

Privacy Policy

Last Updated: 14 September 2026

1. General Provisions and Governing Law

1.1. This Privacy Policy (hereinafter — the “Policy”) sets out the procedure for the processing, storage, use, and protection of the personal data of Users of the **Office Card Service** (hereinafter — the “Service”), provided by **Financial Services LTD** (jurisdiction of incorporation: England and Wales, company number: 15556128, registered office: Flat 201, Lucienne Court, 72 Lindfield Street, London, E14 6GT, United Kingdom; hereinafter — the “Company”).

1.2. This Policy is an integral part of the Company’s [User Agreement](#) and applies together with the [AML/KYC Policy](#) of the Crypto Office Platform, in the part governing the screening of transactions, the identification of risks, and the processing of data for AML/CFT (AML/KYC) purposes within the Service. By using the Service, the User confirms that they have reviewed this Policy and the User Agreement and agrees to the processing of their data in the manner and for the purposes set out in this document.

1.3. This Policy applies equally to the Telegram bot @officeapp and the associated Mini App (Telegram Mini App) through which access to the Service is provided.

1.4. The Service is a separate functional module operating as part of the Main Product on the Crypto Office platform (hereinafter — the “Platform”), operated by SoftVision Innovations S.A. (jurisdiction of incorporation: Republic of Panama, RUC registration number: 155765203; hereinafter — the “Platform Operator”). This Policy governs the Service exclusively; the processing of personal data within the Main Product is governed by the [Privacy Policy](#) of the Crypto Office Platform and the [User Agreement](#) of the Crypto Office Platform. A User’s transition from the Main Product to the Service does not change the data-processing terms applicable to the Main Product.

1.5. The Company performs exclusively technological and informational functions, enabling Users to interact with independent Partners, and does not provide banking, payment, investment, or other licensable financial services, unless expressly stated otherwise.

1.6. The Company’s processing of personal data is carried out in accordance with the data protection laws of England and Wales, including the UK GDPR and the Data Protection Act 2018, in compliance with the principles of minimisation, transparency, and purpose limitation.

1.7. Terms used in this Policy with an initial capital letter that are not expressly defined in the text of this document (including the term “Recorded Balance”) shall have the meaning given to them in the Company’s User Agreement.

2. Role of the Company

The Company performs exclusively technological and informational functions, enabling Users to interact with independent Partners. The Company:

- is not a bank;
- is not an issuer of payment cards;
- is not a payment institution;
- does not provide regulated financial services;
- does not make decisions on the issuance or refusal to issue Card Products.

All Card Products are provided by independent Partners in accordance with their own rules, procedures, compliance requirements, and internal documents. The Partners independently determine the terms on which their services are provided, and the procedure for conducting checks and making decisions in respect of Card Products. The Company does not influence such decisions and shall not be liable for the acts or omissions of the Partners.

3. What Data We Collect

The Company adheres to the principle of data minimisation and collects only such information as is objectively necessary to provide the Service, ensure its security, perform its contractual obligations, and comply with the requirements of applicable law.

The Company does not collect or store the User's identity documents, photographs of the User or of their documents, biometric data, surname, first name, and patronymic as they appear on official documents, residential address, or other similar identification information. The provision of such data to the Company is not required in order to use the Service.

3.1. Account Data

When using the Service, the Company may receive:

- the unique Telegram identifier;
- the username;
- the profile name specified by the User in Telegram;
- the interface language;
- other information automatically provided by the Telegram API.

This data is used solely to identify the User within the Service and to ensure its operation. If the User has previously used the Main Product, identification within the Service is carried out on the basis of the same account; re-provision of data is not required.

3.2. Technical Data

When using the Service, the Company may automatically receive technical information necessary to ensure the stable operation of the Service, including:

- the IP address;
- device information;
- technical system logs;

- information about errors that have occurred.

Such data is used solely to ensure security, diagnose malfunctions, and improve the operation of the Service.

3.3. Operational Data

When using individual functions of the Service, the Company may process information necessary to carry out the relevant operations, including:

- cryptocurrency wallet addresses used when sending top-up instructions;
- transaction identifiers and their execution status;
- types of Digital Assets;
- information on the Recorded Balance and on operations carried out on Card Products.

The Company does not use such information for any purpose other than the provision of the relevant services, the ensuring of security, and compliance with the requirements of applicable law.

3.4. User-Specified Card Names

3.4.1. When applying for their first Card within the Service, the User is required to specify a first name and surname in order to create and correctly display the Cardholder profile in the Service interface.

