X2PROXY

Политика конфиденциальности

Дата вступления в силу: 1 августа 2026 г.

Настоящий документ является переводом официальной версии на английском языке и предоставлен для удобства пользователей. Соотношение языковых версий определяется в порядке, предусмотренном разделом 22 Пользовательского соглашения; Провайдер вправе определить приоритетную языковую версию в отдельном официальном уведомлении.

Оператор сервиса и оператор данных: бренд x2proxy и лицо (лица), фактически осуществляющее администрирование, поддержку, комплаенс-контроль, обработку данных и предоставление доступа к сервису x2proxy, до возможной регистрации юридического лица и/или публикации иных официальных идентификационных данных («Провайдер»).

Контакты: privacy@x2proxy.com — вопросы конфиденциальности и юридически значимые уведомления; support@x2proxy.com — поддержка, включая вопросы оплаты, возврата средств и злоупотреблений; чат поддержки — https://t.me/x2proxysupport; официальный канал — https://t.me/x2proxynews.

Пользователь: физическое лицо, индивидуальный предприниматель, юридическое лицо или иное лицо, использующее сервис x2proxy («Пользователь»).

Настоящая Политика конфиденциальности описывает, какие данные могут обрабатываться при использовании сервиса x2proxy, для каких целей они используются, кому могут передаваться и какими правами обладает Пользователь.

Используя Сервис, Пользователь подтверждает, что ознакомился с настоящей Политикой. Если применимое право требует отдельного согласия на определённые виды обработки, такое согласие запрашивается отдельно, и настоящая Политика его не заменяет.

Провайдер вправе обновлять настоящую Политику. Обновлённая версия вступает в силу с даты, указанной в ней, либо с момента публикации в Сервисе, если иное не предусмотрено императивными нормами права.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цель и статус Политики

1.1.1. Настоящая Политика конфиденциальности регулирует сбор, использование, хранение, раскрытие, защиту и иную обработку данных Пользователей при использовании Сервиса x2proxy.

1.1.2. Политика применяется ко всем формам взаимодействия с Сервисом, включая регистрацию аккаунта, использование прокси-соединений, работу через API, управление субаккаунтами, использование личного кабинета, осуществление платежей, получение бонусного трафика, взаимодействие с Telegram-ботом, обращения в поддержку и получение уведомлений.

1.1.3. Настоящая Политика является неотъемлемой частью условий использования Сервиса и применяется совместно с Пользовательским соглашением, Политикой допустимого использования, Политикой возврата средств и иными документами Провайдера.

1.2. Применимые основания обработки

1.2.1. Провайдер не исходит из того, что любое использование Сервиса автоматически означает универсальное согласие Пользователя на любую обработку данных.

1.2.2. В зависимости от характера обработки Провайдер может ссылаться на необходимость исполнения договора, законные интересы, соблюдение требований применимого права, защиту прав Провайдера или согласие Пользователя, если такое согласие требуется.

1.2.3. Если для отдельных категорий обработки или технологий отслеживания требуется отдельное согласие, оно запрашивается отдельно через соответствующий интерфейс, настройки, баннер или иной допустимый механизм.

1.3. Принципы обработки данных

1.3.1. Провайдер стремится обрабатывать данные законно, добросовестно и прозрачно, в объёме, разумно необходимом для функционирования Сервиса, обеспечения безопасности, исполнения договорных обязательств и соблюдения применимого права.

1.3.2. При обработке данных Провайдер придерживается принципов минимизации данных, ограничения цели, ограничения срока хранения, разумной достаточности, а также конфиденциальности и целостности информации.

1.4. Характер обработки

1.4.1. Обработка данных может осуществляться автоматизированными и неавтоматизированными способами.

1.4.2. Провайдер вправе осуществлять сбор, систематизацию, запись, хранение, использование, передачу, ограничение, удаление, обезличивание и иные операции с данными в объёме, необходимом для достижения целей, указанных в настоящей Политике.

1.5. Общие оговорки

1.5.1. Настоящая Политика применяется в максимально допустимом объёме с учётом императивных норм применимого права о защите данных и электронных коммуникациях.

