Personal Data Processing Policy
Version dated 10 April 2026

1. Purpose, Operator and Scope

1.1. This Personal Data Processing Policy (the "Policy") defines the purposes and general principles of personal data processing, as well as the measures implemented to protect the rights of personal data subjects by the Operator when using the KYC platform (SaaS) – OneKYC – for business.
1.2. This Policy applies to all personnel of the Operator, including employees under employment contracts, trainees, and persons performing work under other agreements, after they have been ознакомлены with it or such obligations have been imposed by concluding agreements with the Operator.
1.3. The requirements of this Policy are also taken into account with respect to other persons where their participation in the Operator's personal data processing activities is necessary, including partners, contractors, service providers, other counterparties, etc., including under personal data processing instructions, by entering into agreements with such persons and imposing the relevant obligations on them.
1.4. Personal Data Operator:
Limited Liability Company "Kyulchoro" (LLC "Kyulchoro")
Registered address: Kyrgyz Republic, Bishkek, Leninsky District, Kyzyl-Adyr St. (Archa-Beshik residential area), 172A
TIN: 01104202510167
Registration No.: 315102-3301-LLC
1.5. For the purposes of this Policy, the terms "personal data", "personal records", "owner of personal records", "processor", "incident in the digital environment", "personal data breach", "cross-border transfer of personal data", and "automated decision" are used in the meanings established by the Digital Code of the Kyrgyz Republic (including Article 1 of the Digital Code of the Kyrgyz Republic).

2. Compliance with Applicable Laws

2.1. This Policy has been developed primarily on the basis of the legislation of the Kyrgyz Republic, as the Operator is registered in the territory of the Kyrgyz Republic.
This Policy uses terms and definitions in accordance with their meanings as defined in the Law of the Kyrgyz Republic "On Information of a Personal Nature" dated 14 April 2008 No. 58. The Operator processes personal data taking into account the requirements of the said law, its subordinate regulations, and regulatory and methodological documents of the governmental authorities of the Kyrgyz Republic authorized in the field of information security and protection of the rights of personal data subjects.
2.2. With regard to relations in the digital environment, including personal data processing, digital identification/authentication, digital resilience and incident response, the Operator takes into account the requirements of the Digital Code of the Kyrgyz Republic dated 31 July 2025 No. 178 (in particular, Articles 57, 63, 73, 75–76, and 77–91).
2.3. Where possible, this Policy also takes into account provisions of other legislation applicable to the Operator's activities in the field of personal data processing (e.g., the GDPR) to the extent not contradicting the legislation of the Kyrgyz Republic.

3. Principles of Personal Data Processing

3.1. The Operator processes personal data on a lawful and fair basis. The main legal grounds and processing principles are determined, inter alia, by Articles 78–79 of the Digital Code of the Kyrgyz Republic. The main legal grounds for processing include:

