

SFIT «TAMCHY»

PERSONAL DATA PROCESSING POLICY

1. Introduction and Scope

This Personal Data Processing Policy (the "Policy") sets out the procedure and purposes for the collection, storage, use and transfer of personal data by the Special Financial and Investment Territory "Tamchy" ("SFIT Tamchy") through the Resident Portal (the "Portal"). The Policy also explains the rights of data subjects and the procedure for protecting them in accordance with applicable law.

This Policy applies to all natural persons whose personal data are transferred through the Portal, including users, applicants for resident status, and representatives of resident organizations.

This Policy has been developed in accordance with:

- Law No. 136 of the Kyrgyz Republic dated 19 June 2025 "On the Special Financial and Investment Territory Tamchy" (the "SFIT Law");
- the SFIT Tamchy Personal Data Protection Rules (the "Rules"), adopted as an act of SFIT Tamchy;
- internationally recognized data protection standards, including the principles of the EU General Data Protection Regulation (GDPR), the DIFC Data Protection Law, and the ADGM Data Protection Regulations.

Summary of key rights. A data subject has the right to access their personal data, request rectification, erasure, restriction of processing and portability, object to certain types of processing, and lodge complaints. See Section 8 for details.

2. Personal Data Operator

The personal data operator (holder/owner) responsible for processing your personal data is SFIT Tamchy (the "Operator") – the Special Financial and Investment Territory "Tamchy", established under Law No. 136 of the Kyrgyz Republic.

The Operator appoints a Data Protection Officer (DPO) responsible for overseeing compliance with this Policy and the Rules.

3. Key Terms and Definitions

For the purposes of this Policy, terms have the meanings set out in Annex A to the SFIT Tamchy Personal Data Protection Rules:

- **Personal data** – any information relating to an identified or identifiable natural person (data subject).
- **Processing** – any operation performed on personal data: collection, recording, storage, alteration, retrieval, use, disclosure, transfer, restriction, erasure or destruction.
- **Data subject** – an identified or identifiable natural person whose personal data are processed.
- **Operator (controller)** – the person determining the purposes and means of processing – SFIT Tamchy.
- **Processor** – a person processing personal data on behalf of the Operator under documented instructions.
- **Consent** – a freely given, specific, informed and unambiguous indication of the data subject's wishes, expressed in written or electronic form or through a clear affirmative action.

- **Personal data breach** — a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
- **Special categories of personal data** — data revealing racial or ethnic origin, citizenship, political opinions, religious beliefs, genetic and biometric data, health data, sex life or sexual orientation.
- **Anonymization** — processing in which identifying elements are removed so that data can no longer be linked to a specific data subject by reasonable means.
- **Resident** — a legal entity registered in SFIT Tamchy and licensed to carry out activities.
- **Authorized state body** — the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic (or its legal successor).
- **SFIT Law** — Law No. 136 of the Kyrgyz Republic dated 19 June 2025 "On the Special Financial and Investment Territory Tamchy".
- **Rules** — the SFIT Tamchy Personal Data Protection Rules adopted as an act of SFIT Tamchy.

4. Categories of Data Subjects and Data Collected

4.1. Categories of Data Subjects

- Portal users (visitors);
- applicants submitting applications for resident status through the Portal;
- representatives of existing and prospective resident organizations;
- employees and officials of SFIT Tamchy bodies interacting with the Portal.

4.2. Categories of Personal Data

Basic identification data: surname, given name, patronymic, date of birth, residential address, telephone number, email address. **Identity document data:** Personal Identification Number (PIN), passport series and number, issuing authority and date of issue, place of birth, citizenship. **Corporate data:** organization name and Taxpayer Identification Number (TIN), legal and physical addresses, representative's position, organization contact details, banking details (where required for contractual purposes). **Technical data:** IP address, device identifiers, browser type and version, pages visited, access times and session duration, cookies (see Section 11).

The Operator ensures that the volume of data collected is adequate, relevant, and limited to what is necessary for the stated processing purposes (the data minimization principle), in accordance with Rule 2.6.

4.3. Special Categories of Personal Data

Identity documents (e.g. passports) may incidentally contain data revealing racial or ethnic origin, citizenship, or biometric data (photographs). Such data are treated as special categories of personal data under Rule 2.10.

The collection, accumulation, storage and use of personal data revealing racial or ethnic origin, citizenship, political opinions, religious or philosophical beliefs, or concerning health and sexual preferences, solely for the purpose of identifying such factors, is prohibited.

