

**ПОЛИТИКА ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ (KYC) И ПРОТИВОДЕЙСТВИЯ
ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ,
И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА (AML) ООО «ПРОФИТДРАЙВ»**

(далее – Политика KYC/AML)

Оператор не является платёжным агентом, банковским платёжным агентом, оператором по переводу денежных средств или иной финансовой организацией. Все расчёты осуществляются Платежным Провайдером. Оператор не принимает денежные средства, не хранит их и не распоряжается ими. Оператор предоставляет исключительно информационно-техническую платформу для взаимодействия.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика идентификации пользователей (Know Your Customer – KYC) и противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (Anti-Money Laundering – AML) (далее – Политика KYC/AML) определяет цели, принципы и порядок осуществления ООО «ПРОФИТДРАЙВ» (далее – Оператор) мер, направленных на: а) идентификацию Пользователей, Партнеров (включая участников Партнёрской программы) и их представителей мобильного приложения «Умный Водитель» (далее – Приложение); б) выявление и предотвращение мошеннических действий, злоупотреблений и иной противоправной деятельности; в) соблюдение требований законодательства Российской Федерации в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее – ПОД/ФТ).

1.2. Политика KYC/AML разработана в строгом соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными применимыми нормативно-правовыми актами Российской Федерации, а также внутренними правилами и регламентами Оператора.

1.3. Настоящая Политика KYC/AML является неотъемлемой частью Пользовательского соглашения, Публичной оферты (договора оказания услуг) для Партнеров, Публичной оферты об участии в Партнёрской программе, а также Политики обработки персональных данных Оператора. Акцепт указанных документов означает полное и безоговорочное согласие субъекта данных с условиями настоящей Политики KYC/AML.

1.4. Оператор обеспечивает конфиденциальность информации, полученной в ходе процедур KYC/AML, и ее защиту от несанкционированного доступа, разглашения или утраты в соответствии с законодательством РФ.

1.5. Оператор оставляет за собой право вносить изменения в настоящую Политику KYC/AML в одностороннем порядке. Актуальная версия Политики KYC/AML размещается в Приложении и на официальном сайте Оператора, что является надлежащим уведомлением субъектов данных.

1.6. Оператор применяет риск-ориентированный подход при проведении процедур идентификации и мониторинга, определяя объем и глубину проверок в зависимости от уровня риска конкретного субъекта данных. Субъекты данных могут классифицироваться по уровням риска (низкий, средний, высокий).

1.7. Оператор вправе ограничивать доступ и функционал Пользователей и Партнёров при наличии обоснованных подозрений нарушения условий Оферты или законодательства. Данные меры могут применяться автоматически.

2. СТАТУС ОПЕРАТОРА В СИСТЕМЕ ФИНАНСОВЫХ ОПЕРАЦИЙ

2.1. Оператор является технологической платформой, предоставляющей Пользователям и Партнерам техническую возможность для взаимодействия по оказанию/получению автоуслуг и реализации/приобретению автотоваров через Приложение.

2.2. Оператор не является кредитной организацией, платежным агентом, оператором по переводу денежных средств, оператором электронных денежных средств и не осуществляет прием, хранение или прямой перевод денежных средств Пользователей и Партнеров.

2.3. Оператор не относится к организациям, непосредственно подпадающей под обязательный контроль в соответствии с ФЗ №115-ФЗ. При этом Оператор применяет отдельные элементы процедур идентификации и мониторинга в целях предотвращения мошенничества, злоупотреблений и соблюдения требований законодательства.

2.4. Все расчеты между Пользователями и Партнерами (включая выплату Вознаграждений Партнёрам Партнёрской программы) осуществляются через сторонние лицензированные платежные сервисы (далее – Платежные Провайдеры), интегрированные в Приложение. Оператор направляет информационные данные Платежному Провайдеру в соответствии с Пользовательским соглашением, Публичной офертой для Партнеров и Публичной офертой об участии в Партнёрской программе.

2.5. Оператор не имеет доступа к полным реквизитам банковских карт Пользователей (таким как номер карты, срок действия, CVV). Обработка платежных данных осуществляется исключительно Платежным Провайдером в соответствии с требованиями стандартов безопасности платежных систем (PCI DSS).

3. ЦЕЛИ И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ СУБЪЕКТОВ ДАННЫХ (КУС)

3.1. Основными целями идентификации являются: а) подтверждение личности субъектов данных; б) проверка достоверности предоставленных сведений; в) предотвращение использования Приложения в незаконных целях, включая мошенничество, отмывание денег, финансирование терроризма, нарушения закона и злоупотребления; г) соблюдение требований применимого законодательства РФ, включая нормы ПОД/ФТ.

3.2. Оператор вправе запрашивать дополнительные сведения на любом этапе взаимодействия с субъектом данных. Дополнительная идентификация может проводиться при: превышении установленных внутренних пороговых значений операций, подозрительной активности, жалобах пользователей в случаях, предусмотренных законодательством РФ или правилами Платежного Провайдера.

