This document is a translation of the original document ("InFinBank" AJ Shaxsga doir ma'lumotlarga ishlov berish va himoya qilish tartibi to'g'risida Nizom" — Regulation on the Procedure for Processing and Protection of Personal Data of "InFinBank" JSC) from Uzbek into English and Russian.

The original document was approved by the Management Board of "InFinBank" JSC (Minutes of the Management Board No. 179 dated June 10, 2026) and registered under No. 12 dated June 16, 2026.

In the event of any discrepancies, inconsistencies, or differences in interpretation between the text of this translation and the text of the original document, the text of the original document in the Uzbek language shall prevail.

REGULATION ON THE PROCEDURE FOR PROCESSING AND PROTECTING PERSONAL DATA

ПОЛОЖЕНИЕ О ПОРЯДКЕ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Table of Contents/Оглавление

1. GENERAL RULES/ ОБЩИЕ ПОЛОЖЕНИЯ .....**Ошибка! Закладка не определена.**

2. PERSONAL DATA CATEGORIZATION/ КАТЕГОРИЗАЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ .....**Ошибка! Закладка не определена.**

3. DATA COLLECTION AND LOCALIZATION/ СБОР И ЛОКАЛИЗАЦИЯ ДАННЫХ **Ошибка! Закладка не определена.**

4. PROCESSING PURPOSES/ ЦЕЛИ ОБРАБОТКИ ..... **Ошибка! Закладка не определена.**

5. TRANSFER OF PERSONAL DATA TO THIRD PARTIES/ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ ..**Ошибка! Закладка не определена.**

6. TECHNICAL AND ORGANIZATIONAL PROTECTION OF PERSONAL DATA/ ТЕХНИЧЕСКАЯ И ОРГАНИЗАЦИОННАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ **Ошибка! Закладка не определена.**

7. STORAGE AND DELETION/ ХРАНЕНИЕ И УНИЧТОЖЕНИЕ **Ошибка! Закладка не определена.**

8. SUBJECTS' RIGHTS/ ПРАВА СУБЪЕКТОВ.....**Ошибка! Закладка не определена.**

9. RESPONSIBILITIES AND APPEALS / ОБЯЗАННОСТИ И ОБРАЩЕНИЯ **Ошибка! Закладка не определена.**

10. CROSS-BORDER TRANSFER / ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА..... **Ошибка! Закладка не определена.**

11. RESPONSIBILITY/ ОТВЕТСТВЕННОСТЬ....**Ошибка! Закладка не определена.**

12. STORAGE/ ХРАНЕНИЕ 15

13. CONCLUSION/ ЗАКЛЮЧЕНИЕ.....15

1. GENERAL RULES

1.1. Purpose

1.1.1. The purpose of this Regulation is to regulate the activities of InFinBank JSC (hereinafter referred to as the Bank) in the field of processing and protecting personal data.

1.2. Regulatory framework

1.2.1. This Regulation is the Bank's primary internal document regulating activities in the field of processing and protecting personal data.

1.2.2. The regulation was developed in accordance with the following:

- The Law of the Republic of Uzbekistan "On Personal Data" (LRU-547, 02.07.2019);
- Law of the Republic of Uzbekistan "On Banking Secrecy" (LRU-530-II dated August 30, 2003);
- "The Model Procedure for Processing Personal Data" (Registered by the Ministry of Justice on November 15, 2023, registration No. 3478);
- The Law of the Republic of Uzbekistan "On Amendments and Additions to the Law of the Republic of Uzbekistan "On Currency Regulation" (LRU-573, 22.10.2019);
- Internal Information Security Rules of the Bank.

1.3. Field of application

1.3.1. This Regulation applies to all types of personal data processing in the Bank:

- Automated processing (in banking information systems);

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цель

1.1.1. Целью настоящего Положения является регулирование деятельности АО «InFinBank» (далее – Банк) в области обработки и защиты персональных данных.

1.2. Нормативная база

1.2.1. Настоящее Положение является основным внутренним документом Банка, регулирующим деятельность в области обработки и защиты персональных данных.

