses from hotel guests via web forms
- Storage of guest personal data and survey responses in encrypted databases
- Automated sentiment analysis of free-text responses using AI
- Generation of reports, dashboards, and analytics for hotel management
- Sending transactional emails (survey invitations, thank-you messages, alerts)
- Optional photo uploads from guests, stored in encrypted object storage

5. Types of Personal Data

The following categories of Personal Data are processed through the Platform:

Category	Examples	Basis
Guest identity	Name, email address	Provided by Controller or guest
Stay information	Room number, check-out date, property name	Provided by Controller
Survey responses	Star ratings, NPS scores, free-text feedback, multiple-choice answers	Provided by guest
Photos	Images uploaded by guests alongside feedback	Provided by guest (optional)
Technical data	IP address, browser user agent, language preference	Collected automatically
Derived data	Sentiment scores, NPS calculations	Generated by the Platform

Special categories of data (Article 9): The Platform does not intentionally collect special categories of personal data. However, free-text survey responses may incidentally contain references to health, disability, or other sensitive information provided voluntarily by guests. The Controller is responsible for informing guests of this possibility.

Page 2 of 11

CPR numbers: The Platform does not collect or process Danish CPR (personal identification) numbers.

6. Categories of Data Subjects

- **Hotel guests:** Individuals who stay at the Controller's properties and submit survey responses.
- **Hotel staff:** Employees of the Controller who use the Platform (name, email, role).

7. Controller Instructions

The Processor shall process Personal Data only on documented instructions from the Controller. The service agreement and this DPA, together with the Controller's use and configuration of the Platform, constitute the Controller's complete documented instructions.

The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction infringes the GDPR or other EU or Danish data protection provisions. The Processor is not obligated to independently assess the legality of the Controller's instructions.

8. Confidentiality

The Processor shall ensure that all persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. This obligation shall survive the termination of this DPA.

9. Security Measures

The Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR. These measures are described in Annex 2.

The Processor shall regularly test, assess, and evaluate the effectiveness of these measures and update them as necessary to address evolving threats.

A description of the Processor's current security practices is available at **https://gaestro.io/security**.

10. Sub-processors

10.1 General Authorisation

Page 3 of 11

The Controller grants the Processor general written authorisation to engage Sub-processors for the processing of Personal Data, subject to the conditions in this Section 10. The current list of approved Sub-processors is set out in Annex 3.

10.2 Notification of Changes

The Processor shall notify the Controller at least **30 days** in advance before adding or replacing a Sub-processor. The notification shall include the Sub-processor's name, location, and the processing activities to be performed.

10.3 Right to Object

The Controller may object to a new or replacement Sub-processor within 14 days of receiving the notification. If the Controller objects on reasonable data protection grounds and the parties cannot resolve the objection, the Controller may terminate the service agreement without penalty.

10.4 Flow-Down Obligations

The Processor shall impose on each Sub-processor, by way of a written agreement, data protection obligations no less protective than those set out in this DPA. The Processor remains fully liable to the Controller for the performance of each Sub-processor's obligations.

11. Deletion and Return of Data

Upon termination of the service agreement, the Controller may export all Personal Data from the Platform for a period of **30 days**. The Processor provides a self-service GDPR data export function accessible to Controller administrators.

After the 30-day export window, the Processor shall delete all Personal Data from its systems, including backups, within **60 days** and shall provide written certification of deletion upon the Controller's request.

The Processor may retain Personal Data beyond this period only where required by applicable EU or Danish law, and only for the duration and purpose specified by such law.

12. Data Subject Rights

The Processor shall assist the Controller in fulfilling its obligations to respond to data subject requests under Articles 15 to 22 of the GDPR, including requests for access, rectification, erasure, data portability, restriction of processing, and objection.

The Platform provides the following self-service tools to the Controller:

- **Data export:** API endpoint for exporting all data associated with a guest email address

Page 4 of 11

- **Data deletion:** API endpoint for permanently deleting all data associated with a guest email address, including survey responses, photos, and derived analytics

If the Processor receives a request directly from a data subject, the Processor shall promptly redirect the data subject to the Controller and inform the Controller of the request.

13. Data Breach Notification

The Processor shall notify the Controller of a Data Breach **without undue delay and no later than 48 hours** after becoming aware of the breach. The notification shall include:

a. A description of the nature of the breach, including the categories and approximate number of data subjects and records affected

b. The name and contact details of the Processor's contact point

c. A description of the likely consequences of the breach

d. A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects

The Processor shall cooperate with the Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of the breach. The Processor shall assist the Controller in meeting its obligations under Articles 33 and 34 of the GDPR (notification to the supervisory authority and to data subjects).

14. Data Protection Impact Assessment

The Processor shall provide reasonable assistance to the Controller in carrying out data protection impact assessments (DPIAs) and, where necessary, prior consultation with the Danish Data Protection Agency (Datatilsynet) or other competent supervisory authority, to the extent that such assistance relates to the processing carried out by the Processor.

15. Audit Rights

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this DPA.

The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller. Audits shall be subject to the following conditions:

- The Controller shall provide at least **30 days** written notice

Page 5 of 11

- Audits shall be conducted during normal business hours and no more than **once per calendar year**
- The auditor shall be bound by confidentiality obligations
- Costs of the audit shall be borne by the Controller

Where the Processor has obtained a relevant third-party certification or audit report (such as SOC 2 or ISO 27001), the Processor may provide this report in lieu of an on-site audit, provided the report is less than 12 months old and addresses the Controller's audit objectives.

16. International Data Transfers

The Processor stores all primary data within the European Union using Cloudflare's EU data centres.

