

PAY HOT

Политика AML/KYC

Противодействие отмыванию денег, финансированию терроризма и финансовому мошенничеству

Оператор платформы	HOT GATE TECHNOLOGY LTDA
CNPJ	67.633.679/0001-27
Версия	1.0
Дата вступления в силу	26 июля 2026 г.
Сайт	https://pay.hot

1. Назначение политики

Настоящая Политика устанавливает подход PayHot к проверке пользователей, проектов, платежных операций и криптовалютных кошельков с целью снижения рисков отмывания денег, финансирования терроризма, мошенничества, обхода санкций и иной незаконной деятельности.

Политика применяется к мерчантам, их представителям и бенефициарным владельцам, плательщикам и получателям выплат в той степени, в которой их данные доступны PayHot или запрашиваются партнерским провайдером.

PayHot не осуществляет финансовые расчеты самостоятельно. Обязательные AML/KYC-процедуры по конкретной операции могут выполнять партнерские банки, платежные организации и криптопроцессинги. PayHot поддерживает эти процедуры собственной риск-ориентированной проверкой и передачей необходимых данных.

2. Основные принципы

- риск-ориентированный подход с учетом категории бизнеса, географии, оборота и платежного сценария;
- проверка до подключения и непрерывный мониторинг после запуска;
- минимизация доступа к данным и конфиденциальность материалов проверки;
- взаимодействие с регулируемыми партнерскими провайдерами;
- приоритет безопасности над скоростью подключения при наличии повышенного риска;
- запрет предупреждать пользователя о конфиденциальных действиях финансового мониторинга, если раскрытие ограничено законом.

3. Роли и ответственность

PayHot собирает и анализирует информацию, присваивает внутренний риск-профиль, применяет антифрод и AML-инструменты, запрашивает документы, ограничивает функции платформы и взаимодействует с партнерами.

Партнерский провайдер самостоятельно выполняет обязанности, возложенные на него применимым законодательством: идентификацию, проверку, мониторинг, принятие решения по операции, хранение обязательных записей и направление сообщений компетентным органам, когда это требуется.

Мерчант обязан предоставлять достоверные сведения, поддерживать их актуальность, контролировать собственных клиентов в необходимом объеме и не использовать Платформу для сокрытия реальных участников или характера деятельности.

4. Проверка мерчанта - KYB/KYC

Объем проверки зависит от модели подключения. PayHot или партнер может запросить:

- имя, дату рождения, гражданство, контактные и идентификационные данные физического лица;
- регистрационные документы, адрес, налоговый номер и полномочия представителя организации;
- структуру владения и сведения о конечных бенефициарных владельцах;
- описание продукта, домены, приложения, Telegram-боты, договоры, тарифы и политику возвратов;
- источники трафика, рекламные материалы, географию клиентов, средний чек и оборот;
- банковские и криптовалютные реквизиты, подтверждение владения счетом или кошельком;
- информацию об источнике средств и экономическом смысле операций.

Проверка может включать сопоставление с официальными реестрами, санкционными и ограничительными списками, списками публичных должностных лиц, базами утраченных документов, негативными публикациями и иными законными источниками.

5. Категории риска

Проекту присваивается уровень риска с учетом совокупности факторов. Внутренняя классификация не является публичной оценкой качества бизнеса и используется для выбора контроля.

Фактор	Примеры
Продукт и модель	Цифровые товары, подписки, посреднические модели, массовые выплаты, криптовалютные операции
География	Страны регистрации, пользователей, банков, партнеров и назначение трансграничных операций
Структура	Прозрачность собственников, полномочий, банковских счетов и связанных лиц
Операции	Оборот, средний чек, скорость, возвраты, аномалии и доля неуспешных попыток
Трафик и репутация	Источники клиентов, жалобы, вводящая в заблуждение реклама, негативные сведения
Криптовалюта	Риск адресов, источников средств, сервисов смешивания, взломов и санкционных связей

6. Усиленная проверка

При повышенном риске могут применяться дополнительные меры:

- расширенный пакет документов и подтверждение источника средств или состояния;
- проверка бенефициаров и связанных компаний;
- ручная проверка проекта и рекламных каналов;
- ограниченные лимиты, резерв, отсрочка расчета или поэтапный запуск;
- дополнительное подтверждение операций и адресов кошельков;
- повторная проверка с повышенной периодичностью;
- отказ в подключении или прекращение обслуживания при неприемлемом риске.

7. Мониторинг операций и AI-антифрод

PayHot анализирует платежный поток в реальном времени или с минимальной задержкой с помощью правил, статистических методов и моделей машинного обучения. Система сопоставляет отдельную операцию с поведением проекта и связанными событиями.