1.5.2. В случае противоречия между настоящей Политикой и императивными нормами права приоритет имеют такие императивные нормы в соответствующей части.

2. КАКИЕ ДАННЫЕ МЫ СОБИРАЕМ

2.1. Общий объём собираемых данных

2.1.1. Провайдер собирает и иным образом обрабатывает только те категории данных, которые необходимы для функционирования Сервиса, учёта потребления трафика, обеспечения безопасности, обработки платежей, рассмотрения обращений, аналитики, бонусных механик и соблюдения требований законодательства.

2.2. Категории собираемых данных

2.2.1. Данные аккаунта могут включать адрес электронной почты, внутренний идентификатор Пользователя, пароль в виде криптографического хеша (если хранение паролей предусмотрено архитектурой авторизации), настройки аккаунта, данные о субаккаунтах, API-ключи, историю входов, историю заказов и покупок, а также иную информацию, необходимую для администрирования Аккаунта.

2.2.2. Технические данные о соединении и использовании могут включать IP-адрес Пользователя, IP-адрес запрашивающей стороны (клиентский IP), данные об устройстве и браузере, user-agent, операционную систему, языковые и региональные настройки, часовой пояс, идентификаторы сессии, временные метки входов, параметры соединения и технические метаданные взаимодействия с интерфейсом, API и функциями прокси.

2.2.3. Данные журналирования прокси-соединений могут включать идентификаторы событий, идентификаторы Пользователя и субаккаунта, идентификаторы прокси-сессии и прокси-пользователя, источник запроса, целевой домен или IP-адрес, целевой порт, выбранную геолокацию, временные метки, статус выполнения запроса, объём трафика, направление трафика, IP-адрес клиента и IP-адрес прокси.

2.2.4. Платёжные данные могут включать адрес кошелька, идентификатор транзакции (tx hash), выбранную сеть, маскированный номер и тип платёжной карты, наименование способа оплаты, идентификатор платежа на стороне поставщика платёжных услуг, сумму, время и статус транзакции, результат риск/фрод-скрининга, IP-адрес и user-agent на момент оплаты, а также иную ограниченную техническую информацию, необходимую для зачисления средств, биллинга и управления рисками. Провайдер не получает и не хранит полный номер платёжной карты, код проверки подлинности карты и данные аутентификации, используемые для подтверждения платежа.

2.2.5. Данные KYC и ограниченных доменов могут включать статус верификации (пройдена / не пройдена / на рассмотрении или аналогичный), референс-ID сервиса, ограниченные риск-флаги, информацию о целях, для которых Пользователь запрашивает разблокировку домена, перечень запрошенных доменов и статус предоставленного доступа к таким доменам. Провайдер не получает от поставщика KYC полный комплект документов Пользователя, если прямо не указано иное.

2.2.6. Данные поддержки и коммуникаций могут включать адрес электронной почты, имя пользователя и/или ID в Telegram, содержание сообщений, вложения, скриншоты, историю обращений, технические журналы, информацию о каналах связи и иные данные, добровольно предоставленные Пользователем при обращении в поддержку или взаимодействии с официальными каналами сервиса.

2.2.7. Данные аналитики и cookie-файлов могут включать статистику посещений, данные о действиях в интерфейсе, данные сессии, реферальные данные или данные атрибуции, идентификаторы локального хранилища, пиксельные события, сигналы безопасности/антифрода, а также агрегированные или псевдонимизированные метрики использования Сервиса.

2.2.8. Данные, относящиеся к Telegram-бонусу и промо-механикам, могут включать факт и статус подписки на Telegram-канал, идентификаторы Telegram-бота, информацию, связывающую взаимодействие в Telegram с Аккаунтом в Сервисе, а также данные, необходимые для предотвращения повторного или недобросовестного получения бонусного трафика.