Where Personal Data is transferred to a Sub-processor located outside the European Economic Area, the Processor shall ensure that an appropriate transfer mechanism is in place, including:

- An adequacy decision by the European Commission (Article 45 GDPR)
- EU-US Data Privacy Framework certification (where applicable)
- Standard Contractual Clauses adopted by the European Commission (Decision 2021/914), supplemented by a Transfer Impact Assessment where required

The current Sub-processor list in Annex 3 includes the applicable transfer mechanism for each Sub-processor located outside the EEA.

17. Liability

The liability of each party under this DPA is subject to the limitations and exclusions of liability set out in the service agreement between the parties. This DPA does not create any independent liability beyond what is specified in the service agreement and applicable law.

18. Term and Amendments

This DPA is effective from the date the Controller begins using the Platform and remains in effect for the duration of the service agreement. The obligations relating to confidentiality, data deletion, and data protection shall survive termination.

The Processor may update this DPA to reflect changes in applicable law, regulatory guidance, or the Processor's processing activities. The Controller will be notified of material changes at least 30 days in advance.

Page 6 of 11

19. Governing Law and Jurisdiction

This DPA shall be governed by and construed in accordance with the laws of Denmark. Any disputes arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the courts of Copenhagen, Denmark.

20. Contact

For questions about this DPA or data protection matters, contact:

Gaestro — Data Protection
Email: privacy@gaestro.io
Website: https://gaestro.io/security

Agreed and accepted:

DATA CONTROLLER	DATA PROCESSOR (GAESTRO)
Name:	Name: Clinton Asonze
Title:	Title: Founder
Date:	Date:

Page 7 of 11

Annex 1 — Description of Processing

Field	Description
Subject matter	Provision of the Gaestro hotel guest feedback SaaS platform
Duration	Duration of the service agreement between Controller and Processor
Nature of processing	Collection, storage, retrieval, analysis (including AI-based sentiment analysis), reporting, transmission (email), and erasure of personal data
Purpose of processing	Enable the Controller to collect guest feedback via surveys, analyze guest satisfaction, generate management reports, and improve hospitality services
Types of personal data	Guest name, email, room number, check-out date, survey responses (ratings, free-text, multiple choice), uploaded photos, IP address, browser user agent, language preference, sentiment scores
Categories of data subjects	Hotel guests; hotel staff (administrators, property managers, property staff)
Special categories (Art. 9)	Not intentionally processed. Free-text responses may incidentally contain sensitive information.
Retention period	Configurable by Controller. Default: 24 months from collection. Controller may request earlier deletion via the GDPR deletion API.

Page 8 of 11

Annex 2 — Technical and Organisational Security Measures

The Processor implements the following measures pursuant to Article 32 of the GDPR:

Encryption

- All data in transit is encrypted using TLS 1.3
- All data at rest is encrypted via Cloudflare D1 (SQLite) and R2 (object storage) built-in encryption
- Session tokens and 2FA secrets are encrypted with application-level cryptographic keys

Access Control

- Role-based access control (RBAC) with three roles: chain administrator, property manager, property staff
- Full tenant isolation: each hotel's data is segregated at the database query level, preventing cross-hotel access
- Property-scoped access: staff members can be restricted to a single property within a chain
- Optional TOTP-based two-factor authentication (2FA) for all user accounts

Session Security

- Secure, HttpOnly session cookies with __Secure- prefix on HTTPS
- 30-minute idle session timeout with automatic expiration
- Session rotation on login to prevent session fixation

Infrastructure Security

- Application hosted on Cloudflare Workers (serverless, no persistent servers to compromise)
- DDoS protection via Cloudflare's global network
- HTTP security headers: HSTS, Content Security Policy, X-Frame-Options DENY, X-Content-Type-Options nosniff, Referrer-Policy, Permissions-Policy
- Rate limiting on authentication endpoints (20 attempts per 15-minute window per IP)

Monitoring and Audit

- Security event logging for failed logins, rate limit triggers, and suspicious activity
- Business audit trail for all significant actions (stay creation, survey changes, user invitations)
- 90-day retention on security events with daily automated cleanup

Page 9 of 11

- Automated alerting on anomalous security event patterns

Input Validation

- Server-side input validation using Zod schema validation
- Parameterised database queries via Drizzle ORM (SQL injection prevention)
- SSRF prevention on webhook URL configuration (private IP range blocking)
- HMAC-SHA256 signed webhook payloads
- File upload size limits (10 MB) and MIME type validation
- Maximum field length enforcement on all text inputs

Data Minimisation

- Guests may submit feedback anonymously
- Email addresses are optional for QR-based survey submissions
- The Platform does not collect CPR numbers or payment information

Personnel

- All personnel with access to personal data are bound by confidentiality obligations
- Access to production systems is restricted to authorised personnel only

Page 10 of 11

Annex 3 — Approved Sub-processors

The following Sub-processors are authorised to process Personal Data on behalf of the Controller as of the effective date of this DPA:

Sub-processor	Purpose	Data Processed	Location	Transfer Mechanism
Cloudflare, Inc.	Application hosting (Workers), database (D1), key-value storage (KV), object storage (R2), CDN	All categories listed in Annex 1	EU data centres (primary); US (corporate)	EU-US Data Privacy Framework + SCCs as fallback
Resend, Inc.	Transactional email delivery (survey invitations, notifications, alerts)	Guest name, email address, hotel name	United States	EU-US Data Privacy Framework + SCCs as fallback
Cloudflare Workers AI	Sentiment analysis of free-text survey responses	Free-text answer content (no identifying information sent)	EU (processed on Cloudflare infrastructure)	N/A (EU processing)

Changes to this Sub-processor list will be notified to the Controller at least 30 days in advance, in accordance with Section 10.2 of this DPA.

Page 11 of 11