Политика AML/KYC Mirocard
Дата последнего обновления: 23.04.2026

Термины и определения
Для целей настоящей Политики следующие термины используются в указанных ниже значениях, если из контекста не следует иное.
1. **Mirocard** - сервис, предоставляющий пользователям доступ к функционалу выпуска, управления и использования виртуальных карт через карточную, платежную, техническую, крипто-инфраструктурную и иную партнерскую инфраструктуру.
2. **Пользователь** - физическое или юридическое лицо, которое регистрируется в Mirocard, проходит проверку, подает заявку на выпуск виртуальной карты, использует виртуальную карту, совершает операции или иным образом получает доступ к функционалу сервиса.
3. **Виртуальная карта** - цифровой платежный инструмент, предоставляемый пользователю через Mirocard в рамках соответствующей карточной программы, BIN, эмитента, процессинга и иных участников карточной инфраструктуры. Виртуальная карта не является банковским счетом, депозитом, вкладом, кредитным продуктом, электронными деньгами или средством хранения средств у Mirocard.
4. **Доступная сумма** - сумма, отображаемая в интерфейсе сервиса и доступная для совершения операций с виртуальной картой в рамках применимой карточной программы. Отображение доступной суммы не означает, что Mirocard хранит средства пользователя или принимает их на депозит.
5. **AML/CFT** - меры по противодействию отмыванию денежных средств и финансированию терроризма, включая выявление, оценку, мониторинг, ограничение и снижение соответствующих рисков.
6. **KYC/KYB** - процедуры идентификации и проверки физических и юридических лиц, включая проверку личности, документов, корпоративных данных, представителей, структуры владения, бенефициарных владельцев, цели использования сервиса, источника средств и иных необходимых сведений.
7. **Комплаенс** - совокупность правил, процедур, проверок, ограничений и решений, направленных на соблюдение применимого законодательства, санкционных требований, требований AML/CFT, требований карточной инфраструктуры, требований партнеров и внутренних процедур управления рисками Mirocard.
8. **Комплаенс-риск** - любой AML/CFT, санкционный, мошеннический, регуляторный, карточный, операционный, репутационный или иной риск, связанный с пользователем, операцией, источником средств, юрисдикцией, мерчантом, виртуальной картой или использованием сервиса.
9. **Риск-ориентированный подход** - подход, при котором объем проверки, лимиты, доступный функционал, мониторинг, ограничения и иные комплаенс-меры определяются с учетом уровня риска конкретного пользователя, операции, юрисдикции, источника средств, карточной программы или иных обстоятельств.
10. **Риск-профиль** - оценка уровня риска пользователя, формируемая Mirocard на основании KYC/KYB-данных, юрисдикции, характера деятельности, источника средств, операций, лимитов, используемого BIN, карточной программы, санкционных, мошеннических и иных комплаенс-индикаторов.
11. **Санкционная проверка, проверка PEP и негативной информации** - проверка пользователя, связанных лиц, операций, юрисдикций, источников средств и иных данных на наличие санкционных совпадений, статуса политически значимого лица, негативной публичной информации или иных комплаенс-индикаторов.
12. **Расширенная проверка** - дополнительная проверка пользователя, операции, источника средств, юридического лица, бенефициарных владельцев или иных обстоятельств при повышенном либо неприемлемом уровне риска.
13. **Источник средств и источник благосостояния** - происхождение конкретных средств, используемых в связи с сервисом, а также происхождение общего благосостояния пользователя или бенефициарного владельца.
14. **Бенефициарный владелец** - физическое лицо, которое прямо или косвенно владеет юридическим лицом, контролирует его либо получает выгоду от его деятельности или использования сервиса.
15. **Связанное лицо** - представитель, директор, уполномоченное лицо, бенефициарный владелец, номинальное лицо, контрагент или иное лицо, связанное с пользователем, операцией, источником средств или использованием сервиса.
16. **Карточная инфраструктура** - совокупность карточной программы, BIN, эмитента, процессинга, карточной сети, партнеров карточной программы и иных участников, обеспечивающих выпуск, обслуживание и использование виртуальных карт.

17.**BIN** - идентификационный номер банковской карты или связанная с ним карточная программа, условия которой могут определять лимиты, комиссии, доступные операции, MCC-ограничения, правила обработки транзакций и иные параметры использования карты.
18.**MCC** - код категории мерчанта, используемый для классификации торговой точки или вида деятельности мерчанта.
19.**Мерчант** - торговая точка, поставщик товаров или услуг, платформа, сервис или иное лицо, у которого пользователь совершает операцию с использованием виртуальной карты.
20.**Операция** - любое действие пользователя, связанное с использованием карточного функционала, включая запрос на пополнение карточного функционала, авторизацию, оплату, отклоненную операцию, возврат, отмену, спор, chargeback или иную связанную процедуру.
21.**Мошенничество и злоупотребление** - любое неправомерное, недобросовестное, нецелевое или запрещенное использование сервиса, аккаунта, виртуальной карты, доступной суммы или иного функционала Mirocard.
22.**Высокорисковая активность** - активность, которая не соответствует риск-профилю пользователя, заявленной цели использования сервиса, экономическому смыслу операций, условиям карточной программы, BIN, MCC, лимитам или иным применимым требованиям.
23.**Запрещенная или ограниченная юрисдикция** - страна, территория или регион, обслуживание которых запрещено или ограничено Mirocard в силу применимого законодательства, санкционных режимов, требований партнеров, требований карточной инфраструктуры или внутренней оценки рисков.
24.**Ограничительные меры** - отказ в регистрации, проверке, выпуске или использовании виртуальной карты, снижение лимитов, ограничение доступного функционала, отклонение или приостановка операции, ограничение доступной суммы, блокировка аккаунта или карты, прекращение обслуживания либо иные меры, применяемые Mirocard для управления комплаенс-рисками.
25.**Партнеры** - эмитенты, карточные программы, партнеры BIN, карточные сети, KYC/AML-провайдеры, процессинговые, платежные, крипто-инфраструктурные, технические и иные обязательные участники инфраструктуры Mirocard.