Могут учитываться частота и скорость операций, повторные попытки, несоответствие географии, резкое изменение суммы или конверсии, последовательность действий, технические идентификаторы, история возвратов, связи между аккаунтами и иные признаки.

AI-анализ помогает обнаруживать новые сочетания факторов, которые не покрываются одним статическим правилом. При срабатывании операция может быть направлена на дополнительную проверку, заблокирована технически или передана партнеру для принятия окончательного решения.

Точные алгоритмы, пороги и веса не публикуются, чтобы не облегчать обход контроля.

8. AML-проверка криптовалютных кошельков

До или после криптовалютной операции PayHot и партнер могут анализировать адрес отправителя и получателя, историю транзакций, источники поступлений и связи с известными категориями риска.

Проверка может выявлять связь с:

- взломами, кражами, мошенничеством и вымогательством;
- санкционными адресами и ограниченными юрисдикциями;
- нелегальными площадками, даркнет-маркетами и запрещенными сервисами;
- миксерами, анонимизаторами и схемами сокрытия происхождения средств;
- нелицензированными или высокорисковыми обменными площадками;
- иными источниками, отмеченными аналитическим провайдером как повышенный риск.

Наличие риск-сигнала не всегда означает незаконность операции, но может потребовать пояснений, документов или выбора другого кошелька. Решение принимается с учетом совокупности обстоятельств и требований партнера.

9. Подозрительные признаки

К признакам, требующим внимания, могут относиться:

- несоответствие операций заявленной деятельности или обороту;
- отсутствие понятного товара, услуги или экономического смысла;
- частые возвраты, chargeback, жалобы и платежи с признаками тестирования карт;
- искусственное дробление сумм, быстрый транзит и попытка немедленного вывода;
- использование множества несвязанных плательщиков для пополнения одного получателя;
- противоречивые документы, скрывание владельцев и отказ объяснить происхождение средств;
- необычная связь с высокорисковыми странами, кошельками или сервисами;
- попытки обойти лимиты, проверки или требования партнерского провайдера.

10. Меры реагирования

При выявлении риска PayHot вправе:

- запросить документы, сведения или объяснение;
- ограничить отдельный метод, проект, вывод или доступ к аккаунту;
- изменить лимиты, порядок подтверждения и уровень мониторинга;
- передать информацию партнерскому провайдеру в необходимом объеме;
- отклонить проект или прекратить сотрудничество;
- сохранить данные и предоставить их компетентному органу на законном основании.

Решение о замораживании, удержании, возврате или перечислении денежных средств принимает партнер, фактически выполняющий финансовую операцию, в соответствии со своими полномочиями и законом.

11. Санкции и ограничительные меры

PayHot и партнеры могут проверять лиц, организации, страны, банки и адреса по применимым санкционным и ограничительным спискам. Операция или сотрудничество могут быть запрещены, если их проведение создает нарушение обязательного ограничения либо неприемлемый риск для инфраструктуры.

12. Хранение и конфиденциальность данных

Материалы AML/KYC хранятся в течение срока, необходимого для выполнения договорных, доказательственных и правовых обязанностей. Доступ предоставляется только уполномоченным лицам и подрядчикам, которым информация необходима для работы.

PayHot не раскрывает пользователю детали внутреннего расследования, конкретные источники риска, алгоритмы или факт возможного сообщения органу, когда раскрытие ограничено законом или может помешать проверке.

13. Обязанности мерчанта

- предоставлять полные и достоверные сведения и обновлять их без задержки;
- использовать только согласованные проекты, домены, товары и источники трафика;
- не принимать платежи за третьих лиц без письменного согласования;
- вести подтверждения заказов, исполнения услуг и возвратов;
- соблюдать санкционные, налоговые, потребительские и иные требования своей юрисдикции;
- незамедлительно сообщать о подозрительной активности и компрометации;
- не пытаться выяснить или обойти внутренние критерии контроля.

14. Права пользователя

Пользователь может запросить исправление неверных идентификационных данных и предоставить пояснения по риск-сигналу. Это не гарантирует одобрение операции или подключения, если партнер или PayHot оценивает риск как неприемлемый.

15. Изменения политики

Политика может обновляться с учетом законодательства, требований партнеров, новых рисков и развития инструментов контроля. Актуальная редакция публикуется на сайте PayHot.

16. Нормативные ориентиры и контакты

Политика разработана с учетом применимых требований Бразилии по предотвращению отмыwania денег, включая Lei nº 9.613/1998, общих международных принципов риск-ориентированного контроля и обязательных правил партнерских провайдеров в соответствующих юрисдикциях.

Вопросы по проверке можно направить на team@pay.hot. В целях конфиденциальности PayHot может не раскрывать отдельные детали внутренней системы мониторинга.