1.2.2. Положение разработано в соответствии с:

- Законом Республики Узбекистан «О персональных данных» (ЗРУ-547 от 02.07.2019);
- Законом Республики Узбекистан «О банковской тайне» (ЗРУ-530-II от 30.08.2003);
- «Типовым порядком обработки персональных данных (Зарегистрирован Министерством юстиции от 15.11.2023 года, регистрационный № 3478);
- Законом Республики Узбекистан о внесении изменений и дополнений в Закон Республики Узбекистан «О валютном регулировании» (ЗРУ-573 от 22.10.2019);
- Внутренними правилами информационной безопасности Банка.

1.3. Область применения

1.3.1. Настоящее Положение применяется ко всем видам обработки персональных данных в Банке:

- Автоматизированная обработка (в банковских информационных системах);

– Non-automated processing (paper questionnaires, dossier);	– Неавтоматизированная обработка (бумажные анкеты, досье);
– Mixed processing (electronic accounting and paper document management).	– Смешанная обработка (электронный учет и бумажный документооборот).
1.3.2. Compliance with the requirements of this Regulation is mandatory for all Bank employees who have access to personal data.	1.3.2. Соблюдение требований настоящего Положения обязательно для всех сотрудников Банка, имеющих доступ к персональным данным.
1.4. Terms and definitions	**1.4. Термины и определения**
1.4.1. The following terms are used in this Regulation:	1.4.1. В настоящем Положении используются следующие термины:
Personal data (PD) – information relating to a specific individual or allowing for their identification, recorded in electronic form, on paper, and (or) on another material medium.	**Персональные данные (ПД) –** информация, относящаяся к конкретному физическому лицу или позволяющая его идентифицировать, зафиксированная в электронном виде, на бумаге и (или) на ином материальном носителе.
Processing of personal data – any action (operation) or set of actions with personal data, including collection, recording, systematization, accumulation, storage, clarification, extraction, use, transfer, depersonalization, blocking, deletion, and destruction.	**Обработка персональных данных –** любое действие (операция) или совокупность действий с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение.
Personal data subject (Subject) – a natural person to whom personal data relates.	**Субъект персональных данных (Субъект) –** физическое лицо, к которому относятся персональные данные.
Automated processing – the processing of personal data using computing equipment.	**Автоматизированная обработка –** обработка персональных данных с помощью средств вычислительной техники.
Blocking – temporary suspension of personal data processing (except in cases where processing is necessary to clarify data).	**Блокирование** – временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения данных).
Depersonalization – actions resulting in the impossibility of determining the belonging of	**Обезличивание –** действия, в результате которых становится невозможным без использования дополнительной информации

personal data to a specific subject without using additional information.

Cross-border transfer – the transfer of personal data to a foreign state's territory, to a government body, or to a foreign individual or legal entity.

Third party - any person who is not a subject of personal data or the Bank, but is associated with them through contractual relations for the processing of personal data.

Deletion – actions resulting in the impossibility of restoring the content of personal data in the information system and the destruction of material media.

2. PERSONAL DATA CATEGORIZATION

2.1. Personal data categories

2.1.1. The bank classifies the processed personal data according to the level of criticalness:

General personal data: surname, first name, patronymic, date and place of birth, address of registration and residence, contact details (phone, e-mail), education, information about labor activity, PINFL, photograph.

Special personal data: information on criminal record (processed only when hiring employees or verifying borrowers by the Bank's security service in accordance with the law).

Biometric data: digital facial photograph, fingerprints (when used), used for identity verification through the State Personalization Center (SPC), the Bank's own biometric system, or the Bank's mobile application.

определить принадлежность персональных данных конкретному субъекту.

Трансграничная передача – передача персональных данных на территорию иностранного государства органу власти, иностранному физическому или юридическому лицу.

Третье лицо – любое лицо, не являющееся субъектом персональных данных или Банком, но связанное с ними посредством договорных отношений по обработке персональных данных.

Уничтожение – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе и уничтожаются материальные носители.

2. КАТЕГОРИЗАЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Категории персональных данных

2.1.1. Банк классифицирует обрабатываемые персональные данные по уровню критичности:

Общие персональные данные: фамилия, имя, отчество, дата и место рождения, адрес регистрации и проживания, контактные данные (телефон, e-mail), образование, сведения о трудовой деятельности, ПИНФЛ, фотоизображение.

Специальные персональные данные: сведения о судимости (обрабатываются только при найме сотрудников или проверке заемщиков службой безопасности Банка в соответствии с законодательством).