1. Общие положения

1.1. Назначение Политики

Настоящая Политика AML/KYC Mirocard, далее - **«Политика»**, определяет общий подход Mirocard к идентификации и проверке пользователей, оценке рисков, санкционному контролю, мониторингу операций и предотвращению неправомерного использования сервиса.
Политика направлена на противодействие отмыванию денежных средств, финансированию терроризма, обходу санкций, мошенничеству, злоупотреблению карточной инфраструктурой, использованию незаконных, неподтвержденных или непрозрачных источников средств, а также иным действиям, создающим AML/CFT, санкционный, мошеннический, регуляторный, карточный, репутационный или иной комплаенс-риск.

1.2. Сфера применения

Политика применяется ко всем физическим и юридическим лицам, которые регистрируются в Mirocard, проходят проверку, подают заявку на выпуск виртуальной карты, используют карточный функционал, совершают операции или иным образом получают доступ к сервису.
Политика применяется совместно с Политикой использования, Политикой конфиденциальности, условиями конкретной карточной программы, условиями эмитента, процессинга, карточной сети, KYC/AML-провайдеров и иных обязательных партнеров.

1.3. Модель работы сервиса

Mirocard предоставляет пользователю доступ к карточному функционалу и интерфейсу управления виртуальными картами с использованием инфраструктуры сторонних партнеров.
Mirocard не является банком, платежным учреждением, эмитентом электронных денег, депозитарием, кастодианом, поставщиком банковского счета или хранителем средств пользователя. Mirocard не принимает депозиты, не открывает банковские счета, не выпускает электронные деньги и не хранит средства пользователей.
Операции, включая пополнение карточного функционала, расчеты, авторизации, списания, возвраты, отмены, споры, chargeback и иные связанные процедуры, могут обрабатываться сторонними участниками инфраструктуры. Mirocard вправе учитывать решения, ограничения, отказы, удержания, возвраты, отмены или иные меры таких участников, если они применяются в соответствии с их правилами, требованиями карточной программы или применимым законодательством.

1.4. Проверки через провайдеров и партнерскую инфраструктуру

Mirocard может проводить KYC/KYB-проверки, санкционные проверки, проверки PEP, проверки негативной публичной информации, проверки на мошенничество, проверки криптовалютных адресов и транзакций, а также иные комплаенс-проверки с использованием сторонних провайдеров, включая Sumsub, иных KYC/AML-провайдеров, провайдеров санкционного скрининга, провайдеров предотвращения мошенничества, провайдеров blockchain-аналитики, карточных, процессинговых, платежных и технических партнеров.
Использование стороннего провайдера не ограничивает право Mirocard самостоятельно принимать решения о регистрации пользователя, прохождении проверки, выпуске или использовании виртуальной карты, лимитах, операциях, дополнительных проверках, ограничениях, блокировках или прекращении обслуживания.
Mirocard также вправе учитывать требования карточных программ, BIN, эмитентов, процессинга, карточных сетей, KYC/AML-провайдеров и иных обязательных участников инфраструктуры.

1.5. Отсутствие гарантии доступа к сервису

Регистрация, предоставление документов, успешное прохождение проверки или ранее предоставленный доступ к функционалу Mirocard не гарантируют пользователю:

- выпуск виртуальной карты;
- доступ к конкретному BIN или карточной программе;
- проведение конкретной операции;
- сохранение лимитов, комиссий или иных условий;
- отсутствие дополнительных проверок;
- непрерывное или бессрочное предоставление сервиса.

Mirocard вправе отказать в регистрации, проверке, выпуске или использовании виртуальной карты, отклонить или приостановить операцию, ограничить функционал, ограничить доступную сумму, заблокировать аккаунт или карту, приостановить обслуживание либо прекратить отношения с пользователем, если это необходимо или целесообразно с учетом AML/CFT, санкционных, мошеннических, карточных, регуляторных, партнерских или иных комплаенс-требований.

2. KYC/KYB и риск-ориентированный подход

2.1. Обязательность проверки

Для использования Mirocard пользователь обязан пройти KYC/KYB-проверку в объеме, определяемом Mirocard с учетом риск-ориентированного подхода, применимого законодательства, требований карточной программы, BIN, эмитента, процессинга, карточной сети, KYC/AML-провайдера, иных обязательных партнеров, доступного функционала, лимитов и характера использования сервиса.
Проверка может проводиться при регистрации, подаче заявки на выпуск виртуальной карты, пополнении карточного функционала, совершении операций, изменении пользовательских данных, повышении лимитов, изменении BIN или карточной программы, выявлении подозрительной активности, пересмотре риск-профиля, а также в иных случаях, когда Mirocard считает это необходимым для комплаенс-целей.
Mirocard вправе отказать в регистрации, выпуске карты, проведении операции или дальнейшем обслуживании, если пользователь не прошел проверку, предоставил неполные, недостоверные, противоречивые или неактуальные сведения, отказался предоставить необходимые документы либо если результаты проверки указывают на неприемлемый уровень риска.

