

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ПЛАТФОРМЫ GetCrypto

1. ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

В настоящей Политике конфиденциальности и обработки персональных данных (далее — «**Политика**») используются следующие термины:

1.1. Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в соответствии с п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — «**152-ФЗ**») Персональные данные не включают информацию, собираемую автоматически (cookie-файлы, IP-адреса, данные геолокации). Подробнее см. раздел 4.1.1 и Политику Cookie.

1.2. Оператор персональных данных (Оператор ПДн) — Общество с ограниченной ответственностью «ГетКрипто», управляющее Платформой GetCrypto, которое организует и осуществляет обработку персональных данных, определяет цели и состав обрабатываемых данных в соответствии с 152-ФЗ (далее — «**GetCrypto**»).

1.3. Обработка персональных данных — любое действие (операция) или совокупность действий, совершаемых с использованием средств автоматизации или без них, включая сбор, запись, хранение, уточнение, передачу, обезличивание, блокирование и уничтожение персональных данных (ст. 3 152-ФЗ).

1.4. Платформа GetCrypto (Платформа) — информационный сервис, доступный по адресу www.getcrypto.ru, предоставляющий пользователям возможность взаимодействия с Операторами обменных пунктов цифровых валют (далее — «**ОП**») без осуществления операций с активами.

1.5. Пользователь — физическое лицо или представитель юридического лица, зарегистрированное на Платформе, которое:

- Является совершеннолетним согласно законодательству РФ;
- Не является сотрудником Оператора ОП.

1.6. Оператор обменного пункта (Оператор ОП) — юридическое лицо, ИП или физическое лицо, прошедшее листинг на Платформе и осуществляющее обмен цифровых активов. Оператор ОП обязан соблюдать требования 115-ФЗ, включая проведение KYC/AML-проверок Пользователей.

1.7. Обменный пункт (ОП) — сервис, управляемый Оператором ОП, осуществляющий операции с цифровыми активами и несущий самостоятельную ответственность за сохранность средств пользователей.

1.8. Учетная запись (Личный кабинет) — персонализированный защищенный раздел Платформы, доступный Пользователю после регистрации и ввода аутентификационных данных (логин и пароль), предназначенный для:

- Управления настройками профиля;
- Доступа к функционалу Платформы, включая размещение Контента Пользователя;
- Просмотра информации об операциях и взаимодействии с Операторами ОП.

1.9. Контент Пользователя — отзывы, оценки и комментарии, размещаемые Пользователем на Платформе в рамках использования Учетной записи, в том числе:

- Отзывы о качестве услуг Операторов ОП;
- Комментарии, касающиеся курсов обмена, скорости транзакций и иных аспектов работы Обменных пунктов.

Контент Пользователя может содержать его **логин** (имя пользователя), который не считается персональными данными в соответствии с ст. 3 152-ФЗ, при условии, что:

- Логин не содержит информации, позволяющей прямо или косвенно идентифицировать Пользователя (например, не совпадает с реальным именем, email или иными данными, связанными с личностью);
- Логин используется исключительно в обезличенном формате (например, «Пользователь №12345») после удаления аккаунта (п. 7.3.1 Политики).

Контент не включает иные персональные данные, не предназначенные для публичного доступа (email, ФИО), и не содержит информации, позволяющей установить личность Пользователя.

1.10. AML (Anti-Money Laundering) — противодействие отмыванию доходов, полученных преступным путем, в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ (далее — «115-ФЗ») и международными стандартами (рекомендации ФАТФ).

1.11. CFT (Counter-Terrorist Financing) — противодействие финансированию терроризма, регулируемое 115-ФЗ и ст. 205–205.5 УК РФ.

1.12. KYC (Know Your Customer) — процедура идентификации и верификации клиентов, проводимая Операторами ОП в соответствии с 115-ФЗ.

1.13. Минимальные данные — базовые данные, необходимые для идентификации физического лица и осуществления конкретных операций с ним. В настоящей Политике под минимальными данными понимаются персональные данные (ФИО, email, логин), обрабатываемые Платформой исключительно для регистрации и технической поддержки.