3.1.1. The Constitution of the Kyrgyz Republic.
3.1.2. The Labour Code of the Kyrgyz Republic.
3.1.3. The Civil Code of the Kyrgyz Republic.
3.1.4. The Tax Code of the Kyrgyz Republic.
3.1.5. The Digital Code of the Kyrgyz Republic.
3.1.6. The Law of the Kyrgyz Republic “On Electric and Postal Communications”.
3.1.7. The Law of the Kyrgyz Republic “On Guarantees and Freedom of Access to Information”.
3.1.8. The Law of the Kyrgyz Republic “On Business Partnerships and Companies”.
3.1.9. The Law of the Kyrgyz Republic “On Mass Media”.
3.1.10. The Law of the Kyrgyz Republic “On Counteracting the Financing of Terrorist Activities and the Legalization (Laundering) of Criminal Proceeds”.
3.2. The content and scope of the processed personal data are determined based on the purposes of processing. Personal data that are excessive or incompatible in relation to the following main purposes are not processed:
3.2.1. Entering into employment relations with individuals, recruitment (reviewing a candidate for a vacancy, assessing skills and experience, informing about selection results, collecting feedback from the candidate, sending information about new suitable vacancies, events and internships of the Operator).
3.2.2. Entering into and extending the Operator’s contractual relationships.
3.2.3. Identifying the parties to the Operator’s contracts, agreements and transactions.
3.2.4. Performance of the Companies’ contractual obligations, including provision of services, performance of works, and granting rights to use the Operator’s software products.
3.2.5. Use by legal entities and individuals of the Operator’s websites and other information resources in accordance with their terms of use and license agreements.
3.2.6. Registration, identification and personalization of users of the Operator’s websites, applications and other information resources; granting access to resources and functions available only to registered users; improving user convenience, improving software products, and improving the quality of services provided and works performed by the Operator.
3.2.7. Communications (including via mass and automated calls) with individuals and legal entities to send notifications, responses to inquiries, mailings and informational messages, including marketing messages, as well as other actions to promote the Operator’s and partner organizations’ software products, goods, works and services.
3.2.8. Protection of the legitimate interests of the Companies, their partners and customers; exercising due (commercial) diligence in selecting counterparties; counteracting unlawful or unauthorized actions and fraud in the use by customers and users of the Operator’s software products, goods, works and services; ensuring information security.
3.2.9. Conducting research within the Operator’s scope of activity and on the use of the Operator’s software products, goods, works and services for development of new software products, expansion of services provided, works performed and goods offered, and quality control.
3.2.10. Collection and processing of analytical and statistical data within the Operator’s scope of activity and on the use of the Operator’s information resources, software products, goods, works and services.
3.2.11. Compliance with applicable labour, accounting, pension and other legislation of the Kyrgyz Republic.
3.2.12. Compliance with other legislation applicable to the Operator’s activities, including international or local legislation.
3.3. The main categories of personal data subjects include:
3.3.1. Visitors and users of the Operator’s websites, applications and information resources.

3.3.2. Individuals who are or were in employment and civil-law relations with the Operator, their close relatives, referees, as well as persons intending to enter into such relations, for example, candidates for vacant positions.
3.3.3. Individuals who are or were in employment and civil-law relations with the Operator's counterparties, as well as persons intending to enter into such relations.
3.3.4. Individuals listed in various state registers, databases, publicly available and other sources obtained lawfully and used when providing services and in the Operator's products as data sources.
3.3.5. Individuals who contact the Operator with inquiries, messages, applications, complaints or proposals using contact details or feedback collection tools.
3.3.6. The Operator's founders.
3.4. For the specified categories of subjects, the following may be processed in accordance with the purposes of processing:
3.4.1. Personal information (last name, first name, patronymic, including previous; gender; year, month, date of birth; age; place of birth; nationality; citizenship).
3.4.2. Contact information (postal address, phone numbers, email addresses, pseudonyms, identifiers in social networks and communication services); registration and actual residence addresses.
3.4.3. Information on identity documents; driver's license; identification numbers in state accounting systems; information on compulsory and voluntary medical insurance policies.
3.4.4. Professional activity (place of work; position; structural unit; personnel number; length of service; participation in legal entities; authority).
3.4.5. Skills and qualifications (education; profession; specialties; foreign languages; completed training courses, internships and practical training).
3.4.6. Family information (marital status; family composition; legal representatives; close relatives).
3.4.7. Social status; property status; information on vehicles.
3.4.8. Information on contracts and agreements and their statuses; participation in partner and bonus programs; referral promo codes; information on products and services used.
3.4.9. References and reviews; information on personnel assessments.
3.4.10. Financial status; payment details; income; information on tax and other contributions to state funds; information on accruals and withholdings, remuneration in other form; information on purchases and orders of goods and services; information on payments.
3.4.11. Information on inclusion in certain state registers, databases and lists.
3.4.12. Military registration information; migration registration information.
3.4.13. Photo and video images; voice information (voice recordings).
As part of KYC verification, the Platform may process selfies/videos and the results of "liveness" checks solely for the purposes of:
(a) verifying the document and confirming that the person presenting the document matches the image in the document;
(b) preventing fraud and unauthorized use of documents.
At the same time, the Operator does not process biometric data for the purposes of digital identification of an individual by performing searches/matching across multiple subjects (1:N) or by comparing against all biometric data available in databases, unless otherwise expressly required or permitted by applicable law. The Operator also does not use the State Biometric Identification System of the Kyrgyz Republic other than in the cases and in the manner expressly provided for by law (Article 48 of the Digital Code of the Kyrgyz Republic).
3.4.14. Documents and copies of documents.
3.4.15. Electronic user data (user identifiers, network addresses, cookies, device identifiers, screen size and resolution, hardware and software information such as browsers, operating system, installed applications, geolocation, language settings, time zone, time and usage statistics of the Operator's applications and information resources, user actions in services, sources of referrals to web pages, search and other queries sent, user-generated content); electronic signature certificates.

