Политика конфиденциальности и использования cookies Mirocard
Дата последнего обновления: 23.04.2026

1. Введение
Настоящая Политика конфиденциальности и использования cookies Mirocard (далее - **«Политика»**) описывает, какие персональные данные мы собираем, для каких целей их используем, кому можем передавать, как защищаем данные, как используем cookies и какие права есть у пользователя.
Настоящая Политика применяется к пользователям сайта, личного кабинета, платформы Mirocard, карточного функционала, процедур KYC/KYB/AML, службы поддержки и иных связанных сервисов Mirocard.

Для целей настоящей Политики **Mirocard** означает сервис, предоставляемый компанией **InnovativeTechnologies OÜ**.

Mirocard не является банком, платежным учреждением, эмитентом электронных денег, депозитарием, кастодианом или хранителем средств пользователя. Обработка данных, связанных с виртуальными картами, операциями, доступной суммой, проверками, пополнениями и карточным функционалом, может осуществляться с участием сторонних провайдеров, включая эмитентов, карточные программы, процессинг, платежные системы, KYC/KYB/AML-провайдеров, blockchain analytics providers, крипто-инфраструктурных провайдеров и иных обязательных участников инфраструктуры.
Использование сервиса Mirocard означает, что пользователь ознакомился с настоящей Политикой.

2. Какие данные мы собираем
Мы собираем и обрабатываем персональные данные в объеме, необходимом для предоставления сервиса, идентификации пользователей, соблюдения требований комплаенса, предотвращения мошенничества, обеспечения безопасности, обработки операций и выполнения правовых обязанностей.
2.1. Регистрационные и контактные данные
Мы можем обрабатывать:
• имя и фамилию;
• адрес электронной почты;
• номер телефона;
• страну проживания;
• гражданство, если применимо;
• адрес проживания или регистрации, если применимо;
• данные аккаунта;
• язык интерфейса и коммуникации;
• историю обращений в службу поддержки;
• иные данные, предоставленные пользователем при регистрации или использовании сервиса.
2.2. KYC/KYB и AML-данные
Для идентификации, верификации, санкционного скрининга, AML/CFT-проверок, fraud-prevention и иных compliance-целей мы можем обрабатывать:
• данные документа, удостоверяющего личность;
• копии, изображения или реквизиты документов;
• дату рождения;
• гражданство;
• адрес проживания;
• селфи, liveness-проверку, видеопроверку или иные данные, необходимые для подтверждения личности;
• сведения о статусе PEP, санкционных совпадениях и adverse media;
• сведения об источнике средств, источнике благосостояния и цели использования сервиса;
• корпоративные данные юридического лица;
• данные представителей, директоров, акционеров и бенефициарных владельцев;
• документы, подтверждающие структуру собственности, полномочия представителей или источник средств;
• результаты KYC/KYB/AML-проверок и внутренней оценки риска.
Если селфи, liveness-проверка, видеоидентификация или иные данные используются способом, который в соответствии с применимым законодательством считается обработкой биометрических данных, такая

обработка осуществляется только при наличии применимого правового основания и дополнительных условий, предусмотренных законодательством о защите данных.

2.3. Данные о карточном функционале и операциях

В связи с использованием виртуальных карт мы можем обрабатывать:

• сведения о выпущенных виртуальных картах;
• статус карты;
• BIN и карточную программу;
• лимиты и применимые ограничения;
• историю операций;
• данные об успешных, отклоненных, отмененных и спорных операциях;
• данные о попытках операций;
• данные о возвратах, reversal, dispute, chargeback и обращениях пользователя;
• информацию о доступной сумме, отображаемой в интерфейсе;
• сведения о комиссиях;
• данные о мерчанте, MCC, валюте, сумме, дате и статусе операции;
• данные, необходимые для рассмотрения спорных, подозрительных или несанкционированных операций.

Отображение доступной суммы или истории операций в интерфейсе Mirocard не означает, что Mirocard хранит средства пользователя.

