

This Data Processing Addendum (DPA) is between the customer identified through its Forum Fortress account (Customer) and Marscastle Ltd trading as Forum Fortress, a company registered in England and Wales (company number 15029091), of Suite 37, 15 Montpellier Road, Torquay TQ1 1DL (Forum Fortress).

1. Incorporation into the service agreement

This DPA forms part of the Forum Fortress Terms of Service where Forum Fortress processes personal data on Customer's behalf. It is incorporated when Customer accepts the Terms or accepts this DPA through an authenticated Forum Fortress account. A separate acceptance record is evidence of that agreement, not a separate set of terms.

2. Definitions

Controller, Processor, Personal Data, Personal Data Breach, Process, Subprocessor and Supervisory Authority have the meanings given by applicable data-protection law. Customer Data means personal data submitted by or for Customer through the Services. Service Agreement means the Forum Fortress Terms of Service and any applicable order for the Services.

3. Scope and precedence

This DPA governs Customer Data processed for Customer under the Service Agreement. If it conflicts with the Service Agreement on processing Customer Data, this DPA prevails to the extent of that conflict. Nothing in it changes Forum Fortress's separately determined processing described in the Privacy Notice and Shared Abuse Intelligence Notice.

4. Roles of the parties

For customer-specific processing, Customer is Controller, or Processor where it operates a forum for another Controller; Forum Fortress is Processor, or Subprocessor as applicable. This includes receiving checks, analysing Customer-submitted data, returning decisions, maintaining customer-specific logs, customer-configured functionality and support.

For account administration, billing, service security, limited shared abuse-prevention intelligence and operation of the public signal checker, Forum Fortress may act as an independent Controller to the extent the relevant information constitutes personal data. Forum Fortress does not seek to establish the real-world identity of forum users and its retained intelligence architecture does not maintain a queryable cross-forum identity or activity graph.

5. Documented instructions

Customer instructs Forum Fortress to receive configured registration, posting and other forum events; normalise submitted identifiers; pseudonymise or one-way transform identifiers; compare each identifier with independently retained abuse-prevention signals; combine signals present in the current submitted request to produce a decision; return a decision and explanation; maintain customer-specific event and decision records; provide support, maintenance and security; and assist with data-subject requests. Combining email and IP signals in a current check does not mean Forum Fortress retains a historical relationship between that email and IP. Customer may give further documented instructions where lawful and technically feasible.

6. Confidentiality

Forum Fortress ensures that persons authorised to process Customer Data are bound by confidentiality obligations or an appropriate statutory duty of confidentiality.

7. Technical and organisational measures

Forum Fortress implements the measures in Schedule 3 and may improve them provided the overall protection is not materially reduced. Customer is responsible for appropriate configuration of its forum and access to the portal.

8. Subprocessors

Customer gives general written authorisation for Forum Fortress to use the subprocessors listed in Schedule 4. Forum Fortress will provide notice of material changes through the versioned subprocessor list. Customer may raise a reasonable data-protection objection; the parties will work in good faith on a reasonable solution, including discontinuing the affected processing where necessary.

9. International transfers

Forum Fortress will not transfer Customer Data internationally unless the transfer is permitted by applicable law and subject to an appropriate safeguard where required. Applicable locations and safeguards are recorded in the current versioned subprocessor list.

10. Data-subject rights

Taking account of the nature of processing, Forum Fortress will provide reasonable assistance through the Services or on request for Customer to respond to data-subject rights requests. Customer remains responsible for responding as Controller unless law requires otherwise.

11. Personal Data Breaches

Forum Fortress will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Data and will provide information reasonably available to assist Customer's compliance obligations.

12. DPIAs and regulatory consultation

Forum Fortress will provide reasonable information and assistance, taking account of the nature of processing and information available to it, for Customer's DPIAs and prior consultations.

13. Deletion or return

At the end of Customer's use of the Services, Forum Fortress will delete or return Customer Data in accordance with Schedule 2, unless retention is required by law. Customer controls its own forum records retained in its local forum system.