3.4.2. The User understands and agrees that the Company does not carry out verification, documentary checking, or cross-checking of the first name and surname entered against identity documents (a passport, an ID card). Any entry made by the User in the interface is deemed technically valid for the purposes of creating the interface record.

3.4.3. The specification of a first name and surname in the Service interface does not constitute an identity-verification (KYC) procedure, does not entail the collection of personal documents, and is used solely for the technical operation of the card module.

3.5. Data on the Security of Use of the Platform

In order to prevent fraud and money laundering and to ensure the security of the Service, the Company may receive from the Platform Operator information on indicia of suspicious or atypical activity by the User within the Platform, including the Main Product. The collection and initial analysis of such information is carried out in accordance with the Privacy Policy of the Crypto Office Platform and its AML/KYC Policy. Such data is used by the Company solely for the purposes of risk assessment and the taking of security measures provided for by this Policy, and is not used for any other purpose.

4. Use of Personal Data

The Company uses personal data solely for purposes necessary for the functioning of the Service. In particular, data may be used to:

- provide the User with access to the Service and its functions;
- process User requests and enquiries to the support team;

- ensure the stable and secure operation of the Service;
- prevent fraud, abuse, and unauthorised use of the Service;
- perform obligations provided for by applicable law, including the Platform's AML/KYC Policy;
- interact with the Partners to the extent necessary to provide the User with the requested services.

The Company does not sell personal data to third parties and does not process it for purposes incompatible with this Policy.

5. Card Services

The Service provides the User with the ability to apply for and use Card Products issued by independent Partners. The Company's role in relation to the issuance and servicing of Card Products is described in Section 2 of this Policy.

The decision to block, Freeze, or otherwise restrict operations on a Card Product is made and carried out exclusively by the Partner in accordance with its own rules and security procedures. Irrespective of the Partner's decision, the Company is entitled, at any time, to fully or partially suspend or restrict the User's access to the Service interface — in particular, upon identifying atypical operations, indications of fraud, unauthorised access, or other suspicious actions, upon a breach of the terms of use of the Service, at the Partner's reasoned request, or in cases provided for by applicable law. Restrictions introduced by the Company are lifted once the circumstances giving rise to them have been resolved.

When using the Service, the User may interact with the interfaces, software modules, APIs, or other technical means of the Partners. Once such interaction has begun, the processing of certain categories of data may be governed by the relevant Partner's documents. The Company recommends that the User review the Privacy Policy and Terms of Use of the relevant Partners, where such documents are made available to the User.

6. Identity Verification

The Company does not collect, request, or store the User's identity documents, including a passport, identity card, driving licence, photographs of the User or of their documents, or biometric data. Completion of identity-verification procedures is not required in order to use the Service provided by the Company.

Where identity verification is required in order to obtain a specific service from a Partner, the corresponding data is provided by the User directly to the Partner. The Company does not receive such documents, does not verify them, and does not store them; where data is technically transmitted through the Company's interface, such transmission is carried out solely for onward delivery to the Partner, without retention of the data by the Company.

In exceptional cases, the Company may request additional information from the User where this is objectively necessary to review the User's enquiry, to comply with legal requirements, or to fulfil reasoned requests from the Partners. Such information is used solely for the

relevant purpose and is deleted once that purpose has been achieved, unless a longer retention period is required by AML/CFT legislation or by the Platform Operator's documents.

7. Disclosure of Personal Data

The Company does not sell, lease, or disclose Users' personal data to third parties, except in the following cases:

- **To the Platform Operator** — to the extent necessary for the technical operation of the Service as part of the Platform, including Account Data (Clause 3.1) and security information (Clause 3.5). The interaction between the Company and the Platform Operator, including the handling of User enquiries through the unified support service, is carried out in accordance with the terms of the User Agreement of the Crypto Office Platform and its Privacy Policy, and on the basis of a Data Processing Agreement entered into between the Company and the Platform Operator, providing for obligations relating to the protection and confidentiality of data.
- **To independent Partners** — solely to the extent necessary to provide the User with the service selected;
- **To providers of technical infrastructure** supporting the operation of the Platform;
- **To providers of information-security services**, data storage, technical support, and maintenance;
- **To competent state authorities** — solely in the cases and manner provided for by applicable law.

The Company is entitled to refuse to provide information in response to requests from state authorities where such requests are excessive, unsubstantiated, or do not comply with the requirements of applicable law.