Биометрические данные: цифровое фотоизображение лица, отпечатки пальцев (при использовании), применяемые для верификации личности через Государственный центр персонализации (ГЦП), собственную систему биометрии Банка или мобильное приложение Банка.

Banking information: bank account and card numbers, account turnover, credit history data, property availability data, income and financial status information.

2.1.2. The processing of personal data concerning racial, national affiliation, political views, religious or philosophical beliefs, health status, and intimate life is not permitted, except in cases directly provided for by law.

2.2. Subjects' categories

2.2.1. The Bank processes the personal data of the following categories of entities:

- Bank employees, relatives of employees, and former employees;
- candidates for vacant positions;
- Bank clients (individuals);
- representatives of legal entities - clients of the Bank;
- counterparties under civil law contracts;
- authors of appeals sent to the Bank;
- other entities, provided they have consent to the processing of data.

3. DATA COLLECTION AND LOCALIZATION

3.1. Collection methods

3.1.1. The collection of personal data is carried out in the following ways:

- receipt of original documents or notarized copies of documents certifying their identity;

Банковская информация: номера банковских счетов и карт, обороты по счетам, данные о кредитной истории, сведения о наличии имущества, информация о доходах и финансовом положении.

2.1.2. Обработка персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни, не допускается, за исключением случаев, прямо предусмотренных законодательством.

2.2. Категории субъектов

2.2.1. Банк обрабатывает персональные данные следующих категорий субъектов:

- сотрудники Банка, родственники сотрудников, бывшие сотрудники;
- кандидаты на вакантные должности;
- клиенты Банка (физические лица);
- представители юридических лиц-клиентов Банка;
- контрагенты по гражданско-правовым договорам;
- авторы обращений, направленных в Банк;
- иные субъекты при наличии их согласия на обработку данных.

3. СБОР И ЛОКАЛИЗАЦИЯ ДАННЫХ

3.1. Способы сбора

3.1.1. Сбор персональных данных осуществляется следующими способами:

- получение оригиналов или нотариально заверенных копий документов, удостоверяющих личность;

– through the "MyID" / "Single Login" (OnelD) / Face IDs system (UzR CB Biometrics System) for electronic identification;

– through the Bank's own biometric system for authorization in the Bank's mobile application;

– applications, questionnaires, and contracts filled out by the subject;

– from open sources (state registers, public databases).

3.2. Localization

3.2.1. The Bank guarantees that the primary collection and storage of personal data of citizens of the Republic of Uzbekistan are carried out on servers located in the territory of the Republic of Uzbekistan.

3.2.2. The use of cloud services from foreign providers is permitted only if there is data mirroring on local servers in the Republic of Uzbekistan and cryptographic protection is applied.

4. PROCESSING PURPOSES

4.1. The Bank processes personal data for the following purposes:

Scoring and risk assessment: analyzing client solvency using automated algorithms and machine learning models to make credit decision-making decisions.

Anti-fraud: real-time monitoring of transactions to identify suspicious transactions and prevent theft from customer accounts.

AML/CFT: identifying and preventing operations related to the legalization of criminal proceeds and the financing of terrorism.

– через систему «MyID» / «Single Login» (OnelD) / Face IDs (Система биометрии ЦБ РУз) для электронной идентификации;

– через собственную биометрическую систему Банка для авторизации в мобильном приложение Банка;

– из заявлений, анкет, договоров, заполняемых субъектом;

– из открытых источников (государственные реестры, публичные базы данных).

3.2. Локализация

3.2.1. Банк гарантирует, что первичный сбор и хранение персональных данных граждан Республики Узбекистан производится на серверах, расположенных на территории Республики Узбекистан.

3.2.2. Использование облачных сервисов зарубежных провайдеров допускается только при наличии зеркалирования данных на локальные серверы в РУз и применения криптографической защиты.

4. ЦЕЛИ ОБРАБОТКИ

4.1. Банк осуществляет обработку персональных данных в следующих целях:

Скоринг и оценка рисков: анализ платежеспособности клиентов с использованием автоматизированных алгоритмов и моделей машинного обучения для принятия решений о выдаче кредитов.

Антифрод: мониторинг транзакций в режиме реального времени для выявления подозрительных операций и предотвращения хищений со счетов клиентов.

ПОД/ФТ: выявление и предотвращение операций, связанных с легализацией

Currency control: submitting reports to the Central Bank, the Accounts Chamber, the Ministry of Finance, the State Tax Committee, and the State Customs Committee of the Republic of Uzbekistan.