3.4.16. Interests and hobbies; personal interests; tastes and preferences; newsletter subscriptions.
3.4.17. Health status; information on disability and incapacity for work.
3.4.18. Information on incentives, awards, disciplinary actions and liability.
3.4.19. Other information provided for by standard forms, established procedures and purposes of processing.
3.5. The Operator processes personal data using a mixed method: with and without automation tools.
3.6. Actions performed with personal data include: collection; recording; systematization; accumulation; storage; clarification (updating, modification); extraction; use; transfer (dissemination, provision, access); depersonalization; blocking; deletion; destruction.
3.7. During processing, the accuracy, sufficiency and relevance of personal data in relation to the purposes of personal data processing are ensured (Article 78 of the Digital Code of the Kyrgyz Republic).
If inaccurate or incomplete personal data are identified, they may be уточнены and updated. Where updating personal data is outside the Operator's area of responsibility, processing may be suspended until the data are updated.
Obligations and liability for timely updating of personal data for certain processing cases may be established by the Operator's agreements.
3.8. Personal data are processed and stored no longer than required by the purposes of processing, unless there are legal grounds for further processing (Article 78 of the Digital Code of the Kyrgyz Republic).
3.9. The processed personal data are subject to destruction or depersonalization upon the occurrence of the conditions listed in this Policy. Where grounds for deletion of personal records as provided for in Article 83 of the Digital Code of the Kyrgyz Republic exist, the Operator deletes personal records without undue delay, provided there are no legal grounds for further retention (for example, for bringing/defending claims or where retention is required by law - Article 83(2) of the Digital Code of the Kyrgyz Republic).
3.10. When carrying out cross-border transfer of personal data, the Operator takes into account the requirements of Article 89 of the Digital Code of the Kyrgyz Republic.
3.10.1. Prior to any cross-border transfer, the Operator verifies whether the recipient's foreign state is included in the list of states ensuring adequate protection of the rights of personal data subjects, if such a list has been approved and published by the sectoral regulator in the field of personal data (Article 89(1)–(3) of the Digital Code of the Kyrgyz Republic).
3.10.2. If the recipient's state is not included in the said list, cross-border transfer is carried out only where there are grounds provided for in Article 89(4) of the Digital Code of the Kyrgyz Republic, in particular:
- where the personal data subject has consented to the cross-border transfer (where applicable); and/or
- for the conclusion and/or performance of a contract where the personal data subject is the beneficiary or a party (or a representative) thereto; and/or
- where adequate protection of the rights of subjects is ensured by the terms of an agreement between the records owner and the processor (or between records owners) (Article 89(4)(6) of the Digital Code of the Kyrgyz Republic), including obligations regarding confidentiality, security, incident handling, return/deletion, access restrictions, and sub-processors.
3.10.3. Before performing a cross-border transfer, the Operator assesses the risks, security measures and data access regime of the recipient and implements organizational and technical measures (e.g., encryption in transit and at rest, access restriction, logging, and contractual safeguards).
3.11. Automated decisions (where applicable): where automated decisions are used that produce legal effects for the data principal or similarly significantly affect them, the data principal is entitled to request that such decisions be discontinued and that they be reviewed with human involvement in accordance with Article 57 of the Digital Code of the Kyrgyz Republic.

