ZeroKey's Data Processing Agreement v2

Company name	ZeroKey Technologies Limited
Company number	15326987
Registered office	South Gate House, Wood Street, Cardiff, Wales, CF10 1EW
Document owner	Joseph Williams (joseph@zerokey.tech)
Version	v2
Effective date	1 July 2026
Next review	1 July 2027

Parties

This Data Processing Agreement (this Agreement) forms part of ZeroKey's Terms of Business and is made between ZeroKey Technologies Limited (Processor), registered in England and Wales with company number 15326987, whose registered office is at South Gate House, Wood Street, Cardiff, Wales, CF10 1EW (ZeroKey); and the Group Administrator as defined in ZeroKey's Terms of Business (the Controller). Each a Party and together the Parties.

Defined Terms

Account: The account a User creates in ZeroKey's Web Application to access the Service. Each Account belongs to a Group and is on either a Free Plan or a Paid Plan. An individual Account constitutes a Group of one, of which the User is the Group Administrator; Accounts may be combined into a larger Group.

Client: An individual or organisation to whom the User provides services.

Client Personal Data: Personal Data relating to a Client. May include Special Category Data, in particular health data. ZeroKey does not store it as a persistent record; any processing is transient and limited to serving the requested operation.

Controller: The party that determines the purposes and means of processing Personal Data.

Data Subject: An identified or identifiable living individual to whom Personal Data relates, as defined in the UK GDPR.

Firm: Any firm, company, partnership or other organisation.

Free Plan: A plan that grants an Account access to Sponsored Integrations only.

Group: One or more Accounts combined and administered together by a Group Administrator. An individual Account constitutes a Group of one. Where a Group is on a Paid Plan, each Account within it is on a Paid Plan and Subscription Fees are payable for each. A Group relates to no more than one Firm, and a Firm may have more than one Group.

Group Administrator: The User responsible for administering a Group. An individual Account constitutes a Group of one, of which the User is the Group Administrator; where Accounts are combined into a larger Group, the Group Administrator is the User assigned to administer it. The Group Administrator carries the Group-level obligations under ZeroKey's Terms of Business, including selecting the Group's Plan and being responsible for the Subscription Fees payable for each Account in the Group. Where the Group Administrator acts on behalf of a Firm, it does so as the Firm's authorised representative.

Integration: An integration and/or connection between two systems, built, delivered and operated by ZeroKey as part of the Service.

Paid Plan: A plan that grants an Account access to all Integrations, including Sponsored Integrations, and requires a Paid Subscription.

Paid Subscription: The paid subscription that a Paid Plan requires, and for which Subscription Fees are payable.

Personal Data: Information relating to an identified or identifiable living individual, as defined in the UK GDPR.

Processor: A party that processes Personal Data on behalf of a Controller.

Service: The services, systems or platforms provided by ZeroKey through its Solutions.

Solution: A service offering of ZeroKey. The Solutions are ZeroKey's Web Browser Extension, ZeroKey's MCP, and ZeroKey's Integration Platform.

Special Category Data: The special categories of Personal Data defined in the UK GDPR, including health data.

Sponsored Integrations: The Integrations made available to Users at no charge under a sponsored Solution.

Sub-processor: A Processor engaged by another Processor to process Personal Data on behalf of a Controller.

Subscription Fees: The subscription fees payable for each Account on a Paid Plan.

User: The individual who accepts ZeroKey's Terms of Business, creates an Account and is registered to use the Service. ZeroKey contracts with the User under ZeroKey's Web Browser Extension and ZeroKey's MCP. The User is the contracting party under ZeroKey's Terms of Business.

ZeroKey's Integration Platform: ZeroKey's integration platform-as-a-service Solution.

ZeroKey's MCP: ZeroKey's MCP (Model Context Protocol) Solution.

ZeroKey's Web Application: ZeroKey's hosted web application: the underlying application that supports ZeroKey's Web Browser Extension and ZeroKey's MCP, through which Users initially create an Account and subsequently log in to access the Service, set up and manage their Integrations, and administer their Account.

ZeroKey's Web Browser Extension: ZeroKey's web browser extension Solution.

1. Purpose and status of the Parties

1.1 This Agreement regulates the processing of Personal Data by ZeroKey when providing technology services that connect and transfer information between systems chosen by the Controller (the Service, as defined in ZeroKey's Terms of Business).

1.2 For these activities, the Group Administrator is the Controller and ZeroKey is the Processor under the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Where the Group Administrator acts on behalf of a Firm (as defined in ZeroKey's Terms of Business) under clause 2.10 of those terms, references in this Agreement to the Controller, and to the Group Administrator as Controller, are to the Firm.

1.3 ZeroKey shall process Personal Data only to deliver the Service and only on documented instructions from the Controller.

1.4 ZeroKey shall not use, access, store, analyse, mine or disclose Client Personal Data except in the strictly technical, automated form necessary to deliver the Service.