3.3. Процедуры идентификации для Пользователей:

а) Первичная идентификация (при регистрации)

Оператор собирает минимально необходимые персональные данные, предусмотренные Пользовательским соглашением (адрес электронной почты (email), пароль, номер телефона (если указан), ФИО (если указаны в профиле), геолокационные данные (при наличии согласия Пользователя), данные об автомобиле).

б) Расширенная/дополнительная идентификация

В рамках дополнительной идентификации могут запрашиваться:

- Копии документов, удостоверяющих личность (паспорт гражданина РФ, водительское удостоверение), содержащие серию, номер, дату выдачи, орган выдачи, фотографию и подпись.
- Сведения о платежных средствах (без доступа к полным реквизитам банковских карт).
- Подтверждение адреса проживания (например, копия квитанции за коммунальные услуги).
- Иные данные, необходимые для соблюдения требований законодательства или предотвращения мошенничества. Обработка указанных данных осуществляется с соблюдением требований законодательства РФ о персональных данных и исключительно в целях, указанных в настоящей Политике. в) Проверка предоставленных Пользователем данных осуществляется по открытым источникам информации, а также может включать сверку данных с официальными государственными реестрами и/или через специализированные сервисы верификации.

3.4. Процедуры идентификации для Партнеров (юридических лиц и индивидуальных предпринимателей) и их представителей (включая Исполнителей и Партнёров Партнёрской программы):

а) Первичная идентификация (при регистрации)

Оператор собирает данные, предусмотренные Публичной офертой для Партнеров и Публичной офертой об участии в Партнёрской программе (полное наименование/ФИО, ИНН, ОГРН/ОГРНИП, КПП (для ЮЛ), юридический и фактический адреса, банковские реквизиты, контактные данные представителя (ФИО, email, телефон), выбранные специализации).

б) Обязательная и углубленная идентификация/верификация

Оператор осуществляет комплексную верификацию предоставленных Партнером данных, включая, но не ограничиваясь:

- Проверку юридического статуса Партнера по государственным реестрам (ЕГРЮЛ/ЕГРИП, реестр самозанятых).
- Проверку банковских реквизитов.
- Анализ деловой репутации Партнера по открытым источникам, негативных отзывов.
- Запрос копий учредительных и регистрационных документов (устав, выписки, свидетельства, лицензии, сертификаты, разрешения на ведение деятельности).
- Запрос копий документов, удостоверяющих личность представителя Партнера (паспорт гражданина РФ), содержащих серию, номер, дату выдачи, орган выдачи, фотографию и подпись.
- Проверка полномочий представителя Партнера (доверенность, приказ о назначении).
- Иные сведения, необходимые для соблюдения требований законодательства РФ (включая ФЗ-115) или предотвращения мошенничества. Обработка указанных данных осуществляется с соблюдением требований законодательства РФ о персональных данных и исключительно в целях, указанных в настоящей Политике.

3.5. В случае отказа субъекта данных (Пользователя, Партнера, представителя Партнера) предоставить запрошенные сведения/документы в случаях, предусмотренных законодательством РФ или правилами Платежного Провайдера, или если предоставленные данные вызывают обоснованные сомнения в их достоверности, Оператор вправе: а) Ограничить или полностью прекратить доступ к функционалу Приложения или Партнёрской программы. Данные меры могут применяться автоматически. б) Направить Платежному Провайдеру информацию для приостановки расчетов. в) Заблокировать учетную запись субъекта данных. г) Отказать в дальнейшем сотрудничестве или регистрации.

4. МОНИТОРИНГ ОПЕРАЦИЙ И ВЫЯВЛЕНИЕ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ (AML)

4.1. Оператор вправе осуществлять мониторинг активности Пользователей, Партнеров и Участников Партнёрской программы в Приложении с целью выявления признаков мошенничества, нарушений условий использования Приложения/Программы и законодательства РФ, а также действий, которые могут быть расценены как подозрительные в контексте ПОД/ФТ.

4.2. Мониторинг осуществляется с использованием автоматизированных систем анализа и включает, но не ограничивается, следующие аспекты: а) Анализ транзакций (частота, объемы, характер, география, суммы). б) Выявление аномалий в поведении субъектов данных (например, резкие изменения активности, подозрительная частота операций). в) Отслеживание попыток обхода правил Приложения или системы оплаты. г) Мониторинг использования нескольких учетных записей или связанных аккаунтов. д) Анализ жалоб и обращений других Пользователей/Партнеров/Партнёров Партнёрской программы. е) Мониторинг отзывов, рейтингов и качества оказываемых услуг. ж) Анализ IP-адресов, геолокации и истории доступа к Приложению при наличии согласия субъекта персональных данных. з) Проверка на участие в списках лиц, причастных к экстремистской деятельности или терроризму, а также в списках подозрительных операций.

4.3. Оператор вправе применять внутренние алгоритмы оценки риска (скоринг), основанные на совокупности факторов поведения, транзакционной активности и иных параметров, что не влечет юридически значимых последствий без участия человека, Окончательные решения, имеющие юридические последствия для субъекта данных, принимаются с участием уполномоченного сотрудника Оператора.