4. Processing as a Sub-Processor and Engagement of Subcontractors

4.1. In addition to acting as a personal data operator, the Operator may act as a person processing personal data on behalf of other personal data operators under contracts and other agreements. Such cases include, for example:

4.1.1. Granting the Operator's customers rights to use software products.

4.1.2. Providing the Operator's customers with services related to data processing.

4.1.3. Joint processing with third-party organizations within the Operator's partnership arrangements.

4.2. Where necessary, the Operator may engage third-party organizations to process personal data as subcontractors, provided that the processing principles are complied with and there is an appropriate contract or agreement with them. Such cases include, for example:

4.2.1. Providing software products, goods, performing works and providing services to the Operator jointly by different Companies, as well as by third-party organizations, technological and other partners of the Operator.

4.2.2. Use of third-party services, computing resources, applications and infrastructure for information processing and for communications with users of software products, works and services, and purchasers of goods.

4.3. Personal data processing under the Operator's contracts and other agreements, including personal data processing instructions, is carried out in accordance with the terms of such contracts/agreements.

4.3.1. Where a processor (subcontractor) is engaged, the relevant agreement/legal instrument must contain the terms provided for by Article 86(4) of the Digital Code of the Kyrgyz Republic, including: the processing period, the nature and purposes of processing, the type of data and categories of data subjects, written instructions, confidentiality and access restriction measures, procedures for rectification/deletion/restriction of processing, and records of processing operations (logging).

4.3.2. The processor is not entitled to engage another processor without the Operator's prior written authorization.

4.3.3. Cross-border subcontractors (added): if the processor/subcontractor is located outside the Kyrgyz Republic or contemplates cross-border transfer/access, the agreement must additionally specify:

- the countries where processing/access will take place;
- the legal basis for the cross-border transfer;
- incident notification requirements (no later than 48 hours from the processor to the records owner);
- requirements for deletion/return of data upon completion of processing and upon the owner's requests;
- a prohibition on / procedure for engaging sub-processors;
- technical measures (encryption, access control, logging, etc.).

5. Obtaining the Data Subject's Consent to Process Their Personal Data

5.1. Where the legal grounds for processing provided for in Article 79(1) of the Digital Code of the Kyrgyz Republic are absent, processing is carried out subject to obtaining the personal data subject's consent.

5.2. Consent must be freely given, specific, informed and conscious, and may be provided in any form that makes it possible to confirm the fact that it was obtained.

5.3. The procedure for withdrawing consent must not be more burdensome than the procedure for providing consent.

5.4. Where personal data are obtained not directly from the subject but from other persons under a contract or processing instruction, the obligation to obtain the subject's consent may be imposed on the person from whom the personal data were obtained.

5.5. If the subject refuses to provide their personal data in the necessary and sufficient scope, the Operator will not be able to perform the actions required to achieve the relevant processing purposes.