When processing special categories of personal data, the Operator applies enhanced protection measures: strict access segregation on a need-to-know basis, reinforced security and logging, documented necessity and proportionality assessments, and a Data Protection Impact Assessment (DPIA) where required by Rule 5.8.

5. Purposes of Personal Data Processing

The Operator processes personal data for the following purposes:

- **Registration and identification** — creating user accounts, verifying identity, managing Portal access rights.
- **Application review** — processing and evaluating applications for SFIT Tamchy resident status.
- **Notification** — informing users of application status, regulatory changes, news and Portal updates.
- **Feedback and support** — providing consultations and responding to enquiries and complaints.
- **Performance of contractual obligations** — performing obligations arising from agreements between the Operator and the data subject or their organization.
- **Analytics and improvement** — gathering statistics and analytics on Portal use to improve services. Data are anonymized where possible.
- **Legal compliance** — meeting obligations under the laws of the Kyrgyz Republic, the SFIT Law, and the Rules.
- **Security** — preventing fraud and ensuring the security and integrity of the Portal.

The Operator does not use personal data for purposes incompatible with those for which they were originally collected, except where a compatibility assessment of purposes has been carried out (Rule 2.5), additional consent has been obtained, or such use is permitted by applicable law.

6. Legal Bases for Processing

The Operator processes personal data on one or more of the following legal bases under Rule 2.3:

- **Consent** — the data subject has given explicit informed consent to one or more specific processing purposes.
- **Contractual necessity** — processing is necessary for the performance of a contract or for taking steps at the data subject's request prior to entering into a contract.
- **Legal obligation** — processing is necessary to comply with the laws of the Kyrgyz Republic, the SFIT Law, or the Rules.
- **Legitimate interests** — processing is necessary to protect the Operator's legitimate interests, except where those interests are overridden by the data subject's fundamental rights. The Operator carries out a Legitimate Interests Assessment (LIA) under Rule 2.12.
- **Vital interests** — processing is necessary to protect the vital interests of the data subject or another person.
- **Public interest** — processing is necessary to perform a task carried out in the interests of SFIT Tamchy or in the exercise of regulatory functions.

Where multiple legal bases apply to a single processing operation, the Operator identifies and documents the primary legal basis. If consent is withdrawn but another legal basis exists (e.g. contractual necessity or legal obligation), the Operator may continue processing on that alternative basis, having notified the data subject.

The applicable legal framework includes: the Constitution of the Kyrgyz Republic; Law No. 136 of the Kyrgyz Republic dated 19 June 2025 "On SFIT Tamchy"; the SFIT Tamchy Personal Data Protection Rules; and other applicable normative legal acts.

7. Consent

Where consent is the legal basis for processing (Rule 2.11):

- consent must be freely given, specific, informed, and unambiguous;
- consent may be expressed in writing, electronically (using an electronic signature in accordance with SFIT Tamchy rules), or through a clear affirmative action (e.g. ticking a box during Portal registration);
- before obtaining consent, the Operator ensures the data subject is informed of the list of data collected, the grounds and purposes of collection and use, the possibility of transfer to third parties, and other potential uses of personal data;
- the data subject may withdraw consent at any time, without affecting the lawfulness of processing carried out before withdrawal;
- withdrawing consent must be as easy as giving it – through the personal account on the Portal or through the Portal Support Service;
- where consent is withdrawn and no other legal basis exists, processing ceases and data are destroyed within the periods set out in Section 13;
- the burden of proving valid consent rests with the Operator (Rule 2.11, para. 72).

7.1. Processing of Minors' Personal Data

The Portal is intended for adult users (aged 18 and over). The Operator does not knowingly collect personal data of persons under the age of 18.

In exceptional cases where processing of a minor's data is required (e.g. where the minor is a beneficial owner or family member referred to in an application), consent must be given or authorized by a person holding parental responsibility. The Operator applies enhanced protection measures in accordance with Rule 2.18 and Annex 6 to the Rules.

If a minor's data have been collected without proper consent, the Operator shall delete them without undue delay.

8. Rights of the Data Subject

Under applicable law, the Rules (Rule 4) and international best practice, data subjects have the following rights:

- **right to information** – to receive clear and transparent information about the processing of personal data;
- **right of access** – to obtain confirmation of processing and a copy of their personal data;
- **right to rectification** – to demand correction of inaccurate or incomplete data without undue delay;
- **right to erasure ("right to be forgotten")** – to request deletion of data that are no longer needed, where consent has been withdrawn, or where processing is unlawful;
- **right to restriction (blocking) of processing** – to restrict processing in certain cases. Restriction takes effect upon receipt of the request;
- **right to data portability** – to receive personal data in a structured, machine-readable format and transmit them to another controller;
- **right to object** – to object to processing based on legitimate interests or public interest;

- **right concerning automated decision-making** — not to be subject to decisions based solely on automated processing, with the right to human intervention and to contest the decision;
- **right to be informed of disclosure/transfer** — to be informed of any transfer of personal data to third parties, including cross-border transfers;
- **right to lodge a complaint** — with the Operator, the Data Protection Officer, the authorized state body, or the SFIT Tamchy dispute resolution bodies (see Section 18).