2.4. Данные о криптовалютном пополнении

Если пользователю доступно криптовалютное пополнение карточного функционала, мы можем обрабатывать:

• тип криптоактива;
• blockchain network;
• адреса отправки и получения;
• transaction hash;
• сумму операции;
• статус обработки;
• результаты blockchain analytics и compliance screening;
• сведения о кошельках, связанных адресах и источнике средств;
• данные, необходимые для проверки источника средств и предотвращения незаконного использования сервиса.

Mirocard не предоставляет кастодиальное хранение криптоактивов пользователя в рамках настоящего сервиса.

2.5. Технические данные

При использовании сайта, платформы и личного кабинета мы можем автоматически собирать:

• IP-адрес;
• тип и версию браузера;
• тип устройства;
• операционную систему;
• идентификаторы устройства, браузера или сессии;
• дату и время входа;
• данные о действиях пользователя в интерфейсе;
• логи безопасности;
• сведения об ошибках, сбоях и технических событиях;
• данные геолокационного характера, если они доступны на основании технических сигналов или разрешений пользователя;
• признаки использования VPN, proxy, TOR или иных технических средств, если это необходимо для безопасности и compliance-целей.

2.6. Cookies и аналогичные технологии

Мы можем использовать cookies, local storage, pixels, tags, идентификаторы сессии и аналогичные технологии. Подробнее об этом указано в разделе 8 настоящей Политики.

2.7. Данные, полученные от третьих лиц

Мы можем получать данные о пользователе от третьих лиц, если это необходимо для предоставления сервиса, проверки пользователя, обработки операций, предотвращения мошенничества или выполнения compliance-требований.

Такие источники могут включать:

• KYC/KYB/AML-провайдеров;
• sanctions, PEP и adverse media screening providers;
• blockchain analytics providers;
• эмитентов, карточные программы, BIN-партнеров, процессинг и платежные системы;
• fraud-prevention providers;
• государственные органы, суды, регуляторов или правоохранительные органы, если применимо;
• иных партнеров и участников инфраструктуры Mirocard.

3. Для каких целей мы обрабатываем данные

Мы обрабатываем персональные данные для следующих целей.

3.1. Предоставление сервиса

Мы используем данные для:
• регистрации и управления аккаунтом;
• предоставления доступа к личному кабинету;
• обработки заявок на выпуск виртуальных карт;
• отображения статуса карт, операций, лимитов и доступной суммы;
• предоставления поддержки;
• выполнения действий, запрошенных пользователем;
• администрирования пользовательских настроек и коммуникаций.

3.2. KYC/KYB, AML/CFT, санкции и комплаенс

Мы используем данные для:
• идентификации и верификации пользователей;
• проверки юридических лиц и бенефициарных владельцев;
• санкционного скрининга;
• PEP/adverse media screening;
• оценки AML/CFT, fraud, sanctions, regulatory и иных compliance-рисков;
• мониторинга операций;
• проверки источника средств и источника благосостояния;
• предотвращения обхода санкций, мошенничества и незаконной деятельности;
• выполнения требований партнеров, эмитентов, карточных программ, процессинга и иной инфраструктуры.

3.3. Работа виртуальных карт и операций

Мы используем данные для:
• выпуска, активации и обслуживания виртуальных карт;
• обработки операций;
• применения лимитов и комиссий;
• рассмотрения отклоненных транзакций;
• обработки refund, reversal, dispute и chargeback;
• взаимодействия с эмитентами, карточными программами, BIN-партнерами, процессингом, платежными системами и иными участниками инфраструктуры.

3.4. Безопасность и предотвращение злоупотреблений

Мы используем данные для:
• защиты аккаунтов;
• выявления подозрительной активности;
• предотвращения несанкционированного доступа;
• расследования fraud, abuse, card testing, account takeover и chargeback abuse;
• предотвращения обхода KYC/KYB, санкционных, территориальных, BIN, MCC, лимитных и иных ограничений;
• обеспечения технической, операционной и информационной безопасности сервиса.