2.3. Источники данных

2.3.1. Данные могут поступать непосредственно от Пользователя, автоматически при использовании Сервиса, от платёжных и KYC-провайдеров, от инструментов аналитики, поддержки, безопасности и противодействия мошенничеству, а также из жалоб, сообщений о злоупотреблениях или иных обращений третьих лиц, если это необходимо для обеспечения работы и безопасности Сервиса.

2.4. Минимизация данных

2.4.1. Провайдер стремится не собирать избыточные данные, не связанные с фактическим функционированием Сервиса или его защитой, и ограничивает объём обработки разумно необходимым минимумом.

3. ДАННЫЕ ЖУРНАЛИРОВАНИЯ

3.1. Общие положения

3.1.1. Провайдер журналирует технические параметры использования Сервиса в объёме, необходимом для учёта потребления трафика, обеспечения безопасности, расследования инцидентов, предотвращения злоупотреблений и соблюдения требований законодательства.

3.1.2. Журналирование носит технический и операционный характер и не направлено на анализ содержимого данных, передаваемых Пользователем.

3.2. Состав журналируемых данных

3.2.1. В рамках функционирования Сервиса могут фиксироваться: уникальный идентификатор события; внутренний ID пользователя; ID субпользователя; ID прокси-сессии; ID прокси-пользователя; исходный/клиентский IP; целевой домен или целевой IP; целевой порт; выбранная страна, регион, штат, город или иные доступные гео-параметры; объём трафика; временные метки; статус/успех/сбой; направление трафика; технические параметры соединения; используемые порты; и иные сервисные атрибуты запроса.

3.3. Цели использования журналов

3.3.1. Указанные данные используются для обеспечения корректной работы Сервиса, учёта потребления трафика и биллинга, выявления и предотвращения злоупотреблений, обеспечения безопасности инфраструктуры, диагностики сбоев, проведения внутренних проверок, разрешения споров и соблюдения обязательных требований законодательства.

3.4. Ограничения на использование журналов

3.4.1. Журналы не используются для анализа содержимого трафика Пользователя и не предназначены для скрытого мониторинга содержания сетевых взаимодействий.

3.4.2. Провайдер вправе использовать технические, поведенческие и риск-сигналы для антифрод- и антизлоупотребительного анализа, но не осуществляет скрытое профилирование на основе содержимого проксируемого трафика.

3.5. Журналы поставщиков сервисной инфраструктуры

3.5.1. Отдельные технические поставщики, обеспечивающие работу определённых компонентов Сервиса, могут вести собственные сервисные журналы и использовать ограниченные данные, необходимые для маршрутизации, учёта, безопасности, диагностики и поддержки соответствующих функций. Такая обработка ограничена стандартными техническими задачами и осуществляется в объёме, необходимом для оказания сервисных услуг Провайдеру.

4. МЫ НЕ ХРАНИМ СОДЕРЖИМОЕ ТРАФИКА

4.1. Общий принцип

4.1.1. Провайдер не собирает, не хранит и не анализирует содержимое проксируемого трафика Пользователя.

4.1.2. Обработка ограничена техническими метаданными соединения, необходимыми для маршрутизации, учёта использования, безопасности, диагностики и поддержки Сервиса.

4.2. Что именно не хранится в качестве содержимого трафика

4.2.1. В рамках обычного функционирования Сервиса не хранятся: тело запроса/payload; содержимое ответа; тексты форм и сообщений, передаваемых через прокси; HTML- или API-содержимое целевых ресурсов; содержимое страниц; учётные данные, передаваемые в рамках проксируемых запросов; а также иные данные, позволяющие восстановить фактическое содержание трафика.

4.3. Транзитный характер обработки

4.3.1. Сервис функционирует как механизм маршрутизации и обработки сетевых запросов в транзитном режиме, без хранения содержимого такого трафика.

4.4. Исключения

4.4.1. Настоящий Раздел не распространяется на данные, которые Пользователь добровольно предоставляет при регистрации, оплате, обращении в поддержку, через Telegram-бота, систему обращений или иные официальные каналы Сервиса, поскольку такие данные не являются содержимым проксируемого трафика.