8. Liability of the Partners

The Partners are independent service providers and are responsible for the processing of personal data carried out by them in the course of providing their own services. The Company shall not be liable for:

- the Partners' decisions on the issuance or refusal to issue Card Products;
- the results of checks and compliance procedures carried out by the Partners;
- the fees, limits, restrictions, terms of service, and internal rules of the Partners;
- the acts, omissions, or decisions of the Partners taken in the course of providing their own services.

Once the User has begun interacting with a Partner, the processing of the corresponding personal data may be carried out in accordance with the privacy policies and other documents of that Partner.

9. Retention and Protection of Data

The Company retains personal data only for such period as is necessary to achieve the purposes of its processing, to perform its contractual obligations, to review Users' enquiries, to ensure the security of the Service, and to comply with the requirements of applicable law.

Upon expiry of the retention period, personal data is deleted, anonymised, or destroyed, unless its further retention is required by law or for the protection of the Company's legitimate interests.

The Company takes reasonable organisational and technical measures to protect personal data against accidental loss, destruction, alteration, unauthorised access, disclosure, or other unlawful use. Notwithstanding the security measures taken, no method of data transmission over the Internet or of electronic storage can guarantee the absolute security of information.

10. Local Data and Similar Technologies

When using the Service through the Mini App (Telegram Mini App), the Company may use local data-storage technologies on the User's device (similar to cookies) to save User settings, maintain the session, ensure proper operation, and improve the convenience of using the Service. Such data is stored on the User's device and may be deleted using the Telegram application's tools or by clearing its cache.

11. User Rights

In the cases provided for by applicable law, the User is entitled to:

- request information about the processing of their personal data;
- obtain access to their personal data;
- request the correction of inaccurate or incomplete data;
- request the erasure of personal data, where there are no lawful grounds for its further processing;
- restrict the processing of personal data in the cases provided for by law;
- withdraw any previously given consent to the processing of personal data, where the processing is carried out on the basis of such consent;
- contact the Company with questions, comments, or complaints relating to the processing of personal data;
- lodge a complaint with the competent supervisory authority — in the United Kingdom, this authority is the Information Commissioner's Office (ICO);
- use other means of protecting their rights provided for by applicable law.

The Company reviews Users' enquiries within a reasonable time and takes the necessary measures within the scope of its authority.

12. Data of Minors

The Service is not intended for persons under 18 years of age. By using the Service, the User represents, warrants, and confirms that they have reached 18 years of age and have full legal capacity to accept the terms of this Policy. The Company does not knowingly collect or process the personal data of minors.

If the Company becomes aware that personal data has been provided by a person under 18 years of age, such data shall be deleted, and that person's access to the Service may be terminated. The legal representatives of a minor are entitled to contact the Company using the contact details set out in this Policy in order to have such data deleted.

13. International Transfers of Data

In order to ensure the operation of the Service, personal data may be processed by the Company, the Platform Operator, its contractors, and the Partners in various jurisdictions, including the jurisdiction of incorporation of the Platform Operator, where necessary for the provision of the relevant services.

The Company takes reasonable measures to ensure an appropriate level of protection for personal data when it is transferred outside the United Kingdom, including through the use of appropriate contractual data-protection mechanisms provided for under the laws of England and Wales, and seeks to engage only those service providers and Partners that ensure an appropriate level of protection of information.

14. Amendments to this Policy

The Company is entitled to amend this Privacy Policy at any time. The current version of the Policy is published in the relevant section of the Service and/or on the official website and takes effect from the moment of its publication, unless otherwise provided for in the new version.

Continued use of the Service after amendments take effect constitutes the User's agreement to the updated version of the Policy.

15. Prevailing Language of the Policy

This Policy is drawn up in the English language. Versions in other languages are provided solely for reference purposes. In the event of any discrepancy between language versions, and in reviewing requests from data subjects or in dealings with supervisory authorities, the English-language version shall prevail.

16. Contact Information

For all matters relating to the processing of personal data, the User may contact the Company using the following contact details:

Legal name: Financial Services LTD

Address: Flat 201, Lucienne Court, 72 Lindfield Street, London, E14 6GT, United Kingdom

Company number: 15556128 (England and Wales)

Email: garmizo@proton.me

Support service: Telegram bot [@office_app_support_bot](#)

Handling of enquiries from Users of the Office Card Service is carried out by the Platform's unified support service on behalf of, and in the interests of, Financial Services LTD.