Labor relations: Regulation of labor relations: processing employee data to maintain personnel records, calculate wages, and ensure pass-through.

Marketing: Marketing and personalization of services: customer profiling to offer individual products and services (requires separate consent from the entity - ort-in).

Ensuring work with partners: fulfilling contractual obligations with counterparties.

Processing of appeals: reviewing complaints, statements, and proposals from clients.

5. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

5.1. The Bank transmits personal data to the following recipients:

State Personalization Center (SPC): for verifying passport data, PINFL, and biometric data of citizens.

Credit bureaus: providing information on borrowers' credit discipline in accordance with the Law "On Credit Information Exchange".

Insurance companies: when issuing insurance for mortgage property or the life of the borrower.

преступных доходов и финансированием терроризма.

Валютный контроль: предоставление отчетности в Центральный банк, Счетная палату, Министерство финансов, Государственный налоговый комитет и Государственный таможенный комитет Республики Узбекистан.

Трудовые отношения: Регулирование трудовых отношений: обработка данных сотрудников для ведения кадрового учета, начисления заработной платы, обеспечения пропускного режима.

Маркетинг: Маркетинг и персонализация услуг: профилирование клиента для предложения индивидуальных продуктов и услуг (требует отдельного согласия субъекта - opt-in).

Обеспечение работы с партнерами: исполнение договорных обязательств с контрагентами.

Обработка обращений: рассмотрение жалоб, заявлений и предложений клиентов.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

5.1. Банк передает персональные данные следующим получателям:

Государственный центр персонализации (ГЦП): для сверки паспортных данных, ПИНФЛ и биометрических данных граждан.

Кредитные бюро: передача данных о кредитной дисциплине заемщиков в соответствии с Законом «Об обмене кредитной информацией».

Страховые компании: при оформлении страхования залогового имущества или жизни заемщика.

Tax and law enforcement agencies: strictly on the grounds provided for by the Criminal Procedure Code, the Tax Code, and the Law "On Banking Secrecy".

Payment systems: for conducting payment operations via bank cards.

5.2. Data transfer terms

5.2.1. The Bank is entitled to transfer personal data to third parties only if:

- written consent of the personal data subject;
- requirements of the legislation of the Republic of Uzbekistan;
- a contract concluded with the entity providing for such a transfer.

5.2.2. The Bank is entitled to entrust the processing of personal data to a third party on the basis of a contract with mandatory inclusion in it:

- a list of all actions involving personal data;
- purposes of processing;
- obligations to ensure confidentiality;
- data protection requirements.

6. TECHNICAL AND ORGANIZATIONAL PROTECTION OF PERSONAL DATA

6.1. Organizational measures

Appointment of a responsible person: by order of the Chairman of the Board, a responsible official is appointed to organize the processing and protection of personal data.

Налоговые и правоохранительные органы: строго по основаниям, предусмотренным Уголовно-процессуальным кодексом, Налоговым кодексом и Законом «О банковской тайне».

Платежные системы: для осуществления платежных операций по банковским картам.

5.2. Условия передачи данных

5.2.1. Банк вправе передать персональные данные третьим лицам только при наличии:

- письменного согласия субъекта персональных данных;
- требования законодательства Республики Узбекистан;
- договора, заключенного с субъектом, предусматривающего такую передачу.

5.2.2. Банк вправе поручить обработку персональных данных третьему лицу на основании договора с обязательным включением в него:

- перечня всех действий с персональными данными;
- целей обработки;
- обязательства по обеспечению конфиденциальности;
- требований по защите данных.

6. ТЕХНИЧЕСКАЯ И ОРГАНИЗАЦИОННАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Организационные меры

Назначение ответственного лица: приказом Председателя Правления назначается должностное лицо,