1.14. Обезличивание данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту без использования дополнительной информации (ст. 3 152-ФЗ). При обезличивании используются методы, соответствующие стандарту ISO/IEC 20889.

1.15. Трансграничная передача данных (Cross-Border Data Transfer) — передача персональных данных на территорию иностранного государства. Платформа не осуществляет такую передачу, за исключением случаев, прямо предусмотренных международными договорами РФ.

1.16. Автоматизированное принятие решений (Automated Decision-Making) — обработка данных без участия человека (например, блокировка аккаунта через алгоритмы машинного обучения). Пользователь вправе потребовать человеческого вмешательства.

1.17. Все остальные понятия и определения, приведенные в настоящей Политике, имеют значения, присвоенные им в «Пользовательском соглашении Платформы GetCrypto».

2. ВВЕДЕНИЕ

2.1. Цель Политики

Политика определяет порядок обработки персональных данных Платформой GetCrypto в соответствии с требованиями:

Федеральные законы:

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»;
2. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты РФ»;
4. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»;
5. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
6. Федеральный закон от 31.07.2020 N 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»;

Постановления Правительства РФ:

1. Постановление Правительства РФ от 29.06.2021 N 1046 «Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных» (госнадзор за ПДн);
2. Постановление Правительства РФ от 21.03.2012 N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» (меры по 152-ФЗ);
3. Постановление Правительства РФ от 01.11.2012 N 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (требования к защите ПДн);
4. Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (ручная обработка);
5. Постановление Правительства РФ от 16.03.2009 N 228 «Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (о Роскомнадзоре);

Приказы Роскомнадзора:

1. Приказ Роскомнадзора от 24.02.2021 N 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения» (согласие на обработку);
2. Приказ Роскомнадзора от 28.10.2022 N 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных» (формы уведомлений);
3. Приказ Роскомнадзора от 05.09.2013 N 996 «Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных» (обезличивание);
4. Приказ Роскомнадзора от 06.04.2010 N 213 «Об утверждении Регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций» (регламент).

Иные документы:

1. Положение Банка России от 15.10.2015 N 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (AML);
2. Указание Банка России от 07.11.2022 N 6308-У «О внесении изменений в нормативные акты Банка России в сфере требований к правилам внутреннего контроля кредитных организаций и некредитных финансовых организаций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (AML);
3. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (техническая защита);
4. ГОСТ Р 56938–2016 от 06.12.2018 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» (виртуализация).
5. Рекомендации ФАТФ (FATF). Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения, включая Правило 12 (риски PEP) и Правило 15 (обязанности посредников).

2.2. Область применения

Политика распространяется на:

- **Пользователей** (п. 1.5. Политики);
- **Операторов ОП** — юридических лиц, ИП и их представителей (руководителей, бенефициаров), проходящих листинг на Платформе, а также периодические аудиты (1.6.).

Политика регулирует обработку:

- **Минимальных данных Пользователей** (ФИО, email) — автоматически через Платформу;
- **Данных представителей Операторов ОП** (паспорт, ИНН, реквизиты) — как автоматическими средствами, так и вручную уполномоченными сотрудниками GetCrypto.

2.3. Принципы обработки данных

GetCrypto обязуется соблюдать следующие принципы (ст. 5 152-ФЗ):

- Законность — обработка только на основании согласия или в рамках исполнения законодательных требований;
- Минимизация данных — сбор исключительно необходимых для заявленных целей сведений;
- Ограничение целей — запрет на обработку, несовместимую с целями, указанными в Политике;
- Конфиденциальность — защита данных от несанкционированного доступа.

2.4. Распределение ответственности

2.4.1. Платформа обрабатывает:

- Минимальные данные Пользователей (ФИО, email) — для регистрации и связи;
- Данные представителей Операторов ОП (паспорт, ИНН, реквизиты) — для верификации и AML/CFT-аудита.

2.4.2. Операторы ОП несут ответственность за:

- Проведение KYC/AML-проверок Пользователей;
- Мониторинг транзакций и передачу данных в Росфинмониторинг.