To exercise these rights, contact the Operator or the Data Protection Officer through the Portal or by other means specified in the relevant sections of this Policy.

8.1. Response Times

- access and information requests — within 7 calendar days, subject to legal restrictions;
- rectification requests — within 7 calendar days;
- restriction (blocking) — from the moment the request is received;
- other requests (portability, objections, automated-decision safeguards) — without undue delay and no later than 30 calendar days;
- in case of refusal — a reasoned written response within 7 calendar days stating the grounds.

All responses are provided free of charge.

9. Obligations of the Data Subject

- to provide accurate and up-to-date information;
- to submit documents containing personal data in the volume necessary for the stated purposes;
- to promptly notify the Operator of any changes to personal data.

Providing inaccurate or misleading information may render it impossible to review applications or provide Portal services.

10. Obligations of the Operator

- to process personal data lawfully, fairly and transparently;
- to collect data only for specified, explicit and legitimate purposes;
- to ensure data minimization — adequacy, relevance and limitation to what is necessary;
- to keep data accurate and up to date;
- to respond to data subject requests within the timeframes set in clause 8.1;
- to provide data subjects with free access to information about their own data;
- to apply appropriate technical and organizational protection measures (Section 13);
- to notify the authorized bodies and affected data subjects of breaches (clause 13.3);
- to carry out data protection impact assessments for high-risk processing (Section 15);
- to maintain a Processing Register and records of processing operations under Rule 5.5;
- to ensure data protection by default and by design for new or significantly modified processing (Rule 5.7);
- to ensure the list of personal data corresponds to the stated collection purposes; expansion for unrelated purposes is prohibited (Rule 2.6).

11. Cookies and Tracking Technologies

The Portal uses cookies and similar technologies to provide functionality, analytics and an improved user experience in accordance with Annex 2 to the Rules.

The following cookie categories apply:

- **strictly necessary** — provide Portal functionality: authentication, security, session management. Retention: until the end of the session or up to 12 months;
- **analytical** — anonymized usage data to improve Portal performance. Retention: up to 24 months;
- **functional** — user settings (language, display options). Retention: up to 12 months.

Cookie settings can be managed via the browser settings or the cookie management center on the Portal. Disabling certain cookie categories may limit functionality.

The Portal does not use advertising or marketing cookies.

12. Data Transfers and Cross-Border Transfers

12.1. Third-Party Recipients

The Operator may transfer personal data to:

- the governing and regulatory bodies of SFIT Tamchy;
- the State Agency for Personal Data Protection and other state bodies of the Kyrgyz Republic (where required by law);
- IT service providers and hosting providers (as data processors under contract in accordance with Rule 5.9);
- professional advisers (legal, audit, consulting) under confidentiality obligations.

The Operator does not sell personal data to third parties.

12.2. Cross-Border Data Transfers

When transferring personal data outside the Kyrgyz Republic or SFIT Tamchy, the Operator ensures compliance with Rule 8:

- transfers are permitted only with authorization under applicable law and appropriate safeguards;
- a Transfer Risk Assessment (TRA) is carried out for each transfer;
- an adequate level of protection may be established by an adequacy decision, participation in an international instrument (Convention 108+), or the Operator's own assessment;
- where the destination country does not provide an adequate level of protection, standard contractual clauses, binding corporate rules or explicit consent are used.

Data subjects may request information about the safeguards applied to cross-border transfers by contacting the Data Protection Officer through the Portal.

13. Data Storage, Security and Breach Notification

13.1. Retention Periods

Personal data are retained no longer than necessary for the purposes of collection, in accordance with the Operator's documented Retention Schedule (Rule 10.3):

- **user account data** — for the term of the account and for 3 years after deletion or last activity;
- **resident-status application data** — for the term of residency and 5 years after its termination;

- **communication records** – 3 years from the date of the last contact;
- **analytical and technical data** – up to 24 months (anonymized where possible);
- **financial / banking data** – for the periods required by financial law (no less than 5 years).