6. Processing of Electronic User Data, Including Cookies

6.1. For the purposes of personal data processing set out in this Policy, the Operator may collect electronic user data on its websites automatically, without requiring user participation or any actions to send data.
6.2. The Operator does not verify the accuracy of electronic data collected this way; the information is processed "as is" in the form in which it is received from the client device.
6.3. Visitors and users of the Operator's websites may be shown pop-up notices about collection and processing of cookies data with a link to the Policy and buttons to accept the processing terms or close the pop-up notice.
6.4. Such notices mean that when visiting and using the Operator's websites, information resources and web applications, information (e.g., cookies data) may be stored in the browser on the user's device, allowing subsequent identification of the user or device, remembering a session, or saving certain user settings and preferences specific to those sites. After being stored in the browser and until expiry or deletion from the device, such information will be sent with each subsequent request to the website on behalf of which it was stored, together with such request, for processing on the Operator's side.
6.5. Processing of cookies data is required by the Operator for proper functioning of websites, in particular functions relating to access by registered users to the Operator's software products, services, works and resources; user personalization; increasing efficiency and convenience of working with websites, as well as other purposes provided for in this Policy.
6.6. In addition to cookies set by the Operator's websites, users and visitors may receive cookies relating to third-party websites, for example, where third-party components and software are used on the Operator's websites. Processing of such cookies is governed by the policies of the relevant websites and may change without notice to users of the Operator's websites. Such cases may include placement on the websites of:
6.6.1. Visit counters, analytics and statistical services such as Yandex.Metrica or Google Analytics to collect traffic statistics for publicly accessible website pages.
6.6.2. Widgets of auxiliary services to collect feedback, organize chats and other types of user communications.
6.6.3. Contextual advertising systems, banner and other marketing networks.
6.6.4. Authorization buttons enabling login via social network accounts.
6.6.5. Other third-party components used by the Operator on its websites.
6.7. Acceptance by the user of cookies processing terms or closing the pop-up notice in accordance with this Policy is considered consent to processing of cookies data on the Operator's websites.
6.8. If the user does not agree to processing of cookies, they must accept the risk that in this case the website's functions and features may not be fully available, and then follow one of the following options:
6.8.1. Configure the browser independently according to its documentation/help so that it does not, on a permanent basis, allow receiving and sending cookies for any websites or for a specific Operator website or third-party component website.
6.8.2. Switch to the browser's "incognito" mode to allow the site to use cookies until the browser window is closed or switched back to normal mode.
6.8.3. Leave the website to avoid further cookies processing.
6.9. The user may manage stored cookies data independently through built-in browser tools, including deleting or viewing information about cookies set by websites, including:
6.9.1. Website addresses and paths to which cookies will be sent.
6.9.2. Names and values of parameters stored in cookies.
6.9.3. Cookie expiration periods.

7. Confidentiality and Security of Personal Data

7.1. The Operator ensures confidentiality of personal data in accordance with applicable law and the terms of the Operator's agreements and contracts, except where:

7.1.1. Personal data are contained in publicly available sources of personal data or are permitted by the subject for dissemination.

7.1.2. The information is subject to mandatory disclosure to third parties, including government authorities, in accordance with the legislation applicable to the Operator.

7.2. The Operator takes necessary and sufficient legal, organizational and technical measures to ensure personal data security and to protect them from unauthorized (including accidental) access, destruction, alteration, blocking of access and other unauthorized actions. Such measures include, in particular:

7.2.1. Appointment of individuals or legal entities responsible for organizing processing and ensuring personal data security in specific Companies.

7.2.2. Issuance of internal policies on personal data processing and information security, and familiarization of employees with them.

7.2.3. Training employees on personal data processing and information security.

7.2.4. Ensuring physical security of premises and processing facilities, access control, security, video surveillance.

7.2.5. Restricting and differentiating access by employees and other persons to personal data and processing facilities, and monitoring actions with personal data.

7.2.6. Identifying threats to personal data security during processing in personal data information systems and creating threat models on that basis.

7.2.7. Using security tools (antivirus tools, firewalls, protection against unauthorized access, cryptographic information security tools), including, where necessary, tools that have undergone conformity assessment in the established manner.

7.2.8. Accounting and storage of information media to prevent theft, substitution, unauthorized copying and destruction.

7.2.9. Backup of information for recovery.

7.2.10. Internal control over compliance with the established procedure, verification of the effectiveness of measures taken, incident response.

7.2.11. Checking that agreements contain, and if necessary including, clauses on confidentiality and security of personal data.

7.2.12. The Operator takes "privacy by design" (constructive data protection) into account when designing and operating technological systems.

7.2.13. The Operator maintains records of operations involving personal records to the extent necessary to confirm compliance with obligations and to investigate incidents.

7.2.14. The Operator designates a person responsible for personal data processing within the organization in cases provided for by Article 88(2)(3) of the Digital Code of the Kyrgyz Republic.