2.5. Правовые основания обработки

- Для **Пользователей** — согласие на обработку данных (п. 1 ч. 1 ст. 6 152-ФЗ), которое предоставляется путем положительного действия (галочки) при регистрации на Платформе. Форма согласия является неотъемлемой частью Пользовательского соглашения и доступна по ссылке: [ссылка].
- Для **Операторов ОП** — исполнение договора (п. 2 ч. 1 ст. 6 152-ФЗ) и соблюдение законодательства (п. 3 ч. 1 ст. 6 152-ФЗ, ст. 6 115-ФЗ).

2.6. Связь с иными документами

Настоящая Политика связана и является неотъемлемой частью:

- Пользовательского соглашения Платформы GetCrypto [ссылка].
- Политики AML/CFT Платформы GetCrypto [ссылка]
- Политики в отношении Cookie-Файлов [ссылка].

3. КАТЕГОРИИ ПДн, ЦЕЛИ И УСЛОВИЯ ОБРАБОТКИ

3.1. Пользователи

3.1.1. Состав данных:

- Email, ФИО, логин.

3.1.2. Цели обработки:

- Регистрация и вход на платформу;
- Техническая поддержка;
- Предоставление возможности публикации Контента Пользователя (отзывов, оценок) в отношении Операторов ОП;
- Идентификация автора Контента Пользователя через логин (имя пользователя) в публичном доступе.
- Публикация логина Пользователя в качестве автора Контента (отзывов) на Платформе.
- Информирование о безопасности аккаунта;
- Противодействие мошенничеству (в рамках функционала платформы);
- Использование автоматически собираемых данных (cookie, логи) для анализа поведения пользователей и улучшения функциональности Платформы (см. Политику Cookie).

3.1.3. Способы обработки:

- Использование cookie-файлов и веб-маяков для обеспечения работы Платформы (детали см. в Политике Cookie);
- Хранение в зашифрованном виде (ст. 19 152-ФЗ). Шифрование данных алгоритмом AES-256;
- Обезличивание логина при удалении аккаунта методом введения идентификаторов с использованием необратимого алгоритма хэширования с "солью" (salt). При этом:
 - (i) Каждому логину присваивается уникальный идентификатор вида «Пользователь №[хэш-сумма]»;
 - (ii) Процесс обезличивания является необратимым и не позволяет восстановить оригинальный логин даже при наличии дополнительной информации;
 - (iii) Таблица соответствия оригиналов и идентификаторов не создается и не хранится;
 - (iv) Идентификаторы генерируются с использованием криптографически безопасного генератора случайных чисел.

3.1.4. Срок хранения:

Персональные данные (ФИО, email) хранятся до удаления учетной записи Пользователя. После удаления аккаунта данные уничтожаются в течение 6 месяцев, за исключением случаев, предусмотренных законодательством (например, для разрешения споров)

3.1.5. Передача третьим лицам:

- Не осуществляется. AML/CFT проводят Операторы ОП.

3.2. Представители Операторов обменных пунктов

3.2.1. Состав данных:

- ФИО, паспорт (скан), ИНН, дата рождения, адрес регистрации;
- Реквизиты счета (для ИП/юрлиц), телефон, email;
- Документы о полномочиях (для бенефициаров и руководителей).

3.2.2. Цели обработки:

- Листинг и верификация (KYC/KYB);
- Проведение AML/CFT-аудита;
- Регулярный аудит;
- Передача данных в Росфинмониторинг при нарушениях (ст. 7 115-ФЗ).

3.2.3. Способы обработки:

- **Верификация документов:**

- (i) Смешанный способ: с помощью автоматизированных систем и ручная проверка сканов паспорта и учредительных документов уполномоченными сотрудниками;
- (ii) Сверка данных с ЕГРЮЛ/ЕГРИП.
- **Шифрование:**
 - (i) Хранение сканов паспортов в зашифрованном хранилище с доступом по ролевой модели.
- **Аудит:**
 - (i) Ежеквартальные проверки систем защиты;
 - (ii) Ежегодный внешний аудит на соответствие 152-ФЗ и 115-ФЗ.