4.5. Ответственность за содержание передаваемой информации

4.5.1. Пользователь самостоятельно несёт ответственность за содержание данных, которые он передаёт через Сервис, и за правомерность соответствующих сценариев использования.

5. ЦЕЛИ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ДАННЫХ

5.1. Общие положения

5.1.1. Провайдер обрабатывает данные исключительно в конкретных и законных целях, связанных с предоставлением Сервиса, обеспечением безопасности, аналитикой, коммуникациями, исполнением обязательств перед Пользователем и соблюдением применимого права.

5.1.2. Если это требуется применимым правом о защите данных, правовыми основаниями обработки могут являться необходимость исполнения договора, совершение действий по запросу Пользователя до заключения договора, законные интересы Провайдера и/или третьих лиц, соблюдение применимого права, защита прав Провайдера и согласие Пользователя, если оно требуется.

5.2. Предоставление услуг и управление аккаунтом

5.2.1. Данные обрабатываются для создания и ведения Аккаунта, управления субаккаунтами, API-ключами и авторизацией, предоставления доступа к функциям прокси, маршрутизации запросов, отображения статистики, применения лимитов и обеспечения работы личного кабинета. В применимых случаях данное основание включает необходимость исполнения договора или совершение действий по запросу Пользователя до его заключения.

5.3. Учёт трафика, биллинг и платежи

5.3.1. Данные обрабатываются для учёта объёма трафика, управления балансом, применения сроков действия пакетов, подтверждения платежей, зачисления средств, предотвращения ошибочных или подозрительных транзакций и ведения сервисного учёта. В применимых случаях обработка основана на исполнении договора, законных интересах и/или императивных требованиях законодательства.

5.4. Безопасность, противодействие мошенничеству и злоупотреблениям

5.4.1. Данные обрабатываются для защиты Сервиса, инфраструктуры, Пользователей и третьих лиц от злоупотреблений, мошенничества, подозрительной активности, сетевых атак, попыток обхода ограничений и нарушений Соглашения, AUP и иных правил. В применимых случаях обработка основана на законных интересах Провайдера и на необходимости соблюдения закона и защиты прав Провайдера.

5.5. KYC, ограниченные домены и проверка сценария использования

5.5.1. Данные обрабатываются для принятия решений о доступе к отдельным ограниченным функциям и доменам, проведения KYC, оценки заявленного сценария использования, управления рисками, обеспечения комплаенса и ограничения недопустимых сценариев использования. В применимых случаях данное основание включает законные интересы, соблюдение закона и защиту прав и безопасности Провайдера.

5.6. Поддержка и сервисные уведомления

5.6.1. Данные обрабатываются для обработки обращений, ответов на запросы, устранения неполадок и направления уведомлений об аккаунте, безопасности, платежах, сроках действия пакетов, статусе запросов на ограниченные домены, доступе к функциям и иных обязательных сервисных уведомлений. Такие уведомления не считаются маркетинговыми.

5.7. Аналитика и развитие продукта

5.7.1. Данные могут обрабатываться для анализа использования Сервиса, улучшения интерфейса, тестирования функциональности, выявления ошибок и оценки стабильности и эффективности продукта. Если это требуется применимым правом, неосновная аналитика и аналогичные технологии активируются только после получения соответствующего согласия.

5.8. Маркетинговые, комьюнити- и промо-коммуникации

5.8.1. Провайдер вправе использовать контактные данные и доступные каналы связи для направления маркетинговых сообщений, новостей о продукте, акций, промо-предложений, сообщений о Telegram-канале и иных коммуникаций рекламного или информационного характера. Если это требуется применимым правом, такие сообщения направляются на основании предварительного согласия; в иных случаях Провайдер вправе опираться на иные допустимые законом основания. Пользователь вправе отказаться от маркетинговых сообщений, однако такой отказ не распространяется на обязательные сервисные уведомления.

5.9. Право, защита прав и разрешение споров

5.9.1. Данные могут обрабатываться для соблюдения применимого права, взаимодействия с компетентными органами, исполнения обязательных запросов, проведения расследований, защиты прав Провайдера, урегулирования претензий и споров, а также установления, осуществления и защиты юридических требований.