2. Description of processing

Item	Description
Subject matter	Secure transmission of data between systems chosen and authorised by the Controller.
Nature of processing	Automatic encrypted transfer initiated by the Controller's actions or configurations.
Purpose	To execute integration instructions provided by the Controller.
Categories of Data Subjects	Clients of the Controller; staff or authorised users of the Controller.
Types of Personal Data	Client Personal Data transmitted through the Service; authentication credentials; non-identifying metadata.
Storage	ZeroKey does not store Client Personal Data as a persistent record; any processing is transient and limited to serving the requested operation (encrypted authentication credentials excepted).
Duration	For the duration of the Service and until deletion under section 8.

3. ZeroKey's obligations as Processor

ZeroKey shall:

3.1 process data only on documented instructions, including Application Programming Interface (API) requests and system configurations by the Controller;

3.2 not access or view Client Personal Data except in the strictly technical, automated form necessary to deliver the Service;

3.3 not store Client Personal Data as a persistent record, any processing being transient and limited to serving the requested operation, except for encrypted authentication credentials;

3.4 ensure all personnel with access to encrypted data are bound by confidentiality;

3.5 implement the security measures described in section 7;

3.6 assist the Controller with Data Subject requests where technically feasible;

3.7 notify the Controller of a Personal Data Breach affecting Client Personal Data in accordance with section 9; and

3.8 make information reasonably available to demonstrate compliance and allow audits in accordance with section 10.

4. Controller obligations

The Controller shall:

4.1 ensure the lawful collection and transfer of Personal Data via the Service;

4.2 provide required privacy notices to Data Subjects;

4.3 ensure that credentials supplied to ZeroKey are authorised and lawfully used; and

4.4 not configure the Service to process unlawful, excessive or unexpected data.

5. Sub-processors

5.1 ZeroKey may use Sub-processors solely for infrastructure, hosting, security, monitoring, and the secure storage of encrypted credentials and metadata.

5.2 Sub-processors must be bound by written contracts offering protections equivalent to this Agreement.

5.3 ZeroKey's primary hosting provider is Amazon Web Services (AWS), operating data centres within the United Kingdom or the European Economic Area (Dublin).

5.4 The current list of Sub-processors is maintained in ZeroKey's Sub-Processor Register and may be requested from joseph@zerokey.tech; the Controller will be notified of material changes.

5.5 If the Controller objects to a Sub-processor on reasonable privacy grounds and the issue cannot be resolved, either Party may terminate the affected Service.

6. International transfers

ZeroKey shall not transfer Personal Data outside the United Kingdom unless lawful safeguards apply, including United Kingdom adequacy regulations, the United Kingdom International Data Transfer Agreement (IDTA), or the Standard Contractual Clauses (SCCs). Details are provided on request.

7. Security measures

ZeroKey shall implement appropriate technical and organisational measures, including:

- encryption in transit and at rest;
- encrypted storage of authentication credentials;
- strict access control and authentication;
- logical segregation of each Controller's integrations;
- monitoring and logging of system events (excluding readable Client Personal Data);
- secure software development and vulnerability management; and
- resilience, disaster recovery and uptime protection.

ZeroKey's infrastructure is hosted on AWS, which maintains industry-recognised certifications (for example ISO 27001).

8. Data retention and deletion

8.1 ZeroKey does not store Client Personal Data as a persistent record; any processing is transient and limited to serving the requested operation.

8.2 Encrypted authentication credentials are retained only while the relevant Account remains open.

8.3 Non-identifying metadata may be retained for up to 12 months for security, operational diagnostics and auditability.

8.4 On termination, ZeroKey shall securely delete credentials and metadata within 60 days, unless retention is required by law.

9. Assistance, impact assessments and breach notification

9.1 ZeroKey shall provide reasonable assistance to the Controller to meet its obligations under the United Kingdom General Data Protection Regulation (UK GDPR) concerning security, breach notifications, data protection impact assessments (DPIAs) and prior consultation where applicable.

9.2 ZeroKey shall notify the Controller, without undue delay and aiming to do so within 48 hours of becoming aware, of a Personal Data Breach affecting data processed as Processor.

10. Audits

10.1 ZeroKey shall provide the documentation necessary to demonstrate compliance with this Agreement.

10.2 Any audit must be conducted with reasonable notice (minimum 30 days); must not compromise security, other Controllers or intellectual property; and is limited to once per year unless required by a regulator or due to a breach.

10.3 Audits shall be at the Controller's cost unless a material breach is identified.

11. Liability

Each Party is liable for its own acts and omissions under the United Kingdom General Data Protection Regulation (UK GDPR) and this Agreement. ZeroKey is not liable for processing carried out in accordance with the Controller's instructions. ZeroKey's liability under this Agreement is subject to the limitations and exclusions of liability set out in clause 12 of ZeroKey's Terms of Business.

12. Governing law

This Agreement is governed by the laws of England and Wales, and disputes are subject to the exclusive jurisdiction of the English courts.