2.2. Проверка физических лиц

В отношении физических лиц проверка может включать:

- идентификацию и верификацию личности;
- проверку документа, возраста и дееспособности;
- проверку гражданства, резидентства и адреса;
- проверку контактных данных;
- проверку с использованием селфи или liveness-процедуры;
- санкционную проверку;
- проверку PEP;
- проверку негативной публичной информации;
- проверку цели использования сервиса;
- проверку характера операций;
- проверку источника средств или источника благосостояния.

2.3. Проверка юридических лиц

В отношении юридических лиц проверка может включать:

- проверку регистрационных и корпоративных данных;

- проверку страны регистрации и фактического места деятельности;
- анализ деловой модели и характера деятельности;
- проверку представителей, директоров и уполномоченных лиц;
- проверку структуры владения;
- проверку бенефициарных владельцев;
- проверку цели использования сервиса;
- санкционную проверку юридического лица и связанных лиц;
- проверку PEP и негативной публичной информации по связанным лицам;
- проверку источника средств или источника благосостояния.

Mirocard определяет объем проверки индивидуально, исходя из риск-профиля пользователя, юрисдикции, характера деятельности, структуры владения, источника средств, операций, доступных лимитов, применимого BIN, карточной программы и требований партнеров.

2.4. Риск-ориентированный подход

Mirocard применяет риск-ориентированный подход к регистрации пользователей, проверке, предоставлению доступа к сервису, выпуску и использованию виртуальных карт, мониторингу операций, установлению лимитов, применению ограничений и принятию иных комплаенс-решений.

При оценке риска Mirocard может учитывать:

- тип пользователя;
- страну гражданства, резидентства, регистрации, ведения деятельности или фактического нахождения;
- результаты KYC/KYB-проверки;
- прозрачность структуры владения;
- сведения о бенефициарных владельцах;
- характер деятельности и цель использования сервиса;
- источник средств или источник благосостояния;
- способ пополнения карточного функционала, включая криптовалютные переводы;
- объем, частоту, характер и географию операций;
- используемый BIN, карточную программу, MCC, лимиты и доступный функционал;
- наличие отклоненных операций, споров, возвратов, отмен или chargeback;
- санкционные, PEP, негативные, мошеннические или иные комплаенс-индикаторы;
- требования эмитента, KYC/AML-провайдера или иных партнеров;
- применимое законодательство, санкционные режимы и внутренние процедуры управления рисками Mirocard.

Перечень факторов не является исчерпывающим. Mirocard вправе учитывать любые иные обстоятельства, которые могут иметь значение для оценки AML/CFT, санкционного, мошеннического, регуляторного, карточного, операционного, репутационного или иного комплаенс-риска.

2.5. Дополнительная и расширенная проверка

Mirocard вправе в любое время запросить у пользователя дополнительные сведения, документы или пояснения, провести повторную проверку, дополнительную проверку или расширенную проверку, если это необходимо для идентификации, оценки риска, подтверждения источника средств, анализа операции, проверки юридического лица, проверки бенефициарных владельцев, соблюдения санкционных требований, предотвращения мошенничества или выполнения иных комплаенс-задач.

Такая проверка может включать:

- подтверждение источника средств или источника благосостояния;
- анализ экономического смысла операций;
- проверку криптовалютных адресов;
- проверку blockchain-данных;
- проверку хэша транзакции;
- проверку связанных адресов, контрагентов, бирж, обменников или иных данных, относящихся к происхождению и движению средств;
- запрос договоров, счетов, выписок, корпоративных документов, налоговых документов или иных подтверждающих материалов.

Пользователь обязан предоставлять достоверные, полные, актуальные и непротиворечивые сведения и документы. Непредоставление запрошенной информации, предоставление недостоверных сведений, сокрытие бенефициарных владельцев, источника средств, цели использования сервиса или связи с запрещенной либо ограниченной юрисдикцией может привести к отказу в обслуживании, ограничению функционала, блокировке аккаунта или карты, ограничению операции, ограничению доступной суммы либо прекращению отношений с пользователем.

2.6. Пересмотр риск-профиля
Риск-профиль пользователя может пересматриваться в течение всего периода использования сервиса, в том числе при изменении данных пользователя, структуры владения, бенефициарных владельцев, характера деятельности, страны гражданства, резидентства, регистрации или фактического нахождения, объема или характера операций, лимитов, BIN, карточной программы, применимых требований партнеров или законодательства.
По результатам пересмотра риск-профиля Mirocard вправе изменить доступный функционал, запросить дополнительные сведения или документы, провести повторную или расширенную проверку, изменить лимиты, ограничить операции, заблокировать аккаунт или карту, ограничить доступную сумму, отказать в дальнейшем обслуживании либо принять иные меры, необходимые для управления риском.

3. Санкционная проверка, PEP и негативная информация
3.1. Общий принцип
Mirocard проводит санкционные проверки, проверки PEP, проверки негативной публичной информации и иные комплаенс-проверки в отношении пользователей, представителей, директоров, уполномоченных лиц, бенефициарных владельцев, связанных лиц, юрисдикций, операций, источников средств и иных данных, относящихся к использованию сервиса.
Такие проверки могут проводиться при регистрации, KYC/KYB-проверке, подаче заявки на выпуск виртуальной карты, пополнении карточного функционала, совершении операций, изменении пользовательских данных, повторной или расширенной проверке, мониторинге активности, пересмотре риск-профиля, а также в иных случаях, когда Mirocard считает это необходимым для комплаенс-целей.
3.2. Санкционные списки и режимы
Mirocard может осуществлять санкционный контроль с использованием применимых санкционных списков, режимов и источников, включая:
- консолидированный санкционный список Европейского союза;
- консолидированный список Совета Безопасности ООН;
- санкционные списки OFAC;
- санкционные списки Великобритании;
- санкционные списки, правила и ограничения, применимые к карточной программе, BIN, эмитенту, процессингу, карточной сети, банкам, платежным провайдерам, KYC/AML-провайдерам или иным обязательным партнерам Mirocard.