3.2.4. Срок хранения:

- 5 лет после прекращения сотрудничества (ст. 7.3 115-ФЗ).

3.2.5. Передача третьим лицам:

- **Обязательная передача:** в Росфинмониторинг при выявлении подозрительных операций.

4. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Права Пользователей (физических лиц)

4.1.1. Пользователь вправе:

- **Право на доступ** (ст. 14 152-ФЗ):
 - (i) Получить подтверждение факта обработки ПДн;
 - (ii) Запросить копию обрабатываемых данных, включая цели, сроки и источники их получения;
 - (iii) Получить информацию о типах cookie, используемых на Платформе, можно в Политике Cookie.
- **Право на исправление** (ст. 14 152-ФЗ):
 - (i) Самостоятельно корректировать данные в Личном кабинете (например, email или логин);
 - (ii) В иных случаях (например, изменение ФИО) — направить запрос через форму обратной связи или email [ссылка]
- **Право на удаление («право на забвение»)** (ст. 21 152-ФЗ):
 - (i) Удалить Учетную запись через настройки профиля, что приведет к обезличиванию данных;
 - (ii) Запросить удаление Контента (отзывов, комментариев) в течение **7 рабочих дней** через Личный кабинет или email.

Примечание: запросы на удаление данных могут быть отклонены в случаях, когда их выполнение нарушает законные интересы GetCrypto (например, при необходимости сохранения доказательств транзакций).

- **Отзыв согласия на обработку:**
 - (i) Отказаться от рассылки, нажав ссылку «Отписаться» в полученном письме;
 - (ii) Для отключения сбора данных через cookie-файлы воспользуйтесь настройками браузера или формой управления cookie на Платформе. Подробнее см. раздел 5 Политики Cookie;
 - (iii) Для полного отзыва согласия — направить запрос на email [ссылка]
- **Право на ограничение обработки** (ст. 21 152-ФЗ):
 - (i) Заблокировать обработку, если:
 - Точность данных оспаривается (на время проверки);
 - Обработка незаконна, но удаление данных не требуется.

Платформа использует аналитические инструменты cookie и трекеры (Yandex.Metrica) для отслеживания паттернов использования сервиса, согласно Политике Cookie. Пользователи могут отключить сбор данных через настройки браузера

4.1.2. Общий порядок реализации прав:

- Запросы направляются:
 - (i) Через форму в Личном кабинете;
 - (ii) По email: [ссылка]
- Для подтверждения личности предоставляется:

- (i) Копия паспорта (страницы с ФИО и регистрацией) или электронная подпись;
 - (ii) Для запросов от Операторов ОП — доверенность/приказ, подтверждающий полномочия.
- Срок ответа: 30 дней с момента получения запроса и подтверждения личности (ст. 14 152-ФЗ).

Основания для отказа:

GetCrypto вправе отказать в выполнении запроса, если:

- Запросы носят необоснованно повторяющийся или систематический характер;
- Выполнение требует непропорциональных технических усилий;
- Реализация угрожает конфиденциальности данных других лиц.

Отказ предоставляется в письменной форме с указанием мотивированных причин.

4.2. Права Операторов ОП (юридических лиц/ИП)

4.2.1. Оператор ОП вправе:

- Запросить информацию о составе, целях и сроках обработки ПДн своих представителей;
- Получить сведения о передаче данных третьим лицам.

4.2.2. Порядок реализации:

- Запрос направляется уполномоченным представителем на email, указанный в договоре с GetCrypto;
- К запросу прилагаются реквизиты договора и документы, подтверждающие полномочия.

Срок ответа на запросы: 30 дней с момента получения (ст. 14 152-ФЗ).

5. ЗАЩИТА ПДн

5.1. Общие принципы

GetCrypto реализует технические и организационные меры защиты персональных данных в соответствии с:

- Статьей 19 Федерального закона № 152-ФЗ;
- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных»;
- Приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

5.2. Автоматизированная обработка

В большинстве случаев персональные данные обрабатываются автоматически без доступа сотрудников. Ручная обработка (например, верификация документов представителей Операторов ОП) осуществляется только уполномоченными сотрудниками, прошедшими соответствующее обучение и подписавшими соглашение о конфиденциальности.

