Data Processing Agreement

Version 1.0 | Effective 13 August 2026

This is Octave's standard controller-to-processor agreement for clinic installations. It forms part of the agreement between a customer and Octave only when a signed order, statement of work or other written agreement incorporates it.

Publishing it here does not by itself create a contract. Project-specific processing details and subprocessors are confirmed before production access.

Request a countersigned copy

1. Scope and definitions

This Data Processing Agreement (the **DPA**) supplements the principal services agreement, statement of work or order between the customer identified there (**Customer**) and Octave Systems Limited, company number 17354693 (**Octave**). The DPA applies whenever Octave processes personal data on the Customer's behalf in providing the agreed services.

Applicable Data Protection Law means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, legislation amending, supplementing or replacing them, including relevant amendments made by the Data (Use and Access) Act 2025, and other binding UK data-protection requirements, in each case as applicable to the services. **Controller**, **processor**, **personal data**, **processing**, **data subject** and **personal-data breach** have the meanings given by Applicable Data Protection Law.

If this DPA conflicts with the principal agreement on a data-protection matter, this DPA prevails. A project document may add detail or strengthen a control but may not reduce the protection in this DPA without a written amendment signed by authorised representatives.

2. Roles, instructions and purpose

The Customer is controller and Octave is processor for Customer personal data. If the Customer is itself a processor, Octave acts as subprocessor and the Customer warrants that its instructions reflect those of the ultimate controller and that it is authorised to appoint Octave.

Octave will process personal data only on documented instructions in the principal agreement, the relevant statement of work, an approved implementation record or another written instruction. If UK law requires other processing, Octave will tell the Customer before processing unless the law prohibits it. Octave will immediately tell the Customer if, in its reasonable

opinion, an instruction infringes Applicable Data Protection Law and will pause only the affected processing unless safety or security requires a wider stop.

Each party acts as an independent controller for ordinary business-contact details used to administer its own relationship with the other party.

3. Octave's processor obligations

Octave will:

- ensure anyone authorised to process personal data is bound by confidentiality, works on a need-to-know basis and acts only as instructed;
- implement and maintain appropriate technical and organisational measures under Article 32 UK GDPR, including the minimum measures in section 9;
- assist the Customer, taking account of the nature of processing and information available, with data-subject rights and Articles 32 to 36 UK GDPR;
- promptly forward any data-subject request and not respond except on the Customer's instruction or where legally required;
- maintain the processor records required by Article 30(2) and provide information reasonably necessary to demonstrate compliance with Article 28;
- not sell Customer personal data, combine one clinic's identifiable data with another's, or use Customer personal data to train a model; and
- return or securely delete Customer personal data at the end of the services as described in section 11.

4. Customer responsibilities

The Customer determines the purposes and essential means of processing. It is responsible for the necessary rights, transparency, lawful bases and consents, including any Article 9 condition, Data Protection Act 2018 Schedule 1 condition, common-law duty of confidentiality position and PECR analysis.

Before production, the Customer will approve the minimum data, retention, architecture, security and incident contacts, subprocessors and transfers. It will complete and approve a DPIA, or a written screening decision that one is not required, before production personal data is ingested, matched, combined, displayed or used for automation. Affected processing will not begin while a required DPIA is incomplete, identifies unmitigated high residual risk or requires prior ICO consultation.

5. Data-subject and regulatory assistance

Taking account of the nature of the processing, Octave will use appropriate technical and organisational measures to help the Customer respond to requests for access, correction, deletion, restriction, objection and portability. Octave will also provide relevant information for security assessments, breach notifications, DPIAs and prior consultation with the ICO.

Octave may charge reasonable fees for material assistance outside its ordinary course where the work does not result from Octave's breach, after first providing a reasonable estimate.

6. Personal-data breaches

Octave will notify the Customer without undue delay after becoming aware of a personal-data breach, and in sufficient time for the Customer to meet its own notification obligations. Octave will not delay the initial notice pending completion of its investigation and will provide further information in phases.

The notice will include, where known, the nature of the incident, affected data and data subjects, likely consequences, containment taken, proposed next actions and a contact point. Octave will preserve relevant evidence, contain affected processing and keep the Customer informed. The Customer decides whether to notify the ICO or affected individuals unless Octave is independently required by law to do so.

7. Subprocessors

The Customer gives general written authorisation for subprocessors identified in the current written subprocessor register supplied for its engagement. No unknown vendor or data source is approved by incorporating this DPA.

Before a subprocessor accesses live Customer personal data, Octave will identify its legal name, purpose, data, processing and remote-access locations and transfer safeguard. Where reasonably practicable, Octave will give at least 15 Business Days' notice of an addition or replacement. The Customer may object on reasonable data-protection grounds. The parties will work in good faith to resolve the objection and, if no reasonable alternative is available, either may terminate the affected processing without terminating unrelated work.