Mirocard также вправе учитывать территориальные, секторальные, товарные, технологические, финансовые и иные санкционные ограничения, даже если конкретное лицо не включено в персональный санкционный список.
3.3. PEP и негативная публичная информация
Mirocard вправе проверять пользователя и связанных лиц на наличие статуса политически значимого лица, а также учитывать негативную публичную информацию, которая может указывать на AML/CFT, санкционный, мошеннический, коррупционный, регуляторный, репутационный или иной комплаенс-риск.
Наличие PEP-статуса или негативной публичной информации не всегда означает автоматический отказ в обслуживании, однако может повлечь дополнительную проверку, запрос источника средств или источника благосостояния, расширенную проверку, ручное рассмотрение, установление дополнительных лимитов или ограничений, усиленный мониторинг либо отказ в обслуживании при неприемлемом уровне риска.
3.4. Санкционные совпадения и запрет обхода ограничений
При выявлении санкционного совпадения, возможного совпадения, связи с запрещенной или ограниченной юрисдикцией, риска обхода санкций, PEP-индикаторов, негативной публичной информации или иных существенных комплаенс-индикаторов Mirocard вправе отказать в регистрации, выпуске или использовании виртуальной карты, отклонить или приостановить операцию, ограничить функционал, запросить дополнительные документы, заблокировать аккаунт или карту, ограничить доступную сумму, прекратить обслуживание либо принять иные меры, необходимые для соблюдения применимых требований и управления рисками.
Пользователю запрещается использовать Mirocard для прямого или косвенного обхода санкций, территориальных ограничений, KYC/KYB-проверки, карточных ограничений, BIN-условий, MCC-ограничений, лимитов или иных комплаенс-требований.
В частности, запрещается использовать сервис в интересах санкционного лица, организации или юрисдикции, через номинальных лиц, подставные структуры, чужие данные, связанные аккаунты, VPN, proxy, TOR или иные средства, если это направлено на сокрытие личности, местонахождения, источника средств, бенефициарного владельца, фактического пользователя или характера операции.

3.5. Нераскрытие деталей проверки
Mirocard вправе не раскрывать пользователю детали санкционной проверки, проверки PEP, проверки негативной публичной информации или иной комплаенс-проверки, включая источники проверки, результаты совпадений, внутреннюю оценку риска, правила эскалации, риск-индикаторы, пороговые значения, модели оценки или конкретные основания принятого решения, если такое раскрытие может нарушить применимое законодательство, санкционные требования, правила карточной программы, требования партнеров, безопасность сервиса, права третьих лиц или эффективность комплаенс-процедур.

4. Запрещенные и ограниченные юрисдикции
4.1. Общий принцип
Mirocard не предоставляет сервис пользователям, которые находятся, зарегистрированы, являются гражданами или резидентами, ведут деятельность либо иным образом связаны с запрещенными или ограниченными юрисдикциями, если такое обслуживание противоречит применимому законодательству, санкционным режимам, AML/CFT-требованиям, требованиям карточной программы, BIN, эмитента, процессинга, карточной сети, иных обязательных партнеров или внутренней оценке рисков Mirocard. Mirocard вправе отказать в регистрации, KYC/KYB-проверке, выпуске или использовании виртуальной карты, проведении операции или дальнейшем обслуживании при выявлении связи пользователя, операции, источника средств, мерчанта, аккаунта или карты с запрещенной или ограниченной юрисдикцией.
4.2. Перечень запрещенных и ограниченных юрисдикций
На дату последнего обновления настоящей Политики Mirocard не предоставляет сервис пользователям, которые являются гражданами, резидентами, зарегистрированы, фактически находятся, ведут деятельность, имеют источник средств либо иным образом связаны со следующими странами и территориями:
- Исламская Республика Афганистан - AF;
- Республика Ангола - AO;
- Беларусь - BY;
- Босния и Герцеговина - BA;
- Республика Ботсвана - BW;
- Содружество Багамских Островов - BS;
- Королевство Камбоджа - KH;
- Республика Бурунди - BI;
- Демократическая Республика Конго - CD;
- Центральноафриканская Республика - CF;
- Республика Конго - CG;
- Алжирская Народно-Демократическая Республика - DZ;
- Республика Эквадор - EC;
- Государство Эритрея - ER;
- Федеративная Демократическая Республика Эфиопия - ET;
- Республика Гана - GH;
- Республика Гвинея - GN;
- Республика Гвинея-Бисау - GW;
- Кооперативная Республика Гайана - GY;
- Республика Гаити - HT;
- Иракская Республика - IQ;
- Исламская Республика Иран - IR;
- Япония - JP;
- Республика Кения - KE;
- Корейская Народно-Демократическая Республика - KP;
- Республика Куба - CU;
- Ливанская Республика - LB;
- Республика Либерия - LR;
- Ливия - LY;
- Республика Союза Мьянма - MM;
- Федеративная Республика Нигерия - NG;
- Исламская Республика Пакистан - PK;
- Республика Сербия - RS;
- Российская Федерация - RU;
- Республика Судан - SD;

- Демократическая Социалистическая Республика Шри-Ланка - LK;
- Федеративная Республика Сомали - SO;
- Республика Южный Судан - SS;
- Сирийская Арабская Республика - SY;
- Тунисская Республика - TN;
- Республика Тринидад и Тобаго - TT;
- Украина - UA;
- Республика Уганда - UG;
- Соединенные Штаты Америки - US;
- Республика Вануату - VU;
- Боливарианская Республика Венесуэла - VE;
- Республика Йемен - YE;
- Республика Зимбабве - ZW;
- Китайская Народная Республика - CN.

