PrimeGuest

PrimeGuest Data Processing Terms

Version 1.0 · Last updated 2 November 2026

These Data Processing Terms form part of the Online Terms under the PrimeGuest Master Terms and apply to every Subscription Agreement that incorporates them, in every country where PrimeGuest is provided. They prevail over the Master Terms on data protection matters. Country-specific data protection terms are in the applicable Country Schedule to the Master Terms.

1. Scope and roles

These terms apply where Cloud10 processes Guest Data and other personal data on the Customer's behalf through the Platform. The Customer is the Controller. Cloud10 is the Processor. These roles carry the equivalent meaning under each Data Protection Law that applies, including Data Fiduciary and Data Processor under Indian law. Other terms used here have the meanings given in the applicable Data Protection Law and the Master Terms.

2. Details of processing

Item	Description
Subject matter	Provision of the Platform and Services
Duration	The Subscription Term and the exit period in clause 22 of the Master Terms
Nature and purpose	Hosting, storage, retrieval, transmission, analysis and automated processing needed to run the Customer's property operations, distribution, guest messaging and reporting
Individuals	Guests, booking contacts, visitors, and the Customer's staff where entered as operational data
Categories of data	Identity and contact details, identity documents, nationality and travel details of foreign guests, booking and stay history, preferences, billing records, payment references and tokens, communications
Location	The Hosting Region stated in the Subscription Agreement, with transfers as set out in clause 6

3. Customer's obligations as Controller

The Customer will:

- have a valid consent or other lawful ground under its Data Protection Law for each processing activity it instructs;

- give Guests the notices that Data Protection Law requires, including notice of the Hosting Region where that law requires it;
- obtain any consent that Data Protection Law requires for the data of children or for special categories of data;
- complete any transfer assessment, risk assessment or regulatory filing that its Data Protection Law requires before instructing a transfer to the Hosting Region or a sub-processor;
- respond to requests and complaints from individuals;
- keep the data it enters accurate and limited to what it needs; and
- give Cloud10 only lawful instructions.

4. Cloud10's obligations as Processor

Cloud10 will:

- process the data only on the Customer's documented instructions, which are the Agreement, the Customer's configuration of the Platform and its support requests, and will tell the Customer if it believes an instruction breaches Data Protection Law;
- ensure that its personnel with access are bound by confidentiality;
- maintain the security safeguards described in clause 13.2 of the Master Terms;
- provide Platform tools that let the Customer access, correct, export and erase Guest Data, and give further reasonable assistance with individuals' requests at its professional services rates;
- notify the Customer of a personal data breach under clause 13.3 of the Master Terms and share the information the Customer needs for its own notifications to authorities and individuals;
- assist the Customer, at the Customer's cost, with data protection impact assessments and consultations with a data protection authority where the law requires them;
- delete or return the data at the end of the Services under clause 22 of the Master Terms; and
- on request, give the Customer information reasonably needed to show compliance with these terms.

5. Sub-processors

The Customer gives Cloud10 general authorisation to engage sub-processors for cloud hosting and storage, channel connectivity, messaging delivery, AI model inference, and support and monitoring tools. Cloud10 will bind each sub-processor to obligations equivalent to these terms and remains responsible for them. Cloud10 will provide its current list of sub-processors, their functions and their processing locations to the Customer on written request. Cloud10 will give 15 days' notice by email before engaging a new sub-processor that will process Guest Data. If the Customer objects on reasonable data protection grounds and the Parties cannot resolve the objection, the Customer may terminate the affected Service and receive a pro rata refund of prepaid Subscription Fees for it.

6. International transfers

6.1 Cloud10 hosts and processes Guest Data in the Hosting Region. Support, messaging delivery and AI inference may involve processing by Cloud10 or a sub-processor outside the Hosting Region.

6.2 Where a transfer of personal data from the country of the Property to the Hosting Region or to a sub-processor is restricted by Data Protection Law, Cloud10 will rely on a mechanism that law recognises: an adequacy decision or approved destination; standard contractual clauses or an equivalent approved instrument, which the Parties will sign on request as an annex to the Subscription Agreement; a certification or accreditation recognised by the competent authority; or another lawful basis available to the Customer.

6.3 The Customer will tell Cloud10 before signing if its Data Protection Law requires a particular transfer instrument, a transfer risk assessment or a regulatory approval, and will complete the steps that fall on it as Controller.

6.4 Cloud10 will not transfer personal data to a country or territory that the Data Protection Law of the Property's country, or the law of India, restricts.

6.5 Where the standard contractual clauses of a jurisdiction are signed, those clauses prevail over these terms to the extent of any conflict for transfers from that jurisdiction.

7. Audit

Once in any 12-month period, Cloud10 will answer the Customer's reasonable written security questionnaire and share its current security summary or certifications. An on-site audit is available only where a regulator requires it or after a confirmed breach affecting the Customer. It will be at the Customer's cost, on 30 days' notice, during business hours and under confidentiality.

8. Retention

Cloud10 will retain Guest Data for the period the Customer configures or instructs. Cloud10 will retain logs for the minimum period that Data Protection Law requires.

9. Regulatory cooperation

Cloud10 will cooperate with the Customer's competent data protection authority as Data Protection Law requires, and will tell the Customer of any enquiry from such an authority about the Customer's data unless the law prevents it.

10. Liability

Each Party bears the penalties and regulatory costs that result from its own breach of Data Protection Law. Cloud10's liability under these terms is subject to clause 18 of the Master Terms and the cap in the Subscription Agreement.

11. Changes in law

Cloud10 may update these terms on notice where needed to comply with a change in Data Protection Law in any country where it provides the Services.