5.10. Ограничения на использование данных

5.10.1. Провайдер не продаёт персональные данные Пользователей.

5.10.2. Провайдер не использует данные для анализа содержимого проксируемого трафика и не формирует скрытый профиль Пользователя на основе такого содержимого.

5.10.3. Провайдер вправе использовать ограниченные технические и коммуникационные данные для управления доступом, безопасности, принятия решений по противодействию злоупотреблениям, коммуникаций и промо-механик, однако такая обработка должна оставаться соразмерной целям Сервиса.

6. KYC И ВЕРИФИКАЦИЯ

6.1. Общие положения

6.1.1. Процедура KYC не является обязательной для всех Пользователей и применяется по усмотрению Провайдера, в том числе в случаях подозрительной активности, запроса доступа к ограниченным доменам, повышенного уровня риска, нестандартного сценария использования либо наличия финансовых, репутационных или юридических рисков.

6.2. Порядок проведения KYC

6.2.1. KYC может проводиться через стороннюю службу идентификации и комплаенса. Провайдер не хранит полный комплект документов, предоставленных Пользователем внешнему поставщику KYC, если это прямо не требуется законом или не связано с отдельной процедурой.

6.2.2. По результатам такой верификации Провайдер, как правило, получает ограниченный набор информации: статус верификации, идентификатор сервиса, отдельные риск-флаги, информацию о заявленном сценарии использования и информацию, необходимую для принятия решения о доступе к запрошенным доменам или функциям.

6.3. Ограниченные домены и проверка сценария использования

6.3.1. Для открытия доступа к отдельным ограниченным доменам Провайдер вправе обрабатывать запрос Пользователя, описание предполагаемого сценария использования, перечень доменов, переписку по обращению, статус KYC и статус ранее открытых доменов.

6.3.2. Такие данные используются исключительно для принятия решения о предоставлении, ограничении или отказе в доступе к соответствующим функциям или доменам.

6.4. Отказ от KYC

6.4.1. Пользователь вправе отказаться от прохождения KYC. Отказ от KYC сам по себе не влечёт автоматического удаления аккаунта или полной блокировки доступа ко всему Сервису, однако доступ к отдельным ограниченным функциям или ограниченным доменам может быть недоступен.

6.4.2. Если действия Пользователя создают финансовые, юридические, репутационные или иные существенные риски, либо имеются основания полагать, что использование Сервиса нарушает правила или закон, Провайдер вправе временно заморозить аккаунт, ограничить отдельные функции, отложить рассмотрение запроса или инициировать дополнительную верификацию.

7. ПЛАТЁЖНЫЕ ДАННЫЕ

7.1. Общие положения

7.1.1. По состоянию на момент подготовки настоящей Политики Сервис поддерживает оплату в криптовалюте, а также оплату банковской картой, переводы через системы быстрых платежей и иные способы, доступные в интерфейсе, через сторонние инструменты и сервисы, обеспечивающие приём, подтверждение, анализ и обработку транзакций.

7.1.2. Провайдер не хранит данные банковских карт и не получает доступа к средствам Пользователя в его кошельке.

7.2. Категории платёжных данных

7.2.1. В рамках обработки платежей в криптовалюте Провайдер вправе фиксировать адрес кошелька, tx hash, сеть, сумму, дату и время, статус транзакции, IP-адрес, user-agent, языковые параметры, идентификаторы сервисной транзакции, оценку риска и иную ограниченную техническую информацию, необходимую для учёта и обеспечения безопасности платежей.

7.3. Цели обработки платёжных данных

7.3.1. Платёжные данные обрабатываются для подтверждения и зачисления платежа, управления балансом, ведения биллинга, предотвращения мошенничества, разрешения платёжных споров, соблюдения требований законодательства и защиты прав Провайдера.

7.4. Верификация платежей и управление рисками

7.4.1. Провайдер вправе использовать технические инструменты и данные от платёжных партнёров для проверки транзакций, выявления аномальной активности, управления рисками и предотвращения chargeback-подобных злоупотреблений, мошеннического пополнения баланса, сетевых ошибок и иных аномалий.