Для целей настоящей Политики связь с запрещенной или ограниченной юрисдикцией может включать гражданство, резидентство, регистрацию, фактическое местонахождение, место ведения деятельности, источник средств, источник благосостояния, нахождение представителей, директоров, бенефициарных владельцев, связанных лиц, мерчантов, контрагентов или иных существенных элементов операции в такой юрисдикции.

Mirocard также вправе ограничивать или запрещать обслуживание пользователей, связанных с иными странами, территориями или регионами, если такое ограничение требуется применимым законодательством, санкционными режимами, требованиями FATF, карточной программы, BIN, эмитента, процессинга, карточной сети, иных обязательных партнеров или внутренней оценкой рисков Mirocard.

Наличие страны или территории в настоящем перечне не обязательно означает, что такая страна или территория полностью запрещена применимым законодательством. Ограничение может быть обусловлено требованиями партнеров, карточной инфраструктуры, санкционными, AML/CFT, мошенническими, операционными, регуляторными или иными комплаенс-рисками.

4.3. Обновление перечня

Mirocard вправе в любое время обновлять, дополнять или изменять перечень запрещенных и ограниченных юрисдикций без отдельного переподписания настоящей Политики или иных пользовательских документов. Изменения могут быть обусловлены изменением санкционных режимов, применимого законодательства, регуляторных требований, требований карточной программы, BIN, эмитента, процессинга, карточной сети, иных партнеров, географии обслуживания, технической доступности или внутренней оценки рисков Mirocard.

Обновленный перечень применяется с момента его публикации на сайте Mirocard, в интерфейсе сервиса, в настоящей Политике или с иной даты, указанной Mirocard.

Продолжение использования сервиса после обновления перечня означает согласие пользователя с применимыми ограничениями, если иное не предусмотрено обязательными нормами применимого законодательства.

4.4. Обязанности пользователя

Пользователь обязан самостоятельно убедиться, что он имеет право использовать Mirocard в соответствии с законодательством своей юрисдикции и не подпадает под ограничения, установленные перечнем запрещенных и ограниченных юрисдикций, правилами карточной программы, санкционными режимами или требованиями применимых партнеров.

Пользователю запрещается использовать сервис из запрещенной или ограниченной юрисдикции, предоставлять недостоверные сведения о гражданстве, резидентстве, регистрации, фактическом местонахождении или связи с такой юрисдикцией, а также использовать третьих лиц, номинальных лиц, чужие аккаунты, VPN, proxy, TOR или иные средства для обхода территориальных, санкционных или комплаенс-ограничений.

При нарушении настоящего раздела Mirocard вправе отказать в регистрации, проверке, выпуске или использовании виртуальной карты, отклонить или приостановить операцию, ограничить функционал, заблокировать аккаунт или карту, ограничить доступную сумму, прекратить обслуживание либо принять иные меры, необходимые для соблюдения AML/CFT, санкционных, карточных, регуляторных или иных комплаенс-требований.

5. Мониторинг операций и запрещенное использование

5.1. Мониторинг операций

Mirocard вправе осуществлять постоянный мониторинг пользователей, аккаунтов, пополнений карточного функционала, операций, виртуальных карт, карточного поведения, технических сигналов, источников средств и иных действий в сервисе для выявления и предотвращения AML/CFT, санкционных, мошеннических, карточных, операционных и иных комплаенс-рисков.
Мониторинг может проводиться до совершения операции, во время ее обработки, после ее совершения, а также в течение всего периода использования сервиса.
При мониторинге Mirocard может учитывать:

- объем, частоту, характер и географию операций;
- способ и источник пополнения карточного функционала, включая криптовалютные переводы;
- blockchain-данные, криптовалютные адреса и связанные адреса;
- используемый BIN, MCC, лимиты и категории мерчантов;
- отклоненные операции, споры, возвраты, отмены и chargeback;
- технические данные, IP-адрес, устройство, геолокационные сигналы и признаки использования VPN, proxy или TOR;
- результаты KYC/KYB-проверки;
- источник средств или источник благосостояния;
- санкционные, PEP, негативные, мошеннические и иные комплаенс-индикаторы.

Mirocard вправе использовать автоматические и ручные методы мониторинга, внутренние процедуры, а также данные сторонних провайдеров, карточной программы, эмитента, процессинга, карточной сети, KYC/AML-провайдера, провайдеров blockchain-аналитики, крипто-инфраструктурных контрагентов и иных обязательных партнеров.

5.2. Запрещенное использование

Пользователю запрещается использовать Mirocard, аккаунт, виртуальные карты, доступную сумму или иной функционал сервиса для:

- отмывания денежных средств, финансирования терроризма, обхода санкций или иной незаконной деятельности;
- мошенничества, обмана третьих лиц, злоупотреблений, проверки карт массовыми или автоматизированными операциями, захвата аккаунта, злоупотребления оспариванием операций или иных неправомерных действий;
- использования незаконных, неподтвержденных, непрозрачных или экономически необъяснимых источников средств;
- обхода KYC/KYB-проверки, проверки источника средств или источника благосостояния, лимитов, BIN-условий, MCC-ограничений, санкционных, территориальных, технических или иных комплаенс-ограничений;
- использования сервиса в интересах третьих лиц, через номинальных лиц, чужие аккаунты, связанные аккаунты, подставные структуры или иные способы обхода проверки и ограничений;
- совершения операций, не соответствующих заявленной цели использования сервиса, риск-профилю пользователя или экономическому смыслу операций;
- совершения операций, нарушающих настоящую Политику, Политику использования, условия карточной программы, требования эмитента, партнеров или применимое законодательство.