3.5. Аналитика и улучшение сервиса

Мы можем использовать технические, статистические, агрегированные или обезличенные данные для:
• анализа работы сайта и платформы;
• улучшения пользовательского интерфейса;
• исправления ошибок;
• повышения надежности и безопасности сервиса;
• оценки эффективности отдельных функций;
• развития и оптимизации продукта.

3.6. Коммуникации
Мы можем использовать контактные данные для:
• отправки сервисных уведомлений;
• сообщений о безопасности;
• уведомлений об изменениях документов;
• ответов на обращения пользователя;
• сообщений о статусе проверок, операций, карт или споров;
• иных обязательных, технических или операционных сообщений.
Маркетинговые сообщения направляются только при наличии надлежащего правового основания и с возможностью отказаться от их получения.
3.7. Защита прав и выполнение обязанностей
Мы можем использовать данные для:
• соблюдения применимого законодательства;
• ведения бухгалтерского, налогового и операционного учета;
• реагирования на запросы компетентных органов;
• урегулирования претензий и споров;
• защиты прав, законных интересов и безопасности Mirocard, пользователей, партнеров и третьих лиц.

4. Правовые основания обработки
Мы обрабатываем персональные данные только при наличии применимого правового основания.
4.1. Исполнение договора
Мы обрабатываем данные, когда это необходимо для предоставления пользователю доступа к сервису, аккаунту, виртуальным картам, операциям, поддержке и связанному функционалу.
4.2. Выполнение правовых обязанностей
Мы обрабатываем данные, когда это необходимо для соблюдения требований законодательства, включая требования по KYC/KYB, AML/CFT, санкциям, реагированию на запросы компетентных органов и выполнению иных правовых обязанностей.
4.3. Законный интерес
Мы можем обрабатывать данные на основании законного интереса Mirocard, пользователей, партнеров или третьих лиц, включая:
• предотвращение мошенничества;
• обеспечение безопасности сервиса;
• защиту прав и законных интересов;
• улучшение сервиса;
• управление рисками;
• расследование нарушений;
• защиту от претензий;
• обеспечение стабильной работы платформы и карточного функционала.
При обработке данных на основании законного интереса мы учитываем баланс между такими интересами и правами пользователя.
4.4. Согласие
Мы используем согласие пользователя, когда это требуется законом, например для отдельных cookies, маркетинговых коммуникаций или иных видов обработки, которые требуют согласия.
Пользователь может отозвать согласие в любое время. Отзыв согласия не влияет на законность обработки, которая была осуществлена до его отзыва.
4.5. Специальные категории данных
Если в рамках liveness-проверки, видеоидентификации, проверки документов или иных процедур обрабатываются данные, которые могут считаться специальными категориями персональных данных, такая обработка осуществляется только при наличии применимого правового основания.
4.6. Защита жизненно важных интересов и публичный интерес
В исключительных случаях мы можем обрабатывать данные, если это необходимо для защиты жизненно важных интересов лица или выполнения задачи в общественных интересах, если такое основание применимо.

5. Кому мы передаем данные
Мы можем передавать персональные данные третьим лицам только в объеме, необходимом для целей, указанных в настоящей Политике.

В зависимости от обстоятельств такие третьи лица могут выступать самостоятельными контролерами, совместными контролерами или обработчиками данных. Их роль определяется характером обработки, договорными условиями и применимым законодательством.

5.1. KYC/KYB/AML-провайдеры

Мы можем передавать данные провайдерам идентификации, верификации, санкционного скрининга, PEP/adverse media screening, blockchain analytics, fraud-prevention и иных compliance-проверок.

5.2. Эмитенты, карточные программы и процессинг

Мы можем передавать данные эмитентам, BIN-партнерам, карточным программам, процессинговым провайдерам, платежным системам и иным участникам карточной инфраструктуры для выпуска, обслуживания, обработки, ограничения, мониторинга и закрытия виртуальных карт и операций.