7.4.2. При выявлении риска Провайдер вправе приостановить зачисление средств, запросить дополнительную информацию, ограничить доступ к Сервису или инициировать дополнительную верификацию.

7.5. Сроки хранения и передача

7.5.1. Платёжные метаданные хранятся в течение срока, указанного в настоящей Политике, и могут передаваться платёжным, аналитическим и комплаенс-сервисам в объёме, необходимом для обработки транзакции, проверки рисков, учёта и соблюдения требований законодательства.

7.6. Ограничение ответственности

7.6.1. Платёжные операции через блокчейн и внешние сервисы зависят от выбранной сети, подтверждений, стабильности сторонних инструментов и корректности действий самого Пользователя. Порядок обработки таких транзакций может дополнительно регулироваться правилами соответствующих сервисов.

7.7. Данные платежей, совершаемых иным способом, чем в криптовалюте

7.7.1. Платежи банковской картой, переводы через системы быстрых платежей и иные некриптовалютные способы оплаты совершаются на платёжной странице или в платёжной форме стороннего поставщика платёжных услуг. Реквизиты платёжного инструмента вводятся Пользователем на стороне такого лица и не проходят через интерфейс Провайдера.

7.7.2. В отношении таких платежей Провайдер получает ограниченные данные: маскированный номер и тип платёжной карты, наименование способа оплаты, идентификатор платежа на стороне поставщика платёжных услуг, сумму, валюту, дату, статус операции и результат проверки риска. Полный номер платёжной карты, код проверки подлинности карты и данные аутентификации, используемые для подтверждения платежа, Провайдеру не передаются и им не хранятся.

7.8. Роль поставщика платёжных услуг

7.8.1. Поставщик платёжных услуг, банк-эквайер и платёжная система самостоятельно определяют цели и способы обработки данных плательщика, которые они собирают сами для осуществления перевода, соблюдения обязательных требований законодательства и управления рисками, и действуют в этой части независимо от Провайдера и в соответствии со своими документами.

7.8.2. Провайдер передаёт таким лицам минимальный объём данных, необходимый для совершения и идентификации платежа, и получает от них данные, указанные в пункте 7.7.2.

7.8.3. Сроки хранения данных плательщика на стороне поставщика платёжных услуг, банка-эквайера или платёжной системы, а также порядок реализации прав в отношении таких данных определяются документами этих лиц.

8. COOKIE-ФАЙЛЫ, АНАЛИТИКА И ИНТЕГРАЦИИ С TELEGRAM

8.1. Используемые технологии

8.1.1. Сервис вправе использовать cookie-файлы и аналогичные технологии, включая строго необходимые cookie-файлы, cookie-файлы аутентификации/сессии, cookie-файлы предпочтений, аналитические cookie-файлы, cookie-файлы безопасности, реферальные идентификаторы или идентификаторы атрибуции, локальное хранилище, пиксели, технические антифрод-скрипты и иные аналогичные средства, используемые для работы, анализа и защиты Сервиса.

8.1.2. В зависимости от конфигурации Сервиса могут использоваться как собственные, так и сторонние инструменты аналитики, продуктовой аналитики, атрибуции, отслеживания производительности, а при необходимости — рекламные или маркетинговые пиксели.

8.2. Цели использования cookie-файлов и аналитики

8.2.1. Такие технологии могут использоваться для аутентификации, управления сессиями, сохранения настроек, обеспечения безопасности, защиты от злоупотреблений, анализа использования интерфейса, улучшения функциональности, диагностики ошибок и измерения эффективности источников трафика и коммуникаций.

8.3. Управление согласием и настройками

8.3.1. Строго необходимые и иные технологии, использование которых допускается без отдельного согласия, могут применяться автоматически в объёме, допускаемом законом.

8.3.2. Аналитические, маркетинговые и иные неосновные технологии включаются только при наличии согласия Пользователя в случаях, когда такое согласие требуется применимым правом. Для этого Сервис вправе использовать cookie-баннер, менеджер согласий, центр настроек или аналогичный механизм управления настройками.