7.2.15. The Operator organizes training for employees.

7.3. Incidents and notifications:

7.3.1. For each incident in the digital environment affecting digital resilience or the rights and legitimate interests of subjects, the Operator notifies the sectoral regulator no later than 72 hours after the incident is discovered.

7.3.2. The processor notifies the records owner about an incident within the timeframe set by the agreement, but no later than 48 hours after discovery.

7.3.3. The notification contains the information provided for by Article 63(7) of the Digital Code of the Kyrgyz Republic and is updated as new information becomes available.

7.4. The Operator implements digital resilience and digital-environment risk management measures proportionate to the nature, scope and purposes of processing.

8. Rights of Personal Data Subjects

8.1. A personal data subject has the right to withdraw consent to personal data processing by sending a relevant request to the Operator or the Operator's authorized representatives in other countries by mail or by personal visit.

8.2. A personal data subject has the right to receive information relating to processing of their personal data, including:

8.2.1. Confirmation of the fact of personal data processing by the Operator.

8.2.2. Legal grounds and purposes of personal data processing.

8.2.3. Purposes and methods of personal data processing used by the Operator.

8.2.4. Name and location of the Operator, information about persons (except employees) who have access to personal data or to whom personal data may be disclosed under a contract/agreement with the Operator or under the legislation of the Kyrgyz Republic.

8.2.5. Processed personal data relating to the relevant personal data subject, the source of their receipt, unless another procedure is provided for by the legislation of the Kyrgyz Republic.

8.2.6. Personal data processing periods, including retention periods.

8.2.7. The procedure for exercising the rights of the personal data subject under applicable law.

8.2.8. Information on completed or planned cross-border transfer of data.

8.2.9. Name or full name and address of the person processing personal data on behalf of the Operator, if processing is or will be entrusted to such a person.

8.2.10. Other information provided for by applicable law and the Operator's agreements.

8.3. A personal data subject has the right to request that the Operator clarify their personal data, block or destroy them if the personal data are incomplete, outdated, inaccurate, unlawfully obtained or not necessary for the stated processing purpose, and to take measures provided for by applicable law to protect their rights.

8.4. If a personal data subject believes that the Operator processes their personal data in violation of applicable law or otherwise violates their rights and freedoms, the subject has the right to appeal the Operator's actions or inaction in the manner provided for by applicable law.

8.5. A personal data subject has the right to protect their rights and legitimate interests, including compensation for losses and/or moral harm, in court.

8.6. The rights of the data subject/data principal are also exercised in accordance with the provisions of the Digital Code of the Kyrgyz Republic.

9. Roles and Responsibility

9.1. The rights, obligations and responsibility of the Operator are determined by applicable law and the Operator's agreements.

9.2. The liability of the Operator's employees involved in personal data processing by virtue of their functional duties for proper processing and unlawful use of personal data is established in accordance with the terms of the contract concluded between the Operator and the employee and the non-disclosure obligation.

9.3. The liability of persons involved in personal data processing under the Operator's instructions for proper processing and unlawful use of personal data is established in accordance with the terms of the contract concluded between the Operator and the counterparty, a confidentiality agreement, or another agreement.

9.4. Persons guilty of violating rules governing processing and information security of personal data bear material, disciplinary, administrative, civil or criminal liability in the manner established by applicable law and the Operator's agreements.

10. Publication and Updating of the Policy

10.1. The Policy is developed by persons responsible for organizing personal data processing in Limited Liability Company "Kyulchoro" and enters into force after approval by the Operator.

10.2. The Policy is a publicly available document of the Operator and provides the possibility for any persons to review its current version, including existing translations into foreign languages, by publishing it on the internet at https://onekyc.io.
10.3. Web forms, templates and standard forms of the Operator for collecting personal data must contain user notices about personal data processing in accordance with this Policy with a reference to it.
10.4. The Policy is valid indefinitely after approval until replaced by a new version. The Operator has the right to amend the Policy without notice to any persons.
10.5. Proposals and comments for amendments to the Policy may be sent by interested persons to info@onekyc.io.