5.3. Крипто-инфраструктурные провайдеры

Если пользователь использует криптовалютное пополнение или связанные функции, данные могут передаваться провайдерам, участвующим в обработке, проверке, конвертации, compliance-анализе или техническом сопровождении таких операций.

5.4. Технические поставщики

Мы можем передавать данные поставщикам хостинга, облачной инфраструктуры, аналитики, кибербезопасности, email-рассылок, CRM, поддержки пользователей, мониторинга, логирования и иных технических сервисов.

5.5. Юридические и профессиональные консультанты

Мы можем передавать данные юристам, аудиторам, бухгалтерам, консультантам и иным профессиональным советникам, если это необходимо для защиты прав, выполнения обязательств, управления рисками или ведения деятельности Mirocard.

5.6. Государственные органы и обязательные получатели

Мы можем раскрывать данные государственным органам, судам, регуляторам, правоохранительным органам, финансовой разведке, санкционным органам или иным обязательным получателям, если это требуется законом, запросом компетентного органа или необходимо для защиты прав Mirocard, пользователей, партнеров или третьих лиц.

6. Международная передача данных

С учетом международного характера сервиса, карточной инфраструктуры, KYC/KYB/AML-провайдеров, blockchain analytics providers, эмитентов, процессинга, карточных программ, крипто-инфраструктурных провайдеров и технических поставщиков персональные данные пользователя могут передаваться и обрабатываться за пределами страны проживания пользователя, включая страны за пределами Европейской экономической зоны.

Если данные передаются в страну, которая не обеспечивает надлежащий уровень защиты персональных данных, мы применяем предусмотренные законом механизмы защиты, которые могут включать:

• стандартные договорные условия;
• договорные обязательства с получателями данных;
• технические и организационные меры безопасности;
• оценку рисков передачи данных;
• иные допустимые safeguards, предусмотренные применимым законодательством.

7. Как мы защищаем данные

Мы применяем технические и организационные меры для защиты персональных данных от несанкционированного доступа, раскрытия, изменения, утраты, уничтожения или неправомерного использования.

Такие меры могут включать:

• шифрование передачи данных;
• контроль доступа;
• двухфакторную аутентификацию;
• журналирование действий;
• ограничение доступа по ролям;
• мониторинг подозрительной активности;
• резервное копирование;
• проверку поставщиков;
• внутренние процедуры безопасности;
• обучение сотрудников и подрядчиков;
• договорные обязательства по конфиденциальности и защите данных.

Несмотря на принимаемые меры, ни один способ передачи или хранения данных не может быть полностью безопасным. Пользователь обязан соблюдать правила безопасности аккаунта, использовать надежный пароль, не передавать данные доступа третьим лицам и своевременно сообщать о подозрительной активности.
В случае нарушения безопасности персональных данных мы примем меры для оценки инцидента, минимизации возможного ущерба и уведомления пользователей или компетентных органов, если такое уведомление требуется применимым законодательством.

8. Cookies и аналогичные технологии

8.1. Что такое cookies

Cookies - это небольшие файлы, которые сохраняются на устройстве пользователя при посещении сайта или использовании платформы. Аналогичные технологии могут включать local storage, pixels, tags, SDK, идентификаторы устройства и идентификаторы сессии.

8.2. Какие cookies мы используем

Мы можем использовать следующие категории cookies.

Обязательные cookies

Необходимы для работы сайта и платформы, включая авторизацию, безопасность, управление сессией, предотвращение мошенничества и доступ к защищенным разделам. Эти cookies не требуют отдельного согласия, если они строго необходимы для предоставления сервиса, запрошенного пользователем.

Функциональные cookies

Помогают запоминать настройки пользователя, например язык интерфейса, регион или предпочтения. Такие cookies используются при наличии применимого правового основания.