	ответственное за организацию обработки и защиты персональных данных.
Differentiation of access rights: access to personal data is granted only to employees whose job duties require processing such data, after undergoing security verification and signing a non-disclosure agreement.	**Разграничение прав доступа:** доступ к персональным данным предоставляется только сотрудникам, должностные обязанности которых требуют обработки таких данных, после прохождения проверки службой безопасности и подписания обязательства о неразглашении.
Personnel training: conducting annual training for employees regarding the requirements of personal data legislation.	**Обучение персонала:** проведение ежегодного обучения сотрудников требованиям законодательства о персональных данных.
Internal control: conducting regular audits of the compliance of personal data processing with the requirements of the legislation and this Regulation.	**Внутренний контроль:** осуществление регулярных аудитов соответствия обработки персональных данных требованиям законодательства и настоящего Положения.
6.2. Technical measures	**6.2. Технические меры**
Logging and monitoring: Any employee's access to the client's personal data is recorded in the Information Leak Prevention System (DLP) with subsequent recording in the Information and Security Event Management System (SIEM). Unauthorized access to data constitutes a serious disciplinary sanction, up to and including dismissal;	**Логирование и мониторинг:** любое обращение сотрудника к персональным данным клиента фиксируется в системе предотвращения утечки информации (DLP) с дальнейшей фиксацией в системе управления информацией и событиями безопасности (SIEM). Несанкционированный доступ к данным является снованием для дисциплинарного взыскания вплоть до увольнения;
Cryptographic protection: the application of encryption for personal data during transmission via communication channels and storage in databases.	**Криптографическая защита:** применение шифрования персональных данных при передаче по каналам связи и хранении в базах данных.
Antivirus protection: the use of certified antivirus protection tools on all workstations and servers.	**Антивирусная защита:** использование сертифицированных средств антивирусной защиты на всех рабочих станциях и серверах.
Internetwork shielding: installation of software and hardware complexes to protect the network perimeter.	**Межсетевое экранирование:** установка программно-аппаратных комплексов для защиты периметра сети.

Backup: daily creation of database backups containing personal data.

6.3. Physical protection

- storage of paper documents in non-combustible metal cabinets;
- organization of a restricted access regime to the archive premises;
- installation of video surveillance systems in document storage rooms.

7. STORAGE AND DELETION

7.1. Periods for storing personal data

7.1.1. Personal data shall be stored in the Bank for no longer than required by the purposes of their processing, except in cases where the storage period is established by legislation or contract.

7.1.2. The retention period for personal data of clients is 5 (five) years after the closure of the last account or full repayment of the loan, unless otherwise provided by the legislation on countering money laundering and terrorist financing.

7.1.3. Personal data of employees shall be stored for the duration of the employment contract and for 75 years after its termination (in accordance with archival legislation).

7.2. Procedure for deleting personal data

7.2.1. Upon expiration of the established storage periods or if there are other legal grounds, personal data shall be destroyed using the following methods:

Paper documents: are destroyed by mechanical shredding (crushing) with a secrecy

Резервное копирование: ежедневное создание резервных копий баз данных с персональными данными.

6.3. Физическая защита

- хранение бумажных документов в несгораемых металлических шкафах;
- организация пропускного режима с ограничением доступа в помещения архива;
- установка систем видеонаблюдения в помещениях хранения документов.

7. ХРАНЕНИЕ И УНИЧТОЖЕНИЕ

7.1. Сроки хранения персональных данных

7.1.1. Персональные данные хранятся в Банке не дольше, чем этого требуют цели их обработки, за исключением случаев, когда срок хранения установлен законодательством или договором.

7.1.2. Срок хранения персональных данных клиентов составляет 5 (пять) лет после закрытия последнего счета или полного погашения кредита, если иное не предусмотрено законодательством о противодействии легализации доходов и финансированию терроризма.

7.1.3. Персональные данные сотрудников хранятся в течение срока действия трудового договора и 75 лет после его прекращения (в соответствии с архивным законодательством).

7.2. Порядок уничтожения персональных данных

7.2.1. По истечении установленных сроков хранения или при наличии иных законных оснований персональные данные подлежат уничтожению следующими способами:

Бумажные документы: уничтожаются путем механического шреддирования (измельчения) с уровнем секретности не

level not lower than R-4 (fragments no larger than 2×15 mm).

Electronic data: are deleted without the possibility of restoration through multiple re-recordings (at least 7 cycles) or the physical destruction of information carriers.

7.2.2. The destruction of personal data is formalized by an act signed by a commission appointed by order of the Chairman of the Board.

7.3. Depersonalization for statistical purposes

7.3.1. To conduct analytical and statistical research, personal data may be depersonalized in such a way that, without using additional information, it is impossible to determine their affiliation with a specific subject.