5.3. Технические меры защиты

GetCrypto применяет следующие меры:

5.3.1. Шифрование данных:

- При передаче: TLS 1.2+ с использованием сертификатов, выпущенных аккредитованными Минцифры РФ удостоверяющими центрами;
- При хранении: алгоритм AES-256 для баз данных и сканов документов.

5.3.2. Контроль доступа:

- Двухфакторная аутентификация (2FA) для сотрудников;
- Ролевая модель доступа (на основе принципа минимальных привилегий).

5.3.3. Защита инфраструктуры:

- Межсетевые экраны (Next-Generation Firewalls) с фильтрацией трафика;
- Система обнаружения вторжений (IDS) с ежедневным мониторингом.

Система защиты данных соответствует требованиям: ГОСТ Р 56938-2016; Приказа ФСТЭК России № 21.

5.3.4. Обезличивание:

- Использование алгоритмов хэширования с 'солью' для обезличивания персональных данных с обеспечением необратимости преобразования. Логины пользователей в опубликованном Контенте заменяются на уникальные идентификаторы (например, «Пользователь №12345») при удалении аккаунта.

5.4. Организационные меры защиты

5.4.1. Обучение сотрудников:

- Ежегодные тренинги по 152-ФЗ и внутренним политикам;
- Тестирование знаний в сфере защиты данных.

5.4.2. Аудит и мониторинг:

- Ежеквартальные внутренние проверки систем защиты;
- Ежегодный независимый аудит на соответствие ISO 27001 и требованиям 152-ФЗ.

5.4.3. Резервное копирование:

- Ежедневное резервное копирование данных представителей Операторов ОП;
- Хранение резервных копий только на территории РФ в течение 90 дней.

5.4.4. Реагирование на инциденты:

- Внутренний регламент при утечках данных (срок уведомления Роскомнадзора — не позднее 72 часов с момента обнаружения).

5.5. Требования к третьим лицам

В случае привлечения подрядчиков для обработки данных (например, хостинг-провайдеров):

- Заключается договор, обязывающий соблюдать 152-ФЗ;
- Проводится оценка их соответствия требованиям Постановления № 1119.

6. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ

6.1. Общие условия передачи

GetCrypto передает персональные данные третьим лицам только в случаях, предусмотренных законодательством РФ, или при наличии согласия субъекта ПДн (ст. 6, 7 152-ФЗ).

6.2. Передача данных Пользователей (физических лиц)

6.2.1. Принципы передачи:

- Персональные данные Пользователей (ФИО, email) **не передаются третьим лицам**, за исключением:
 - (i) Обезличенного логина (имени учетной записи) в составе Контента (отзывов, оценок), который не позволяет установить личность (ст. 3 152-ФЗ);
 - (ii) Обезличенные данные, не являющиеся персональными, собранные с помощью cookie, могут передаваться рекламным и аналитическим партнерам (Яндекс.Метрика). Подробнее см. раздел 3.3 Политики Cookie;

6.2.2. Ответственность за AML/CFT:

- Проведение проверок Пользователей (KYC/AML) и передача их данных в Росфинмониторинг осуществляются Операторами ОП, а не GetCrypto.

6.3. Передача данных представителей Операторов ОП

6.3.1. Обязательная передача в государственные органы (ст. 7 115-ФЗ):

- Данные передаются в Росфинмониторинг при выявлении подозрительных операций.

Состав передаваемых данных:

- (i) ФИО, паспортные данные (серия, номер, дата выдачи);
- (ii) Описание нарушений (с указанием статей 115-ФЗ).

Порядок передачи:

- (i) Через защищенный канал связи (VPN с шифрованием TLS 1.3);

- (ii) С оформлением сопроводительного письма за подписью уполномоченного сотрудника GetCrypto.

Согласие не требуется — передача является обязанностью GetCrypto по закону.