Аналитические cookies

Используются для анализа работы сайта, понимания поведения пользователей, улучшения интерфейса и качества сервиса. Если такие cookies не являются строго необходимыми, они используются только после получения согласия пользователя.

Маркетинговые cookies

Используются для показа релевантной рекламы, измерения эффективности рекламных кампаний и настройки маркетинговых коммуникаций. Такие cookies используются только после получения согласия пользователя.

8.3. Управление cookies

При первом посещении сайта пользователю может быть показан cookie-banner или центр настроек cookies.
Пользователь может:
• принять все cookies;
• отклонить необязательные cookies;
• настроить категории cookies;
• изменить или отозвать согласие в дальнейшем.
Необязательные cookies не устанавливаются до получения согласия пользователя, если такое согласие требуется законом.
Пользователь также может управлять cookies через настройки браузера. Отключение некоторых cookies может повлиять на работу отдельных функций сайта или платформы.

8.4. Отзыв согласия

Пользователь может изменить настройки cookies или отозвать согласие через доступный инструмент управления cookies, если такой инструмент доступен, либо через настройки браузера.

9. Автоматизированная обработка и оценка рисков

Для целей KYC/KYB/AML, санкционного скрининга, предотвращения мошенничества, управления рисками, безопасности и соблюдения требований карточной инфраструктуры мы можем использовать автоматизированные или частично автоматизированные инструменты анализа.
Такие инструменты могут помогать выявлять:
• санкционные совпадения;
• PEP/adverse media indicators;
• подозрительные операции;
• несоответствие риск-профилю;
• признаки fraud, abuse, account takeover или card testing;
• признаки chargeback abuse;

• связь с запрещенными или ограниченными юрисдикциями;
• признаки использования сервиса в нарушение правил, лимитов, BIN, MCC или compliance-требований.
Результаты автоматизированного или частично автоматизированного анализа могут влиять на необходимость дополнительной проверки, запрос документов, ограничение функционала, отказ в выпуске карты, приостановку операции, блокировку карты или аккаунта либо отказ в обслуживании.
Если решение принимается исключительно на основе автоматизированной обработки и создает для пользователя юридические или аналогичные существенные последствия, пользователь имеет права, предусмотренные применимым законодательством, включая право запросить участие человека в рассмотрении решения, выразить свою позицию и оспорить решение, если такие права применимы.

10. Сроки хранения данных
Мы храним персональные данные только столько времени, сколько необходимо для целей, для которых они были собраны, а также для выполнения правовых обязанностей, разрешения споров, предотвращения мошенничества, проведения проверок, обработки операций и защиты прав Mirocard.
Сроки хранения зависят от категории данных, цели обработки, применимого законодательства, требований AML/CFT, санкционного комплаенса, карточной инфраструктуры, а также необходимости защиты прав.
10.1. Данные аккаунта
Данные аккаунта хранятся в течение срока использования сервиса и после прекращения использования в течение периода, необходимого для выполнения правовых обязанностей, защиты прав, предотвращения мошенничества и урегулирования возможных претензий.
10.2. KYC/KYB/AML-данные
KYC/KYB/AML-данные, документы проверки, результаты скрининга, сведения об источнике средств, risk-profile records и связанные compliance-записи могут храниться в течение срока, установленного применимым законодательством, требованиями AML/CFT, санкционного комплаенса, карточной инфраструктуры и внутренними процедурами хранения.
10.3. Данные об операциях
Данные об операциях, виртуальных картах, доступной сумме, комиссиях, возвратах, reversal, dispute и chargeback могут храниться в течение срока, необходимого для выполнения договорных, бухгалтерских, налоговых, AML/CFT, санкционных и иных правовых обязанностей, а также для рассмотрения претензий и споров.
10.4. Технические данные
Технические логи, данные безопасности и сведения об использовании сервиса могут храниться в течение срока, необходимого для обеспечения безопасности, расследования инцидентов, предотвращения мошенничества и поддержания работы платформы.
10.5. Cookies
Срок хранения cookies зависит от их категории и конкретного назначения. Session cookies удаляются после завершения сессии, а persistent cookies могут храниться дольше в пределах срока, указанного в настройках cookies, cookie-banner или ином доступном инструменте управления cookies.
После истечения применимого срока хранения данные удаляются, обезличиваются или архивируются, если дальнейшее хранение не требуется по закону или для защиты прав.