8. SUBJECTS' RIGHTS

8.1. Personal data subjects have the following rights:

Right to receive information: to receive complete information from the Bank about the existence, composition, and purposes of the processing of your personal data;

Right to rectification: to request the correction of inaccurate, outdated, or incomplete personal data;

Right to restrict processing: to request the restriction of processing of your personal data if it was obtained unlawfully or is not necessary for the stated processing purposes;

Right to deletion: to request the deletion of your personal data if it is no longer needed for the purposes of processing and is not subject to mandatory retention under AML/CFT legislation or archival laws;

ниже Р-4 (фрагменты размером не более 2×15 мм).

Электронные данные: удаляются без возможности восстановления методом многократной перезаписи (не менее 7 циклов) или физического уничтожения носителей информации.

7.2.2. Уничтожение персональных данных оформляется актом, подписываемым комиссией, назначаемой приказом Председателя Правления.

7.3. Обезличивание для статистических целей

7.3.1. Для проведения аналитических и статистических исследований персональные данные могут быть обезличены таким образом, чтобы без использования дополнительной информации было невозможно определить их принадлежность конкретному субъекту.

8. ПРАВА СУБЪЕКТОВ

8.1. Субъекты персональных данных имеют следующие права:

Право на получение информации: получать от Банка полную информацию о наличии, составе и целях обработки своих персональных данных;

Право на уточнение: требовать уточнения неточных, устаревших или неполных персональных данных;

Право на блокирование: требовать блокирования персональных данных, если они являются незаконно полученными или не являются необходимыми для установленных целей обработки;

Право на удаление: требовать удаления персональных данных, если они больше не нужны для целей обработки и не подлежат обязательному хранению по законодательству о ПЛД и ФТ или архивному законодательству;

Right to withdraw consent: withdraw your consent to the processing of personal data at any time.

Right to protection: to appeal the Bank's actions to the authorized body or through judicial proceedings;

Right to compensation: to demand compensation for material and moral damages caused by violations of personal data legislation.

9. RESPONSIBILITIES AND APPEALS

9.1. The subject of personal data is obliged:

– provide reliable and up-to-date personal data;

– to timely notify the Bank of changes in personal data (change of passport, residential address, contact details) within 3 (three) working days from the moment of change.

9.2. Procedure for the subjects' appeal

9.2.1. The subject may send a request for information regarding their personal data in the following ways:

- in person at any branch of the Bank with the presentation of an identity document (ID card);

- through the personal account of an internet bank or a mobile application using an electronic digital signature or biometric identification (Face ID);

- a written appeal sent to the address of the Bank's head office.

9.2.2. The Bank is obliged to review the entity's request and provide a response within 10 (ten) days from the moment the request is received.

Право на отзыв согласия: в любое время отозвать свое согласие на обработку персональных данных.

Право на защиту: обжаловать действия Банка в уполномоченном органе или в судебном порядке;

Право на возмещение ущерба: требовать возмещения материального и морального вреда, причиненного нарушением законодательства о персональных данных.

9. ОБЯЗАННОСТИ И ОБРАЩЕНИЯ

9.1. Субъект персональных данных обязан:

– предоставлять достоверные и актуальные персональные данные;

– своевременно уведомлять Банк об изменении персональных данных (смена паспорта, адреса проживания, контактных данных) в течение 3 (трех) рабочих дней с момента изменения.

9.2. Порядок обращения субъектов

9.2.1. Субъект может направить запрос о предоставлении информации о своих персональных данных следующими способами:

- лично в любом филиале Банка с предъявлением документа, удостоверяющего Личность (ID-карта);

- через личный кабинет интернет-банка или мобильного приложения с использованием электронной цифровой подписи или биометрической идентификации (Face ID);

- письменным обращением, направленным по адресу головного офиса Банка.

9.2.2. Банк обязан рассмотреть запрос субъекта и предоставить ответ в течение 10 (десяти) дней с момента получения обращения.

10. CROSS-BORDER TRANSFER

10.1. Cross-border transfer of personal data is carried out to the territory of foreign states that ensure equal protection of the rights of personal data subjects**.**

10.2. Cross-border transfer of personal data to the territory of foreign states that do not ensure their uniform protection is permitted only in cases established by the legislation of the Republic of Uzbekistan.