6.3.2. Передача третьи лицам - поставщикам услуг:

Данные могут передаваться:

- **Хостинг-провайдерам** — для хранения на серверах в РФ на основании договора поручения обработки персональных данных (ч. 3 ст. 6 152-ФЗ). Договор предусматривает:
 - Соблюдение субподрядчиками требований 152-ФЗ и настоящей Политики;
 - Запрет на использование данных вне целей, прямо указанных в договоре;
 - Обязательство обеспечивать конфиденциальность и защиту данных.
- **Платежным системам** — передаются только реквизиты счета Оператора ОП при проведении лицензионных платежей (для ИП/юрлиц).

6.4. Требования к третьим лицам

Все третьи лица обязаны:

- Обрабатывать данные **исключительно в рамках договора** (ч. 3 ст. 6 152-ФЗ);
- Соблюдать конфиденциальность и обеспечивать защиту данных в соответствии с 152-ФЗ, 149-ФЗ и 187-ФЗ «О безопасности критической информационной инфраструктуры»;
- Уничтожить данные по истечении срока действия договора или по требованию Оператора.

Договоры с третьими лицами включают:

- Перечень допустимых операций с данными;
- Санкции за нарушение условий обработки.

7. ХРАНЕНИЕ И ЛОКАЛИЗАЦИЯ ДАННЫХ

7.1. Сроки хранения

7.1.1. Для Пользователей (физических лиц):

- **Персональные данные** (ФИО, email) хранятся **до удаления учетной записи**, за исключением случаев, когда:
 - (i) Закон требует продлить срок (например, для исполнения судебных решений, ст. 21 152-ФЗ);
 - (ii) Данные необходимы для разрешения споров (максимально — **6 месяцев** с момента удаления аккаунта).
- **Обезличенные данные** (логины в опубликованных отзывах) хранятся **бессрочно** в формате, исключающем идентификацию личности (например, «Пользователь №12345»);
- **Автоматически собираемые данные** (например, cookie), не являющиеся Персональными данными, хранятся в соответствии с Политикой Cookie.

7.1.2. Для представителей Операторов ОП:

- Данные (паспорт, ИНН, реквизиты) хранятся **5 лет** с момента прекращения договора (ст. 7.3 115-ФЗ; ст. 23 НК РФ).

7.2. Локализация данных

Все персональные данные обрабатываются и хранятся **исключительно на территории РФ** на серверах в дата-центре уровня Tier III (Москва), соответствующем требованиям:

- ГОСТ Р 56938–2016 от 06.12.2018 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»;
- Приказа ФСТЭК России от 18.02.2013 № 21

7.3. Уничтожение данных

Порядок уничтожения:

7.3.1. **Обезличивание:**

- Логины Пользователей заменяются на уникальные идентификаторы, полученные путем необратимого хэширования с добавлением уникальной «соли» (salt) (например, «Пользователь №[хэш-сумма]»);
- Процесс обезличивания обеспечивает невозможность восстановления оригинальных логинов;
- После процедуры обезличивания все исходные данные подлежат необратимому удалению.

Обезличивание осуществляется методами, соответствующими Приказу Роскомнадзора № 996.

7.3.2. Физическое стирание: Данные удаляются с носителей с использованием методов, соответствующих стандарту NIST SP 800–88 (гарантированное удаление без возможности восстановления).

7.3.3. Документирование: Составляется акт об уничтожении, подписанный уполномоченным сотрудником и ответственным за информационную безопасность.

Сроки уничтожения:

- Для Пользователей — в течение 30 дней после истечения срока хранения;
- Для Операторов ОП — не позднее 10 рабочих дней после истечения 5-летнего срока.

7.4. Исключения

GetCrypto вправе сохранить данные дольше установленных сроков **только**:

- По требованию регуляторов (например, Росфинмониторинга) в рамках проверок;
- Для исполнения судебных решений или разрешения споров.

7.5. Отказ от ответственности

- GetCrypto не обязан хранить данные бессрочно и не несет ответственности за их уничтожение по истечении установленных сроков.