Octave will impose equivalent Article 28 obligations on each subprocessor and remains fully liable to the Customer for that subprocessor's performance of those obligations as required by Applicable Data Protection Law.

8. International transfers

Octave will not make a restricted transfer, including by permitting remote access by a separate legal person outside the UK, unless it is identified in the subprocessor register, the Customer has been notified, and the applicable adequacy regulation, International Data Transfer Agreement, UK Addendum or other lawful mechanism, transfer risk assessment and supplementary safeguards have been completed and documented.

Where the agreed architecture uses Supabase, the production database is configured for the London region. Because Supabase, Inc. is a US company and may provide support or administrative access from the US, it is not authorised for live personal data until the engagement's register, provider DPA, UK Addendum and transfer risk assessment are complete.

9. Technical and organisational measures

Control	Minimum working measure
Access	Named accounts, least privilege and MFA for privileged or production access; no shared production credentials; secrets stored securely.
Data security	Encryption in transit and at rest for production personal data and backups, with documented exceptions only where equivalent safeguards are approved.
Environments	Appropriate separation of test and production; synthetic data outside production wherever reasonably possible; only agreed workflow data is used.
Identity and workflow safety	Deterministic matching for automated actions; ambiguity goes to human review; shadow mode, suppressions, rate limits, duplicate prevention, stop control, human handoff and action logging.
Change control	Input validation, dependency management, controlled deployment and rollback appropriate to the installation.
Monitoring and resilience	Error alerting, incident escalation, platform-appropriate backups, a tested restoration approach and manual fallback.
Suppliers	Risk-based review before go-live; written processor terms; location, transfer and access review for suppliers that may see live data.
People, AI and deletion	Need-to-know access and confidentiality; no personal data in AI without section 10 approval; deletion covers active data, logs, exports, temporary files and backup expiry.

10. AI use and identity matching

No AI service may process personal data or be used to determine identity, eligibility, individualised patient-facing content or clinical action unless the parties first sign change control recording the provider, purpose, data, roles, subprocessors, transfers, retention, no-training controls, security, testing, human oversight, and DPIA and clinical-safety outcomes.

Automated actions, messages and source-system write-backs may use only deterministic patient matches approved in the implementation plan. Ambiguous, conflicting or duplicate records are excluded and routed to human review. Probabilistic or AI-based matching requires

signed change control, an updated DPIA and renewed clinical-safety approval.

11. Return and deletion

On termination or expiry of the relevant services, Octave will, at the Customer's written choice, return or securely delete the personal data and existing copies, except where UK law requires retention or where data is securely held in backups pending deletion through the ordinary backup-expiry cycle. If the Customer does not give its choice within 30 days after being asked, Octave may securely delete the data. Octave may retain anonymised compliance records that do not identify patients or disclose Customer confidential information.

12. Audit and compliance information

Octave will allow for and contribute to audits by the Customer or its appointed auditor on reasonable notice. Documentary evidence will be used first where reasonably sufficient. Except following a breach attributable to Octave or where required by the ICO, an audit is limited to once in any 12-month period on at least 10 Business Days' notice during normal business hours. The auditor must be independent, not a competitor and bound by confidentiality. An audit may not access another customer's data or include intrusive testing without separate written agreement.

13. Liability, term and governing law

This DPA remains in effect for as long as Octave processes Customer personal data. Liability, termination and dispute terms are those in the principal agreement. Unless that agreement expressly provides otherwise, English law governs and the courts of England and Wales have exclusive jurisdiction.

Schedule 1 - Processing details

The following standard particulars are completed or narrowed in the signed statement of work or approved implementation record before the relevant processing begins.

Subject matter	Agreed data integrations, internal operational views, workflow automations, logging, support and measurement.
Duration	From first authorised access until the relevant personal data is returned or deleted after termination.
Nature	Collection from agreed source systems, matching, structuring, storage, retrieval, workflow evaluation, approved communications, logging, reporting, export and deletion.

Purpose	The purposes documented for the project, which may include patient-journey coordination, operational visibility, approved workflows and measurement.
Data subjects	Customer patients and prospective patients; authorised Customer users; limited supplier and support contacts where necessary.
Personal data	Contact and identity data, source-system identifiers, appointment and journey events, payment status, communication preferences, workflow actions and audit data, limited to the approved field list.
Special-category data	Health data may be inferred from a person's relationship with a clinic, appointment or journey status, relevant test status and care communications. Clinical notes, diagnostic result values, prescribing information and treatment decisions are excluded unless expressly added by signed change control.
Frequency	As required during the agreed services and any subsequently agreed operating period.

To incorporate this DPA into an Octave engagement or request a countersigned copy, email privacy@octave.ventures.

Octave Systems Limited · Company 17354693 · Registered in England and Wales · Supplier security and privacy contact: privacy@octave.ventures