5.3. Запрещенные и ограниченные категории операций

Пользователю запрещается использовать Mirocard и виртуальные карты для операций, связанных с запрещенными или ограниченными категориями, включая:

- операции, приравненные к получению наличных или переводу средств;
- денежные эквиваленты и квази-денежные операции;
- азартные игры, ставки, лотереи и игровые сервисы;
- товары и услуги для взрослых;
- покупку криптовалюты, токенов, цифровых активов, услуги обмена, P2P-платформы или иные крипто-сервисы, если такие операции запрещены условиями конкретной карточной программы, BIN, MCC или правилами Mirocard;
- мерчантов повышенного риска;
- MCC повышенного риска;
- финансовые пирамиды, мошеннические схемы, инвестиционное мошенничество или вводящие в заблуждение практики;
- darknet markets, миксеры, тумблеры, программы-вымогатели, взломы, украденные данные, незаконные маркетплейсы или иную запрещенную либо высокорисковую активность;

- санкционные лица, запрещенные или ограниченные юрисдикции, санкционные товары, услуги, сектора или виды деятельности;
- терроризм, экстремизм, торговлю оружием, наркотиками, людьми, незаконным контентом или иную преступную деятельность.

Конкретная доступность или запрет отдельных операций может зависеть от карточной программы, BIN, MCC, эмитента, процессинга, карточной сети, требований партнеров и внутренней оценки рисков Mirocard.

5.4. Высокорисковая активность

Mirocard вправе считать подозрительной или высокорисковой любую активность, которая не соответствует риск-профилю пользователя, заявленной цели использования сервиса, экономическому смыслу операций, условиям карточной программы, BIN, лимитам, MCC-ограничениям или иным применимым требованиям.

К высокорисковой активности могут относиться:

- нетипичные или повторяющиеся операции;
- повышенная доля отклоненных операций;
- частые споры, возвраты, отмены или chargeback;
- операции с мерчантами повышенного риска;
- признаки массовой проверки карт;
- признаки захвата аккаунта;
- злоупотребление оспариванием операций;
- попытки обхода ограничений;
- использование нескольких аккаунтов;
- использование номинальных лиц;
- использование VPN, proxy или TOR для сокрытия фактического местонахождения;
- связь операций, адресов, источников средств, мерчантов или пользователя с санкционными, мошенническими, AML/CFT или иными комплаенс-рисками.

5.5. Меры по результатам мониторинга

При выявлении запрещенного использования, высокорисковой активности, подозрительной активности или иных комплаенс-индикаторов Mirocard вправе:

- запросить дополнительные сведения или документы;
- провести повторную проверку или расширенную проверку;
- снизить лимиты;
- ограничить функционал;
- отклонить или приостановить запрос на пополнение карточного функционала;
- отклонить или приостановить карточную операцию;
- ограничить обработку возврата, отмены, спора или chargeback, если это допустимо применимыми правилами;
- ограничить доступную сумму;
- заблокировать аккаунт или виртуальную карту;
- отказать в дальнейшем обслуживании;
- передать информацию партнерам или компетентным органам, если это требуется или допустимо применимыми требованиями;
- принять иные меры, необходимые для соблюдения AML/CFT, санкционных, мошеннических, карточных, регуляторных, партнерских или внутренних требований Mirocard.

Если соответствующая операция, доступная сумма, криптоактив, возврат, отмена или карточная процедура обрабатывается сторонним участником инфраструктуры, Mirocard вправе учитывать решения, ограничения, удержания, отказы, возвраты, отмены или иные меры, примененные таким участником.

6. Ограничения, блокировки и отказ в обслуживании

6.1. Право применять ограничения

Mirocard вправе в любое время применять временные или постоянные ограничения в отношении пользователя, аккаунта, виртуальной карты, доступной суммы, пополнения карточного функционала, операции или отдельных функций сервиса, если это необходимо или целесообразно для соблюдения AML/CFT, санкционных, мошеннических, карточных, регуляторных, партнерских или внутренних требований управления рисками.

Такие меры могут применяться по инициативе Mirocard, а также по требованию или с учетом требований карточной программы, BIN, эмитента, процессинга, карточной сети, KYC/AML-провайдера, крипто-инфраструктурного контрагента, банка, платежного провайдера, компетентного органа или иного обязательного участника инфраструктуры.

6.2. Основания для ограничений

Ограничения могут применяться, в частности, при наличии или подозрении на:

- непрохождение KYC/KYB-проверки;
- отказ от повторной проверки;
- непредоставление запрошенных документов;
- предоставление недостоверных, неполных, противоречивых, неактуальных или поддельных сведений;
- неподтвержденный, непрозрачный или экономически необъяснимый источник средств или источник благосостояния;
- AML/CFT, санкционный, мошеннический, регуляторный, карточный, операционный, репутационный или иной комплаенс-риск;
- связь с санкционным лицом, запрещенной или ограниченной юрисдикцией, запрещенным мерчантом, MCC или запрещенной категорией операций;
- мошенничество, злоупотребление, массовую проверку карт, захват аккаунта, злоупотребление оспариванием операций или несанкционированную активность;
- обход или попытку обхода KYC/KYB, санкционных, территориальных, BIN, MCC, лимитных, технических или иных ограничений;
- нарушение настоящей Политики, Политики использования, условий конкретной карты, условий карточной программы, требований эмитента, партнеров или применимого законодательства;
- требование, рекомендацию или ограничение со стороны эмитента, карточной программы, партнера BIN, процессинга, карточной сети, KYC/AML-провайдера, крипто-инфраструктурного контрагента, банка, платежного провайдера, регулятора, правоохранительного органа или иного компетентного лица.