8. ОТВЕТСТВЕННОСТЬ И ОГРАНИЧЕНИЯ

8.1. Ограничения ответственности GetCrypto

GetCrypto принимает все необходимые и достаточные меры защиты персональных данных в соответствии со ст. 19 № 152-ФЗ, Постановлением Правительства РФ № 1119, включая использование сертифицированных средств защиты, шифрование данных и регулярный аудит безопасности.

При этом **GetCrypto** не гарантирует абсолютную защиту от несанкционированного доступа, утечек или иных нарушений, возникших вне зоны контроля Платформы.

- **Пользователь обязан:**
 - (i) Использовать сложные пароли и не передавать их третьим лицам;
 - (ii) Немедленно уведомлять GetCrypto о подозрениях в компрометации учетной записи [ссылка]
- **GetCrypto не несет ответственности:**
 - (i) За безопасность данных, переданных через ненадежные каналы связи (например, email, SMS) после их отправки;
 - (ii) За последствия, вызванные действиями/бездействием Пользователя (нарушение правил безопасности, утрата пароля).

8.1.2. Контент Пользователя:

- Пользователь несет исключительную ответственность за достоверность и законность размещаемого Контента (отзывов, комментариев). GetCrypto вправе:
 - (i) Удалить Контент, нарушающий законодательство РФ (например, содержащий персональные данные третьих лиц без согласия);
 - (ii) Заблокировать Учетную запись за массовое размещение фейковых отзывов или спама.
- GetCrypto не проверяет достоверность Контента, но проводит модерацию:
 - (i) Автоматическую проверку всех материалов в течение 24 часов;
 - (ii) Ручную проверку при выявлении подозрений (срок — до 72 часов).

8.1.3. Технические сбои:

GetCrypto принимает все разумные меры для обеспечения доступности, целостности и защиты данных в соответствии с ст. 19 152-ФЗ, включая:

- Регулярное тестирование систем на устойчивость к DDoS-атакам;
- Использование сертифицированных средств защиты информации.

Однако GetCrypto не несет ответственности за:

- (i) Перебои в работе Платформы, вызванные обстоятельствами непреодолимой силы (масштабные DDoS-атаки, действия третьих лиц, форс-мажор), при условии, что Оператор (GetCrypto) выполнил требования ст. 19 152-ФЗ;
- (ii) Искажение данных, возникшее из-за использования Пользователем устаревших версий ПО или ненадежных каналов связи.

8.2. Запрещенные действия

8.2.1. Пользователям запрещено:

- Использовать Платформу для незаконных целей (включая отмывание денег, финансирование терроризма);
- Размещать Контент, нарушающий права третьих лиц (например, персональные данные без согласия);
- Создавать множественные Учетные записи для манипуляции рейтингами Обменных пунктов;
- Передавать логины/пароли третьим лицам или использовать ботов для автоматизации взаимодействия.

Последствия нарушений: Удаление Контента и блокировка Учетной записи.

8.3. Территориальные ограничения

- Обработка данных осуществляется только на территории РФ. Пользователи из юрисдикций, где использование Платформы запрещено (например, страны, внесенные в список ФАТФ), несут ответственность за соблюдение локальных законов.

8.4. Модерация и управление Контентом

Правила модерации:

8.4.1. Контент проверяется на соответствие требованиям законодательства РФ и внутренним правилам Платформы, включая:

152-ФЗ:

- Запрет на распространение ПДн третьих лиц без их согласия (ст. 7);
- Соблюдение принципов законности и конфиденциальности обработки ПДн.

115-ФЗ (противодействие AML/CFT):

- Блокировка контента, связанного с легализацией доходов, финансированием терроризма, мошенническими схемами.

149-ФЗ (ст. 15.1–15.7):

- Удаление информации, призывающей к насилию, экстремизму, разжигающей межнациональную рознь;
- Блокировка материалов, содержащих детскую порнографию, пропаганду наркотиков, иной запрещенной информации.

436-ФЗ (защита детей от вредоносной информации):

- Ограничение доступа к контенту, нарушающему возрастные ограничения.