8.3.3. Пользователь вправе в любое время изменить настройки cookie-файлов через доступный интерфейс, настройки браузера или иные средства управления, если они доступны в конкретной конфигурации Сервиса.

8.4. Сторонние инструменты аналитики и маркетинга

8.4.1. В зависимости от конфигурации продукта Провайдер вправе использовать собственную аналитику, решения, аналогичные Google Analytics, инструменты продуктовой аналитики, системы отслеживания событий, рекламные и атрибуционные инструменты и иные технические средства анализа или коммуникации. Конкретный перечень используемых инструментов может изменяться.

8.4.2. Провайдер стремится ограничивать объём данных, передаваемых таким инструментам, использовать по возможности агрегированные, псевдонимизированные или иным образом минимизированные данные и не использовать такие инструменты для анализа содержимого проксируемого трафика.

8.5. Telegram-бонус и Telegram-бот

8.5.1. Для предоставления бонусного трафика, связанного с подпиской на Telegram-канал, Провайдер вправе использовать Telegram-бота и иные интеграции с Telegram.

8.5.2. В рамках таких механик могут обрабатываться: имя пользователя в Telegram, ID в Telegram, факт и статус подписки на канал, техническая информация о взаимодействии с ботом, информация, связывающая аккаунт в Telegram с аккаунтом в Сервисе, а также данные, необходимые для предотвращения повторного или недобросовестного получения бонуса.

8.5.3. Данные Telegram-интеграции могут использоваться для подтверждения выполнения условий бонуса, поддержания каналов связи с Пользователем, учёта источников коммуникации, предотвращения злоупотреблений и направления дополнительных уведомлений о работе Сервиса.

8.5.4. Взаимодействие Пользователя с Telegram также регулируется собственными политиками и правилами Telegram, на которые Провайдер не может полностью влиять.

8.6. Сроки хранения

8.6.1. Срок хранения cookie-файлов и связанных с ними аналитических данных зависит от категории технологии и её назначения. Строго необходимые cookie-файлы могут храниться в течение сессии или иного срока, разумно необходимого для работы Сервиса; аналитические и аналогичные данные, если иное не указано в конкретном интерфейсе, хранятся в сроки, указанные в настоящей Политике, либо в иной, более короткий или более длительный срок, обоснованный категорией cookie-файла, законными интересами безопасности или требованиями законодательства.

9. СРОКИ ХРАНЕНИЯ ДАННЫХ

9.1. Общие положения

9.1.1. Провайдер хранит данные в течение срока, необходимого для достижения целей обработки, обеспечения безопасности, разрешения споров, предотвращения злоупотреблений и соблюдения требований законодательства.

9.2. Базовые сроки хранения

9.2.1. Если иной срок не требуется законом, отдельной процедурой или предписанием о сохранении данных, применяются следующие ориентировочные сроки хранения: (a) данные журналирования, технические данные соединения, журналы безопасности и противодействия злоупотреблениям — до 730 дней; (b) платёжные метаданные, информация о транзакциях и иные платёжные журналы — до 365 дней; (c) данные cookie-файлов и аналитики — до 180 дней, если иное не определено категорией cookie-файла или настройками конкретного инструмента; (d) обращения в поддержку, сообщения и иные коммуникации с Пользователем — до 365 дней.

9.2.2. Данные аккаунта могут храниться в течение срока действия аккаунта и разумного периода после его удаления в объёме, необходимом для биллинга, безопасности, предотвращения злоупотреблений, разрешения споров, соблюдения комплаенс-требований и защиты прав Провайдера.

9.3. Продление сроков хранения

9.3.1. Провайдер вправе продлить срок хранения отдельных данных при наличии спора, расследования, внутренней проверки, предписания о сохранении данных, запроса правоохранительных органов, комплаенс-требования, необходимости защиты прав Провайдера, необходимости предотвращения злоупотреблений или иных разумных оснований безопасности.