On expiry of the retention period and once the collection purpose has been achieved, personal data are subject to secure destruction within 14 calendar days (Rule 10.2). Destruction is recorded in a Destruction Act (Rule 10.8). Where appropriate, the Operator may anonymize data instead of destroying them (Rule 10.9).

13.2. Security Measures

The Operator applies technical and organizational measures in accordance with Rule 6:

- encryption of data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent);
- role-based access on a need-to-know basis;
- regular security assessments, vulnerability testing and penetration tests;
- firewalls, intrusion detection systems and anti-malware tools;
- physical security of data storage facilities;
- staff training on data protection and information security;
- contractual security obligations for third-party processors;
- logging, monitoring and access traceability;
- back-ups, recovery and resilience;
- secure destruction of data carriers.

Security measures comply with ISO/IEC 27001 and SOC 2 standards and are subject to audit at least once a year (Rule 6.14).

13.3. Breach Notification

In the event of a personal data breach, the Operator, in accordance with Rule 7:

- notifies the authorized state body without undue delay and no later than 72 hours after detecting the breach (Rule 7.8);
- notifies SFIT Tamchy of critical incidents within 24 hours (Rule 7.7);
- notifies affected data subjects where there is a high risk to their rights and freedoms (Rule 7.9): describing the nature of the breach, likely consequences, measures taken and recommendations to mitigate harm;
- documents the breach in the Incident Log and Breach Register (Rule 7.10).

14. Automated Decision-Making and Profiling

The Operator does not currently carry out automated decision-making or profiling that produces legal effects on data subjects.

If such processing is introduced, the Operator will ensure: prior notification in line with the transparency principle, the right to meaningful human intervention and to contest the decision, a DPIA covering automated-decision systems, and decision logs (Rule 9).

15. Data Protection Impact Assessment (DPIA)

The Operator carries out a DPIA before any processing likely to result in a high risk (Rule 5.8): large-scale processing of special categories of data, systematic profiling, processing using new technologies, and large-volume cross-border transfers. DPIA results are documented and provided to the authorized state body and SFIT Tamchy governing bodies on request.

16. Children's Data

The Portal is intended for adult users. The Operator does not knowingly collect data of persons under 18. The procedure for processing minors' data in exceptional cases is set out in clause 7.1.

17. Updating, Correcting and Deleting Data

Inaccurate, incomplete or unlawfully processed data are subject to correction, blocking or deletion under Rule 4. If personal data have been collected unlawfully, the data subject may demand their blocking or destruction (Rules 4.6, 4.7). In case of unlawful collection, the Operator destroys the data and notifies the data subject.

Upon written request, the Operator provides information on the fact and purposes of processing; the legal basis and methods of processing; the categories of data; retention periods; the data subject's rights; data recipients; and details of any cross-border transfers.

18. Complaints and Dispute Resolution

If you believe that your personal data are being processed in breach of your rights, you may lodge a complaint with:

- the Operator – through the Portal or by other available means;
- the Data Protection Officer – through the Portal;
- the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic;
- the SFIT Tamchy International Centre for Dispute Resolution (ICDR).

The Operator acknowledges receipt of a complaint within 3 working days and provides a substantive response within 30 calendar days. Data subjects may also seek damages and compensation for moral harm in court (Rule 4.11).

19. Changes to this Policy

The Operator may amend this Policy to reflect changes in legislation, the Rules, or processing operations. Material changes are communicated by publication on the Portal with at least 14 calendar days' prior notice and, where necessary, by notifying registered users through the Portal.

Continued use of the Portal after the effective date of changes constitutes acceptance. Where material changes affect the legal basis of processing, fresh consent may be sought. All Policy versions are kept in a Version Log.

20. Governing Law and Jurisdiction

This Policy is an Act of SFIT Tamchy and is governed by applicable law in the following order: (a) Law No. 136 of the Kyrgyz Republic and other normative legal acts of the Kyrgyz Republic of higher legal force; (b) Acts of SFIT Tamchy, including this Policy and the Rules; (c) English law as adopted by SFIT Tamchy under the Application of English Law Rules (AELR).

In case of conflict between this Policy and the Personal Data Protection Rules, the Rules prevail. Disputes are resolved at the SFIT Tamchy ICDR or the competent courts of the Kyrgyz Republic in accordance with applicable law.

21. Language Versions

This Policy is published in Kyrgyz. Official translations into other languages are published on the Portal. In case of discrepancy between language versions, the Kyrgyz version prevails to the extent it does not conflict with applicable law.

22. Contacts

For any questions, requests or complaints regarding this Policy or the processing of your personal data, please contact us through the Portal Support Service.

© 2026 SFIT Tamchy. All rights reserved.