10.3. Before cross-border transfer of personal data to the receiving organization, the Bank ensures the signing of a confidentiality agreement containing obligations to protect the transmitted data**.**

11. RESPONSIBILITY

11.1. Officials and employees of the Bank shall be held liable for violations of the legislation on personal data in accordance with the legislation of the Republic of Uzbekistan:

Administrative liability: Article 46^2 of the Code of Administrative Responsibility of the Republic of Uzbekistan provides for the imposition of a fine for violating the rules for processing personal data.

Criminal liability: Article 141^2 of the Criminal Code of the Republic of Uzbekistan establishes criminal liability for the illegal collection or dissemination of data.

Civil Liability: The Bank is liable for material and moral damage caused by the leakage or unlawful use of personal data.

10. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА

10.1. Трансграничная передача персональных данных осуществляется на территорию иностранных государств, обеспечивающих равноценную защиту прав субъектов персональных данных.

10.2. Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих их единообразную защиту, допускается только в случаях, установленных законодательством Республики Узбекистан.

10.3. Перед осуществлением трансграничной передачи персональных данных организации-получателю Банк обеспечивает подписание соглашения о конфиденциальности, содержащего обязательства по защите передаваемых данных.

11. ОТВЕТСТВЕННОСТЬ

11.1. Должностные лица и сотрудники Банка несут ответственность за нарушение законодательства о персональных данных в соответствии с законодательством Республики Узбекистан:

Административная ответственность: статья 46^2 Кодекса об административной ответственности Республики Узбекистан предусматривает наложение штрафа за нарушение правил обработки персональных данных.

Уголовная ответственность: статья 141^2 Уголовного кодекса Республики Узбекистан устанавливает уголовную ответственность за незаконное собирание или распространение данных.

Гражданско-правовая ответственность: Банк несет ответственность за причиненный материальный и моральный вред вследствие утечки или неправомерного использования персональных данных.

11.2. Violation of the requirements of this Regulation by Bank employees shall constitute grounds for applying disciplinary measures, up to and including the termination of the employment contract.

12. STORAGE

12.1. The original copy of this Regulation is stored in the Bank's Legal Department. The electronic copy of this Regulation in .PDF format is stored on a common server for official use. The electronic copy of this Regulation in .DOCX format is stored in the Legal Department and the Information Security Department..

13. CONCLUSION

13.1. This Regulation shall enter into force from the moment it is approved by the Bank's Management Board.

13.2. All amendments and additions to this Regulation are approved by the Management Board upon submission by the Bank's Information Security Department, taking into account changes in legislative and regulatory norms, and shall enter into force from the date of their approval by the Bank's Management Board.

13.3. Control over the compliance of Bank employees with the terms of this Regulation is carried out by their direct supervisors, employees of the Information Security Department, and other authorized employees.

13.4. This Regulation is mandatory for review by all Bank employees who have access to personal data.

13.5. Bank employees must report identified deficiencies in the Regulation and violations of its requirements to the Information Security Department.

11.2. Нарушение требований настоящего Положения сотрудниками Банка является основанием для применения мер дисциплинарного воздействия вплоть до расторжения трудового договора.

12. ХРАНЕНИЕ

12.1. Оригинальный экземпляр настоящего Положения хранится в Юридическом департаменте Банка. Электронный экземпляр настоящего Положения в формате .PDF хранится на общем сервере для служебного пользования. Электронный экземпляр настоящего Положения в формате .DOCX хранится в Юридическом департаменте и департаменте Информационной безопасности.

13. ЗАКЛЮЧЕНИЕ

13.1. Настоящее Положение вступает в силу с момента его утверждения Правлением Банка.

13.2. Все изменения и дополнения к настоящему Положению утверждаются Правлением по представлению Департаментом Информационной Безопасности Банка с учетом изменений законодательных и регулирующих норм и вступают в силу с даты утверждения их Правлением Банка.

13.3. Контроль за соблюдением работниками Банка условий настоящего Положения осуществляют их непосредственные руководители, работники Департамента Информационной безопасности и другие уполномоченные работники.

13.4. Настоящее Положение обязательна к ознакомлению для всех работников Банка, имеющих доступ к персональным данным.

13.5. Работники Банка должны сообщать об обнаруженных недостатках в Положении, и нарушениях требований настоящего Положения Департаменту Информационной Безопасности.

13.6. This Regulation shall be reviewed as necessary, but at least once every twelve months.	**13.6.** Настоящее Положение пересматривается по мере необходимости, но не реже одного раза в двенадцать месяцев.