Пользовательское соглашение:

- Запрет на спам, коммерческую рекламу без согласия, размещение вредоносного ПО.

8.4.2. По итогам проверки Контент может быть:

- **Одобен** (если соответствует требованиям);
- **Отклонен с уведомлением автора** (с указанием нарушенных норм);
- **Заблокирован** (при наличии признаков незаконности до предоставления доказательств легальности).

Сроки реагирования на жалобы:

8.4.3. В случае поступления жалобы на незаконный контент от Пользователей или уполномоченных органов (Роскомнадзор, Росфинмониторинг):

- Предварительная проверка проводится в течение **24 часов** (ст. 15.7 149-ФЗ);
- При подтверждении нарушения контент блокируется незамедлительно, но не позднее **1 рабочего дня** с момента жалобы.

Обжалование решений:

8.4.4. Пользователь вправе обжаловать блокировку через службу поддержки в течение **7 дней** с момента уведомления.

- Срок рассмотрения апелляции — **10 рабочих дней** (с направлением мотивированного ответа).
- Если блокировка подтверждена, контент остается недоступным. В случае отмены решения доступ восстанавливается в течение **3 рабочих дней**.

Примечание:

- При обработке жалоб GetCrypto руководствуется положениями ст. 10.1–10.3 149-ФЗ (порядок ограничения доступа к информации).
- Пользователь несет ответственность за достоверность предоставляемых данных (ст. 13.11 КоАП РФ).

8.5. Исключения ответственности

GetCrypto не отвечает за:

- Действия Операторов ОП (проведение транзакций, AML-проверки);
- Ущерб, вызванный передачей Пользователем данных третьим лицам;
- Использование данных из открытых источников (например, обезличенных логинов в отзывах).

8.6. Ответственность за предоставление данных

Для Операторов ОП:

- GetCrypto не несет ответственности за последствия, связанные с предоставлением недостоверных данных (например, недействительные паспорта, поддельные документы о полномочиях). При выявлении нарушений доступ к Платформе может быть приостановлен без компенсации убытков;
- Операторы ОП обязаны своевременно обновлять данные своих представителей и бенефициаров. GetCrypto вправе запросить актуальные документы в любой момент.

8.7. Риски, связанные с использованием данных доступа

GetCrypto не отвечает за:

- Ущерб, вызванный передачей логинов/паролей третьим лицам
- Потери данных

из-за несоблюдения рекомендаций по безопасности (например, использование слабых паролей, отсутствие антивирусного ПО).

8.8. Проверка данных и приостановка доступа

GetCrypto вправе:

- Проводить внеплановые проверки данных Операторов ОП (включая запрос документов от третьих лиц);
- Блокировать доступ к Платформе при подозрении в мошенничестве или нарушении AML/CFT-требований.

9. АВТОМАТИЧЕСКИ СОБИРАЕМЫЕ ДАННЫЕ

Платформа использует технологии автоматического сбора данных - cookie-файлы, логи сервера, веб-маяки и аналогичные технологии для анализа поведения Пользователей, улучшения функциональности, персонализации контента, обеспечения безопасности и показа релевантной рекламы. Эти данные не содержат персональной информации, но могут использоваться в сочетании с ней.

Подробная информация о типах cookie, сроках хранения, целях их использования и управлении настройками доступна в Политике Cookie: [\[ссылка\]](#)

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Срок действия и изменения в Политике:

GetCrypto оставляет за собой право вносить изменения в настоящую Политику, в том числе при изменении законодательства. Изменения вступают в силу через 10 дней после их публикации на Платформе. В исключительных случаях (требования регуляторов) — немедленно.

Пользователи и Операторы ОП уведомляются об изменениях по e-mail.

10.2. Разрешение споров:

Споры, возникающие в связи с применением настоящей Политики, разрешаются в судах Российской Федерации по месту нахождения GetCrypto.

10.3. Контакты

- Электронная почта: [ссылка]
- Форма обратной связи на сайте.

Вопросы, связанные с использованием cookie, направляйте на email: [ссылка]

Дата вступления в силу: [дата]

Версия Политики: 1.0