Перечень оснований не является исчерпывающим. Mirocard вправе применить ограничения в любых иных случаях, когда продолжение обслуживания, проведение операции или предоставление функционала создает или может создать комплаенс-риск для Mirocard, пользователей, партнеров или карточной инфраструктуры.

6.3. Виды мер

В зависимости от характера риска Mirocard вправе применить одну или несколько мер, включая:

- отказ в регистрации, проверке, выпуске или использовании виртуальной карты;
- запрос дополнительных сведений, документов, пояснений, источника средств или источника благосостояния;
- проведение повторной проверки, дополнительной проверки или расширенной проверки;
- снижение лимитов;
- изменение доступного функционала;
- ограничение отдельных BIN или карточных программ;
- отклонение, отмену или приостановку операции;
- отказ в обработке или приостановку пополнения карточного функционала;
- ограничение доступной суммы;
- блокировку виртуальной карты или аккаунта;
- отказ в обработке отдельных запросов пользователя, если это допустимо применимыми правилами;
- прекращение обслуживания пользователя;
- передачу информации партнерам, эмитенту, карточной программе, регулятору, правоохранительным органам или иным компетентным лицам, если это требуется или допустимо применимыми требованиями;
- иные меры, необходимые для соблюдения AML/CFT, санкционных, мошеннических, карточных, регуляторных, партнерских или внутренних требований Mirocard.

Mirocard не хранит средства пользователей. Если ограничение связано с операцией, доступной суммой, возвратом, отменой, спором, chargeback или иной процедурой, фактическая обработка такой процедуры может зависеть от стороннего участника инфраструктуры и его правил.

6.4. Применение мер без предварительного уведомления

Ограничительные меры могут применяться без предварительного уведомления пользователя, если предварительное уведомление может:

- создать риск обхода проверки или ограничений;
- нарушить применимое законодательство или санкционные требования;
- противоречить требованиям партнеров или карточной инфраструктуры;
- затруднить предотвращение мошенничества;
- снизить эффективность AML/KYC, санкционных или иных комплаенс-процедур;
- нарушить права третьих лиц или безопасность сервиса.

6.5. Нераскрытие причин

Mirocard вправе не раскрывать пользователю конкретные причины отказа, ограничения, блокировки, приостановки операции, ограничения доступной суммы или прекращения обслуживания, если раскрытие может нарушить применимое законодательство, санкционные требования, правила карточной программы, требования партнеров, безопасность сервиса, права третьих лиц или эффективность AML/KYC, санкционных, мошеннических и иных процедур управления рисками.

7. Обработка и передача AML/KYC-данных

7.1. Общий принцип

Для целей KYC/KYB, AML/CFT, санкционного комплаенса, предотвращения мошенничества, мониторинга операций, оценки рисков, обработки карточных операций и выполнения требований партнеров Mirocard вправе собирать, использовать, проверять, анализировать, хранить и передавать данные пользователя в объеме, необходимом для предоставления сервиса, проведения проверок, принятия комплаенс-решений и соблюдения применимых требований.

Такие данные могут включать:

- идентификационные данные и документы;
- сведения о юридическом лице, представителях и бенефициарных владельцах;
- результаты KYC/KYB-проверки;
- результаты санкционной проверки;
- результаты проверки PEP и негативной публичной информации;
- сведения об источнике средств или источнике благосостояния;
- сведения о пополнениях карточного функционала, операциях, виртуальных картах, BIN, MCC, отклоненных операциях, спорах, возвратах, отменах и chargeback;
- blockchain-данные;
- технические и security-данные;
- риск-индикаторы, результаты мониторинга и внутренней оценки риска.

Подробные условия обработки персональных данных, включая правовые основания, сроки хранения, международную передачу данных, права пользователя и порядок их реализации, определяются Политикой конфиденциальности Mirocard.

7.2. Передача данных партнерам и провайдерам

Mirocard вправе передавать AML/KYC и комплаенс-данные третьим лицам, если это необходимо или целесообразно для проведения проверки, предоставления сервиса, выпуска и обслуживания виртуальных карт, обработки операций, мониторинга, управления рисками, предотвращения мошенничества, исполнения требований партнеров или соблюдения применимого законодательства.

Такие третьи лица могут включать:

- KYC/AML-провайдеров, включая Sumsub;
- провайдеров санкционной проверки, проверки PEP, негативной публичной информации, предотвращения мошенничества и идентификации личности;
- эмитентов, карточные программы, партнеров BIN, процессинговых провайдеров и карточные сети;
- провайдеров blockchain-аналитики, крипто-инфраструктурных провайдеров, биржевых, ликвидностных или расчетных контрагентов, банки и платежных провайдеров;
- облачных, хостинговых, security, аналитических, support, technical и outsourcing-провайдеров;
- аудиторов, юридических советников, консультантов и иных профессиональных представителей Mirocard;
- регуляторов, правоохранительные органы, суды, санкционные органы, государственные органы или иные компетентные лица, если такая передача требуется или допустима применимыми требованиями.

