



SUITE.DIVINUS

Privacy Policy

UK GDPR · Data Protection Act 2018

Version 1.0 · Last Updated: 2026-09-25

Legal artefact ID: legal_privacy_v1

Provider: DivinusGratia Ltd

Company Number: 13994252

Registered Office: Croydon, Greater London, England

Contact: info@divinusgratia.co.uk

Platform: <https://suite.divinusgratia.co.uk>

PRIVACY POLICY

1. Who we are

This Privacy Policy explains how DivinusGratia Ltd (“we”, “us”, “Provider”), company number 13994252, registered office Croydon, Greater London, England, processes personal data in connection with the Suite.Divinus platform (<https://suite.divinusgratia.co.uk>). Contact: info@divinusgratia.co.uk.

Suite.Divinus is a multi-tenant SaaS operations platform. Customers operate Workspaces that may include websites, CMS/UEE surfaces, media, workflows, scheduling bridges, reporting, SamAI, Fire Evolution Packs (including Martex), commerce administration wrapping Medusa, and portals for staff, residents, members and volunteers.

2. Roles under UK data protection law

We comply with UK GDPR and the Data Protection Act 2018.

- Customer (organisation subscriber) = Controller for Customer operational data and End User data processed in their Workspace (including resident, member, volunteer, staff and portal content they choose to store).
- DivinusGratia Ltd = Processor when we process that Customer operational data to provide the Service on the Customer’s documented instructions (including Platform configuration and the Suite.Divinus Master Agreement / DPA).
- DivinusGratia Ltd = Independent Controller for account, authentication, billing, security, abuse prevention, legal compliance, product telemetry necessary to operate the Platform, and our own marketing (where consented).

Where we act as processor, further terms are set out in the Data Processing Addendum.

3. Categories of personal data

Depending on how the Platform is used, we may process:

- Account Data — names, emails, phone numbers, roles, password hashes, organisation contact emails, invite metadata.
- Billing Data — plan, commercial status, invoices, payment method tokens held by payment processors, compliance acknowledgements (including refunds/chargeback policy acceptance).
- Workspace / Organisation Data — tenant identifiers, organisation type, branding, domain settings, entitlement and activation state.
- Customer Data / Uploaded Content — documents, media, CMS pages, workflow records and other content uploaded or created in a Workspace.
- Website Data — public site content, publish state, domain bindings (auto / path / custom).
- End User Data — staff, resident, member and volunteer profiles and related operational records where the Customer uses those portals.
- Security Logs — authentication events, device identifiers, rate-limit and abuse signals, Support Access / impersonation audit metadata where implemented.
- Technical Data — IP address, user agent, session identifiers, approximate diagnostics.
- Analytics Data — first-party, consent-gated visitor page views and sessions for Customer public sites where analytics is enabled (default retention approximately 90 days unless the Customer’s settings specify otherwise within platform limits).
- AI Processing Data — prompts, context and outputs submitted to SamAI or related AI features where entitled; processed to deliver the feature to the Customer.

4. Purposes and lawful bases

Purpose	Typical lawful basis
Provide and secure the SaaS Service	Contract / legitimate interests
Billing and debt management	Contract / legitimate interests / legal obligation
Customer support and Support Access	Contract / legitimate interests
Prevent fraud, abuse and security incidents	Legitimate interests / legal obligation
First-party visitor analytics (consent-gated)	Consent

Purpose	Typical lawful basis
Optional marketing communications	Consent
Comply with law and regulators	Legal obligation

5. How we use Customer Data (important commitments)

- We do not sell Customer Data.
- We do not license Customer Data to unrelated customers.
- We do not use Customer Data to train foundation models for unrelated customers unless explicitly agreed in writing.
- AI features process prompts/outputs to deliver the feature to the Customer and may involve AI model subprocessors listed in our Subprocessor Schedule.

6. Sharing

We share personal data with subprocessors necessary to operate the Platform (hosting/database, SaaS payment collection such as Square and/or Stripe as configured, commerce engine Medusa where used, scheduling bridge Cal.diy where used, email delivery, AI model providers, CDN/storage, security tooling). Customer-configured integrations (including the Customer's own commerce payment credentials) are controlled by the Customer.

We may disclose data to professional advisors, debt recovery agents where permitted, or authorities where legally required.

7. International transfers

Where personal data is transferred outside the UK, we use appropriate safeguards (including UK adequacy decisions or UK IDTA/Addendum mechanisms) as applicable.

8. Retention

We retain personal data only as long as needed for the purposes above, including:

- Account and billing records for the Subscription term and a subsequent period for disputes, tax and legal compliance.
- Billing suspension preserves Workspace data under platform post-grace policy; soft-delete and Pending Activation purge eligibility follow Platform retention schedules (explore 14 days; idle freeze 30 days; purge eligibility after freeze 60 days — as implemented).
- Visitor analytics: default approximately 90 days.
- Invite tokens may expire on short fixed periods (including approximately 72 hours where implemented).

9. Security

We apply technical and organisational measures appropriate to a multi-tenant SaaS service, including access control, logical tenant separation, encrypted transport where applicable, and rate limiting. Absolute security cannot be guaranteed.

10. Your rights (individuals)

Under UK GDPR, individuals may have rights of access, rectification, erasure, restriction, portability, and objection, and rights related to automated decision-making where applicable. If we process your data as a processor for a Customer, please contact that Customer (controller) first. You may also contact us at info@divinusgratia.co.uk. You may complain to the Information Commissioner's Office (ICO) at <https://ico.org.uk/>.

11. Children

The Platform is directed at organisations. It is not intended for children to create accounts. Customers remain responsible for any End User age-appropriateness in their sector.

12. Changes

We may update this Policy. Material changes will be indicated by updating the version/date and, where required, by notice or renewed acceptance against a versioned legal artefact ID (platform default privacy artefact: legal_privacy_v1).

13. Contact

DivinusGratia Ltd, Company No. 13994252, Croydon, Greater London, England. Email: info@divinusgratia.co.uk.
Web: <https://suite.divinusgratia.co.uk>.