



## ZeroKey's Data Privacy Notice v2

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

### 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.

**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.

**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. Who we are

This privacy notice explains how ZeroKey Technologies Limited (ZeroKey, we, our or us) collects, uses, stores and protects Personal Data when you interact with our website, products, services and communications. ZeroKey is a United Kingdom-based technology company providing secure data-integration software for financial advisers and other regulated firms.

We respect your privacy and protect Personal Data in line with the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and applicable Information Commissioner's Office (ICO) guidance.

ZeroKey Technologies Limited. Registered office: South Gate House, Wood Street, Cardiff, Wales, CF10 1EW. Registered in England and Wales, company number 15326987.

ZeroKey is the data controller only for information you provide to use our website, request a demonstration or communicate with us, and for billing, account administration, marketing communications, and analysing how the Service is used to maintain and improve it and to provide management information. ZeroKey acts as a data processor on behalf of the regulated firms that use our technology (each acting as the data controller of the Personal Data of its clients); when acting as a processor, our activities are governed by ZeroKey's Data Processing Agreement with the relevant data controller.

For all privacy enquiries, contact [joseph@zerokey.tech](mailto:joseph@zerokey.tech).

## 2. Personal Data we collect as controller

We collect and process the following Personal Data when you interact directly with ZeroKey:

Category	Examples
Identity data	Name, job title, organisation
Contact data	Email address, phone number
Account and billing data	Login information, contract details, invoices



Category	Examples
<b>Marketing preferences</b>	Newsletter sign-ups, event registrations
<b>Technical website data</b>	Cookies, online identifiers, browser and device data
<b>Service usage data</b>	Usage, performance and error-diagnostic data relating to your use of the Service, including data attributable to a User or Group

We do not knowingly collect data relating to children. As a controller, we do not collect or process Special Category Data (for example health, ethnicity or biometric data).

### 3. Data processed through integrations (ZeroKey as processor)

ZeroKey software allows organisations to connect systems and transfer information securely. When Users use the Service, Client Personal Data may pass through it. ZeroKey handles that data as follows:

- we do not store Client Personal Data as a persistent record, and any processing is transient and limited to serving the requested operation;
- we do not view, analyse or use Client Personal Data except in the strictly technical, automated form necessary to deliver the Service; and
- our systems transmit data over encrypted connections using Transport Layer Security (TLS).

Client Personal Data transmitted through the Integrations may include Special Category Data (for example health data). ZeroKey does not store it as a persistent record; any processing is transient and limited to serving the requested operation. The only data ZeroKey stores is the minimum technical data required to operate securely: encrypted authentication and connection credentials; service configuration settings; and minimal metadata (for example the timestamp of a connection, or whether an Application Programming Interface (API) route succeeded or failed). This metadata does not identify adviser clients and cannot be used to reconstruct client records. The providers that support the Service are listed in ZeroKey's Sub-Processor Register.

### 4. How we collect Personal Data

We collect Personal Data directly from you when you request information or a product demonstration, subscribe to updates or marketing, create a user account, sign a contract with us, or communicate with us. We also collect limited technical data automatically when you visit our website (see section 11, Cookies).

### 5. How we use Personal Data (as controller)

Purpose	Legal basis
<b>To provide and manage your account</b>	Performance of a contract
<b>To respond to enquiries and support requests</b>	Legitimate interest (business communication)
<b>To issue invoices, take payment and manage billing</b>	Performance of a contract
<b>To maintain platform security, auditing and fraud prevention</b>	Legitimate interest (system security)
<b>To maintain, improve and develop the Service and to generate statistics and insights</b>	Legitimate interest (service improvement and analytics)
<b>To provide management information to Users and Groups</b>	Performance of a contract
<b>To send product updates or marketing where</b>	Consent



Purpose	Legal basis
requested	
To send relevant business-to-business communications to existing Users	Legitimate interest (soft opt-in)

You may withdraw consent or opt out of marketing at any time by emailing [joseph@zerokey.tech](mailto:joseph@zerokey.tech) or using the unsubscribe links in our messages.

## 6. Sharing Personal Data

We only share Personal Data with cloud hosting and software providers used for secure storage and email; payment, billing and administration providers; Users where processing relates to their accounts; and legal, regulatory or compliance bodies where required by law. We never sell Personal Data, and all service providers are bound by confidentiality and data-processing agreements. The current list is maintained in ZeroKey's Sub-Processor Register.

## 7. International transfers

ZeroKey's core services and infrastructure are hosted on Amazon Web Services (AWS) in the United Kingdom, with an encrypted backup retained in the European Economic Area (Dublin).

ZeroKey uses Cloudflare to protect and route its web and application traffic. Cloudflare routes each request to the nearest data centre and terminates Transport Layer Security (TLS) there; for traffic originating in the United Kingdom, that data centre is ordinarily in the United Kingdom. Because Cloudflare operates a global network and is a United States-headquartered provider, processing at a data centre outside the United Kingdom cannot be fully excluded (for example during failover). Any such processing is transient and occurs only while data is in transit, and may include Client Personal Data and potentially Special Category Data. Where Personal Data is processed outside the United Kingdom in this way, ZeroKey relies on the appropriate safeguards described in this section. Cloudflare is listed in ZeroKey's Sub-Processor Register.

For certain supporting functions, ZeroKey uses third-party providers that may process limited Personal Data outside the United Kingdom, for example Mailchimp (United States) for email newsletters and marketing communications. Where Personal Data is transferred outside the United Kingdom, ZeroKey relies on appropriate safeguards to ensure equivalent protection, including the United Kingdom International Data Transfer Agreement (IDTA) and/or the Standard Contractual Clauses (SCCs) as approved by the Information Commissioner's Office (ICO).

A current list of third-party providers and transfer mechanisms is maintained in ZeroKey's Sub-Processor Register and is available on request by contacting [joseph@zerokey.tech](mailto:joseph@zerokey.tech).

## 8. Data security

We apply technical and organisational measures to protect data, including encryption in transit and at rest; strict access controls and authentication; network and system monitoring; and segregation of User integrations. We notify you and the Information Commissioner's Office (ICO) where we are legally required to do so in the event of a data breach, in accordance with ZeroKey's Personal Data Breach Response Policy.

## 9. Data retention

Data type	Retention
Website and enquiry data	Up to 24 months



Data type	Retention
User account and billing records	6 years (legal requirement)
Integration metadata (non-identifiable)	Up to 12 months
Authentication keys and credentials	Only while the relevant Account remains open, then securely deleted within 60 days of the Account closing

We do not store Client Personal Data as a persistent record; any processing is transient and limited to serving the requested operation. You may request deletion of any Personal Data we hold as controller (see section 10).

## 10. Your rights

Individuals have rights under the United Kingdom General Data Protection Regulation (UK GDPR), including the right to access your Personal Data; rectify inaccuracies; request deletion (where applicable); object to certain processing; restrict processing; request transfer of your data (data portability); and withdraw consent (where consent is the legal basis). Requests should be sent to [joseph@zerokey.tech](mailto:joseph@zerokey.tech). We will respond within one calendar month unless the request is complex.

## 11. Cookies

We use essential cookies for website functionality and optional analytics cookies with your consent. Full details are provided in ZeroKey's Cookie Policy (linked on our website).

## 12. Complaints

If you have concerns about how we use your data, contact us at [joseph@zerokey.tech](mailto:joseph@zerokey.tech). You also have the right to complain to the Information Commissioner's Office (ICO) at <https://ico.org.uk/global/contact-us/> or by telephone on 0303 123 1113.