4.4. Оператор вправе использовать автоматизированные антифрод-системы для выявления подозрительной активности.

5. ПРИЗНАКИ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ

5.1. К признакам подозрительной активности могут относиться, но не ограничиваются ими: а) Попытки использования Приложения в незаконных целях (например, для легализации преступных доходов, финансирования терроризма, киберпреступлений). б) Предоставление недостоверных, неполных или противоречивых данных при регистрации, в процессе идентификации или в профиле. в) Резкие и необоснованные изменения в характере активности (например, внезапный значительный рост объемов Заказов/операций/привлечений без объективных причин, не характерный для обычного поведения). г) Многочисленные или необоснованные отказы от Заказов, инициирование возвратов или оспаривание транзакций. д) Попытки обхода системы оплаты Приложения, прямое взаимодействие с целью уклонения от комиссии или Вознаграждения. е) Использование учетной записи, не соответствующее заявленному профилю деятельности (например, регистрация как ИП, но выполнение заказов, не соответствующих ОКВЭД). ж) Поступление большого количества однотипных или серьезных жалоб от других Пользователей/Партнеров. з) Признаки манипуляции рейтингами, отзывами, количеством Заказов или привлечений. и) Необычные или нестандартные запросы на вывод средств или совершение операций. к) Использование поддельных документов или данных.

6. МЕРЫ РЕАГИРОВАНИЯ НА ПОДОЗРИТЕЛЬНУЮ АКТИВНОСТЬ И НАРУШЕНИЯ

6.1. В случае выявления признаков подозрительной активности, нарушений условий использования Приложения/Программы или требований законодательства, Оператор вправе при наличии обоснованных оснований полагать нарушение условий использования Приложения или требований законодательства: а) Ограничить или временно приостановить доступ субъекта данных к функционалу Приложения или Партнёрской программы с уведомлением. б) Направить информацию Платежному Провайдеру для приостановки операций. в) Запросить дополнительные сведения или

документы для проведения углубленной проверки (due diligence). г) Заблокировать учетную запись субъекта данных. д) Аннулировать рассчитанное Вознаграждение (для Партнёров Партнёрской программы) или Заказы/операции, связанные с выявленными нарушениями. е) Отменить все активные Заказы. ж) Передавать информацию в уполномоченные государственные органы в случаях и порядке, предусмотренных законодательством Российской Федерации. з) Привлечь виновное лицо к гражданско-правовой ответственности, потребовать полного возмещения убытков, причиненных Оператору.

7. ВЗАИМОДЕЙСТВИЕ С ПЛАТЕЖНЫМИ ПРОВАЙДЕРАМИ

7.1. Оператор взаимодействует с Платежными Провайдерами, которые осуществляют фактическую обработку платежей, резервирование, списание и перечисление денежных средств между всеми участниками Приложения.

7.2. Оператор в рамках своих полномочий предоставляет Платежному Провайдеру необходимую информацию для проведения транзакций, а также направляет информацию для приостановки, удержания или возврата средств в соответствии с условиями Пользовательского соглашения, Публичной оферты для Партнеров, Публичной оферты об участии в Партнёрской программе и настоящей Политики КУС/AML.

7.3. Субъект данных понимает и соглашается, что Платежный Провайдер может самостоятельно осуществлять свои собственные процедуры идентификации и верификации, а также мониторинг операций в соответствии с законодательством и внутренними правилами Платежного Провайдера, и Оператор не несет за это ответственности.

8. КОНФИДЕНЦИАЛЬНОСТЬ, ХРАНЕНИЕ И ЗАЩИТА ДАННЫХ

8.1. Персональные данные субъектов данных, собранные в рамках настоящей Политики КУС/AML, обрабатываются, хранятся и защищаются Оператором в строгом соответствии с Политикой обработки персональных данных Оператора.

8.2. Сроки хранения данных, полученных в рамках процедур КУС/AML, определяются с учетом требований законодательства РФ о ПОД/ФТ (не менее 5 лет с даты прекращения отношений с клиентом) и иного применимого законодательства.

8.3. Оператор принимает все необходимые правовые, организационные и технические меры для защиты персональных данных от несанкционированного или неправомерного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

8.4. Оператор ведет учет и хранение информации о действиях субъектов данных (логирование) в целях обеспечения безопасности, разрешения споров и соблюдения законодательства.

8.5. Все решения, принятые в рамках КУС/AML, фиксируются и могут быть проверены (audit trail).

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящая Политика КУС/AML является обязательной для всех сотрудников Оператора, имеющих отношение к обработке персональных данных и взаимодействию с субъектами данных.

9.2. Любые вопросы, касающиеся настоящей Политики КУС/AML, могут быть направлены Оператору по адресу электронной почты support@profitdrive.pro.

10. Реквизиты Оператора: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ПРОФИТДРАЙВ" ИНН 5250072720 КПП 525001001 ОГРН 1195275051476 Юридический адрес: 607693, Нижегородская Область, г Нижний Новгород, д. Подлесово, д. 28, кв. 24 Генеральный директор Винокуров М.А.