7.3. Международная передача данных

С учетом международного характера сервиса, карточной инфраструктуры, криптовалютных пополнений, KYC/AML-провайдеров, эмитентов, процессинговых провайдеров, карточных сетей и технических партнеров данные пользователя могут передаваться и обрабатываться за пределами страны проживания пользователя, в том числе за пределами Европейской экономической зоны.

Такая передача осуществляется в соответствии с Политикой конфиденциальности Mirocard, применимым законодательством о защите данных и используемыми Mirocard договорными, организационными или техническими мерами защиты данных.

7.4. Хранение AML/KYC-данных

Mirocard вправе хранить AML/KYC и комплаенс-данные в течение срока, необходимого для предоставления сервиса, выполнения AML/CFT, санкционных, мошеннических, карточных, регуляторных, налоговых, бухгалтерских, договорных и иных применимых требований, обработки операций, споров, возвратов,

отмен, chargeback, претензий, внутренних проверок, расследований и защиты прав Mirocard, пользователей, партнеров или третьих лиц.
Mirocard может продолжать хранить отдельные AML/KYC и комплаенс-данные после прекращения обслуживания пользователя, если такое хранение требуется или допустимо применимым законодательством, требованиями партнеров, карточной инфраструктуры, внутренними процедурами управления рисками или необходимостью защиты прав и законных интересов Mirocard.

7.5. Конфиденциальность комплаенс-информации

Mirocard вправе не раскрывать пользователю внутренние AML/KYC и комплаенс-данные, включая результаты риск-оценки, скоринга, пороговые значения, риск-индикаторы, результаты санкционной проверки, проверки PEP, проверки негативной публичной информации, blockchain-анализа, проверки на мошенничество, мониторинга, ручной проверки, внутренней эскалации или конкретные основания отдельных комплаенс-решений.
Раскрытие такой информации может быть ограничено, если оно может нарушить применимое законодательство, санкционные требования, требования компетентных органов, правила карточной программы, требования эмитента или партнеров, безопасность сервиса, права третьих лиц либо снизить эффективность AML/KYC, санкционных, мошеннических или иных процедур управления рисками.

8. Заключительные положения

8.1. Приоритет комплаенс-требований

Mirocard вправе применять любые меры, необходимые или целесообразные для соблюдения AML/CFT, санкционных, мошеннических, карточных, регуляторных, партнерских и иных требований управления рисками.
Если использование сервиса пользователем создает или может создать AML/CFT, санкционный, мошеннический, регуляторный, карточный, операционный, репутационный или иной комплаенс-риск, Mirocard вправе ограничить или прекратить предоставление сервиса независимо от того, предусмотрена ли конкретная ситуация прямо в настоящей Политике.
В случае противоречия между интересами пользователя и необходимостью соблюдения применимых комплаенс-требований, требований карточной программы, BIN, эмитента, процессинга, карточной сети, KYC/AML-провайдера, компетентного органа или иного обязательного партнера Mirocard вправе применить более строгий подход.

8.2. Нераскрытие внутренних процедур

Настоящая Политика является публичным документом и не раскрывает внутренние процедуры Mirocard, включая внутренние правила проверки, риск-скоринг, пороговые значения, риск-индикаторы, правила мониторинга, матрицу эскалации, санкционные и мошеннические сценарии, правила blockchain-аналитики, критерии принятия решений, материалы внутренних проверок и иные элементы комплаенс-модели.
Mirocard вправе не раскрывать пользователю такие сведения, а также конкретные основания отдельных комплаенс-решений, если раскрытие может нарушить применимое законодательство, санкционные требования, требования компетентных органов, правила карточной программы, требования эмитента или партнеров, безопасность сервиса, права третьих лиц либо снизить эффективность AML/KYC, санкционных, мошеннических или иных процедур управления рисками.

8.3. Изменение Политики

Mirocard вправе в любое время изменять, дополнять или обновлять настоящую Политику, включая положения о KYC/KYB-проверке, санкционном контроле, запрещенных и ограниченных юрисдикциях, мониторинге операций, запрещенном использовании, ограничениях, блокировках, обработке данных и иных комплаенс-мерах.
Изменения могут быть обусловлены изменением применимого законодательства, санкционных режимов, списков FATF, требований карточной программы, BIN, эмитента, процессинга, карточной сети, KYC/AML-провайдера, партнеров, операционной модели, внутренней оценки рисков или функционала сервиса.
Обновленная редакция Политики применяется с момента ее публикации на сайте Mirocard, в интерфейсе сервиса, в личном кабинете пользователя или с иной даты, указанной Mirocard.
Продолжение использования сервиса после обновления Политики означает согласие пользователя с обновленной редакцией, если иное не требуется применимым законодательством.

8.4. Язык и толкование

Настоящая редакция Политики составлена на английском языке. Если Политика предоставляется на нескольких языках, применимой и приоритетной считается версия на английском языке, если Mirocard прямо не укажет иную приоритетную версию.
Заголовки разделов используются только для удобства и не влияют на толкование настоящей Политики.

Если какое-либо положение настоящей Политики признается недействительным, незаконным или неисполнимым, это не влияет на действительность и исполнимость остальных положений.

8.5. Связь с другими документами

Настоящая Политика применяется совместно с Политикой использования, Политикой конфиденциальности, условиями конкретной карточной программы, условиями эмитента, процессинга, карточной сети и иных партнеров.

В случае противоречия между настоящей Политикой и иными пользовательскими документами Mirocard в части AML/CFT, санкционного комплаенса, KYC/KYB, мониторинга операций, ограничений, блокировок или отказа в обслуживании приоритет имеет настоящая Политика, если иное не требуется применимым законодательством или обязательными правилами карточной инфраструктуры.