14. Compliance information and audits

Forum Fortress will make available information reasonably necessary to demonstrate compliance with this DPA and allow reasonable audits or inspections, subject to reasonable notice, confidentiality, security requirements, and avoiding disruption. Where an independent audit report reasonably addresses the request, Forum Fortress may provide that first.

15. Apparently unlawful instructions

Forum Fortress will inform Customer if, in its opinion, an instruction infringes applicable data-protection law, unless prohibited from doing so.

16. Liability and the Service Agreement

Liability under this DPA is subject to the liability provisions of the Service Agreement, except where applicable law provides otherwise. Nothing in this DPA limits rights that cannot lawfully be limited.

17. Changes

Forum Fortress may publish a new DPA version to reflect legal, regulatory or service changes. Published versions are immutable. A material version marked as requiring reacceptance will be clearly identified; a prior acceptance remains evidence of the version accepted.

18. Governing law

This DPA is governed by the law and jurisdiction stated in the Service Agreement.

Schedule 1 ? Processing details

****Subject matter.**** Forum spam, malicious automation, fraud and platform-abuse detection.

****Nature and purpose.**** Receiving and analysing configured forum actions, normalising identifiers, comparing independently retained signals, combining signals present in the current request, returning decisions and explanations, providing customer logs, support and security. The service does not maintain a queryable cross-forum identity graph or historical email-to-IP association.

****Duration.**** The service term plus documented operational deletion, backup and legal-record periods. Raw event identifiers and submitted content are retained for no more than five days; allowed events are then completely deleted and create no persistent intelligence. Qualifying adverse customer events may retain redacted outcome, reason-code and non-raw decision metadata for the account lifetime.

****Data subjects.**** Forum registrants, members, posters, visitors, moderators and administrators where their data appears in a configured event.

****Data categories.**** IP address; derived subnet; email address and domain; username; user-agent information; submitted content or extracts; URLs and domains; timestamps; site and event references; forum-action metadata; decision and explanation information; support communications; telephone number/CLI where support is used; and related technical security signals.

****Special-category data.**** Not requested or intentionally targeted, though user-submitted content may incidentally contain it.

Schedule 2 ? Retention and deletion

Raw submitted identifiers and content are retained for no more than five days. Allowed events are completely deleted after that operational window and do not contribute to persistent intelligence. Active customer accounts may retain redacted or pseudonymised adverse-event outcomes and explanations for the account lifetime. Detached abuse-prevention indicators may remain only where separated from customer, site, event, content, identifier and cross-forum attribution. Account deletion immediately removes live customer-specific sites, configuration, API credentials, events, decisions, support records (unless held) and attribution. Vultr automatic backups are normally about 14 days; deleted data may remain in the overall backup rotation, including encrypted Backblaze B2 EU Central backups, for up to 60 days. Marscastle also controls an offline UK backup. Support transcripts, summaries and call metadata follow account-lifetime retention; raw local call audio is normally deleted after 30 days unless held. Limited billing, contractual, complaint, security and legal records may be retained separately

where justified.

Schedule 3 ? Technical and organisational measures

Measures include authenticated portal access, restricted administrative access, transport protections, tenant-scoped access controls, logging and monitoring, secure development practices, backups, data minimisation, raw-data expiry, deletion of allowed activity, pseudonymisation or one-way transformation where appropriate, non-relational retained intelligence, API credential protection, customer-log access controls, rate-limited public lookup and deletion procedures. The current versioned Security Measures document provides the operational detail.

Schedule 4 ? Subprocessors

The current immutable provider registry version 2026-08-02.2 is incorporated into this DPA. The customer-data subprocessor schedule is: Vultr (global infrastructure, backups and limited summary inference); Backblaze (encrypted B2 EU Central/Amsterdam disaster-recovery backups); OpenAI (conditional AI support, including Realtime and Responses); Andrews & Arnold / AAISP (conditional support-call carriage); and ProxyCheck.io (conditional IP-only network-risk enrichment, HTTPS with 'tag=0'). Stripe and MXroute are separately described as other providers in the Privacy Policy and are not ordinary customer-data subprocessors for forum checks. Provider changes are versioned and notified with reasonable advance notice, normally 30 days where reasonably possible.