11. Права пользователя
В зависимости от применимого законодательства пользователь может иметь следующие права в отношении своих персональных данных.
11.1. Право на доступ
Пользователь вправе запросить подтверждение того, обрабатываем ли мы его персональные данные, а также получить информацию о такой обработке и копию данных.
11.2. Право на исправление
Пользователь вправе запросить исправление неточных или неполных персональных данных.
11.3. Право на удаление
Пользователь вправе запросить удаление персональных данных, если для этого есть основания, предусмотренные законом.
Удаление может быть ограничено, если данные необходимы для выполнения правовой обязанности, KYC/KYB/AML-требований, санкционных требований, защиты прав, рассмотрения споров, предотвращения мошенничества или выполнения иных законных целей.
11.4. Право на ограничение обработки

Пользователь вправе запросить ограничение обработки данных в случаях, предусмотренных законом, например если он оспаривает точность данных или возражает против обработки.

11.5. Право на переносимость данных

Пользователь вправе получить персональные данные, предоставленные им, в структурированном, общеупотребимом и машиночитаемом формате, если это применимо и технически возможно.

11.6. Право на возражение

Пользователь вправе возражать против обработки данных, основанной на законном интересе, если у него есть основания, связанные с его конкретной ситуацией.

Пользователь вправе в любое время возражать против обработки данных для прямого маркетинга.

11.7. Право отозвать согласие

Если обработка основана на согласии, пользователь вправе отозвать согласие в любое время. Отзыв согласия не влияет на законность обработки до момента отзыва.

11.8. Права в отношении автоматизированных решений

В случаях, предусмотренных применимым законодательством, пользователь вправе запросить участие человека в рассмотрении решения, выразить свою позицию и оспорить решение, если такое решение принято исключительно на основе автоматизированной обработки и имеет юридические или аналогичные существенные последствия.

12. Как воспользоваться своими правами

Для реализации прав пользователь может связаться с нами по адресу:

Email: support@mirocard.com

Мы можем запросить дополнительную информацию для подтверждения личности пользователя и защиты данных от несанкционированного раскрытия.

Мы отвечаем на запросы без неоправданной задержки и, как правило, не позднее одного месяца с момента получения запроса. Если запрос является сложным или поступило несколько запросов, срок ответа может быть продлен еще на два месяца. В таком случае мы уведомим пользователя о продлении и причинах задержки в течение одного месяца с момента получения запроса.

Мы можем отказать в выполнении запроса полностью или частично, если такой отказ допускается применимым законодательством, например в связи с KYC/KYB/AML-обязанностями, санкционными требованиями, требованиями карточной инфраструктуры, защитой прав, расследованием мошенничества или необходимостью сохранить данные по закону.

13. Данные несовершеннолетних

Сервис Mirocard не предназначен для лиц, не достигших возраста совершеннолетия в своей юрисдикции. Мы не намеренно собираем данные несовершеннолетних. Если нам станет известно, что данные несовершеннолетнего были предоставлены без надлежащего основания, мы примем разумные меры для удаления или ограничения обработки таких данных, если иное не требуется законом.

14. Изменения настоящей Политики

Мы можем изменять настоящую Политику в связи с изменением сервиса, карточного функционала, партнерской инфраструктуры, законодательства, требований комплаенса, технических процессов или деловой практики.

Обновленная версия Политики может быть опубликована на сайте, в интерфейсе сервиса, в личном кабинете пользователя или направлена пользователю иным доступным способом.

Изменения вступают в силу с даты публикации, если в обновленной версии не указана иная дата.