9.4. Удаление и обезличивание

9.4.1. По истечении применимого срока данные удаляются, деидентифицируются или обезличиваются в разумный срок, если их дальнейшее хранение не требуется законом или для защищаемой законом цели.

9.5. Хранение после удаления аккаунта

9.5.1. Удаление аккаунта не означает немедленного удаления всех данных. Отдельные категории данных, включая журналы, данные безопасности, биллинга и переписки, а также иные сервисные записи, могут храниться в установленные сроки и в целях, допускаемых законом.

9.6. Хранение подтверждений для платёжных споров

9.6.1. Данные, подтверждающие предоставление Сервиса и получение оплаты, включая записи биллинга, журналы потребления трафика, идентификаторы операций и переписку с Пользователем, хранятся не менее шести месяцев с даты операции в целях рассмотрения запросов на возврат средств и споров, инициированных через банк, платёжную систему или поставщика платёжных услуг.

9.6.2. Если такой спор инициирован, срок хранения соответствующих данных может быть продлён до его разрешения в соответствии с пунктом 9.3.1.

10. РАСКРЫТИЕ ДАННЫХ

10.1. Общие положения

10.1.1. Провайдер вправе раскрывать данные Пользователя только в случаях, прямо предусмотренных настоящей Политикой, применимым правом, запросами компетентных органов, обязательными решениями, а также если это необходимо для защиты прав, интересов и безопасности Провайдера, Пользователей, третьих лиц или инфраструктуры Сервиса.

10.2. Основания для раскрытия

10.2.1. Данные могут раскрываться: (a) по законному и надлежащим образом оформленному запросу государственного, судебного или иного уполномоченного органа; (b) для предотвращения, расследования или пресечения мошенничества, злоупотреблений, нарушений Соглашения/AUP, угроз безопасности или иных неправомерных действий; (c) для защиты прав и законных интересов Провайдера; (d) если это необходимо для исполнения договора или обеспечения работы отдельных компонентов Сервиса; (e) в иных случаях, допускаемых законом.

10.3. Объём раскрытия

10.3.1. При раскрытии данных Провайдер руководствуется принципом минимизации и передаёт только тот объём информации, который объективно необходим для достижения соответствующей цели.

10.3.2. По общему правилу раскрытие может включать технические журналы, IP-адреса, временные метки, статусы действий, идентификаторы сервиса, платёжные метаданные, статус KYC, записи поддержки и иную ограниченную техническую или учётную информацию.

10.3.3. Провайдер не раскрывает содержимое проксируемого трафика, поскольку такие данные не собираются и не хранятся в рамках обычного функционирования Сервиса.

10.4. Оценка запросов и уведомление

10.4.1. Провайдер вправе оценивать законность и обоснованность поступающих запросов и, если это допускается законом, ограничивать или отклонять избыточные, неопределённые или неподтверждённые запросы.

10.4.2. Уведомление Пользователя о раскрытии данных может не осуществляться, если это запрещено законом, может помешать расследованию, создать риск безопасности или иным образом противоречить защищаемой цели раскрытия.

11. ТРЕТЬИ ЛИЦА И МЕЖДУНАРОДНЫЕ ПЕРЕДАЧИ ДАННЫХ

11.1. Категории третьих лиц

11.1.1. Для функционирования Сервиса Провайдер вправе привлекать сторонних поставщиков технических, платёжных, комплаенс-, аналитических, коммуникационных, сервисных и иных услуг.

11.1.2. К таким категориям могут относиться, в частности: платёжные и транзакционные сервисы; поставщики KYC и комплаенс-услуг; технические, сетевые, инфраструктурные поставщики и поставщики услуг безопасности; поставщики аналитики и продуктовой аналитики; поставщики email-рассылок, мессенджеров, систем обращений и иных каналов связи; профессиональные консультанты; а также государственные органы и иные лица, которым данные должны быть раскрыты по закону.

11.2. Объём обработки третьими лицами

11.2.1. Такие лица получают только те данные, которые необходимы для выполнения соответствующей функции. В зависимости от категории поставщика это могут быть данные аккаунта, данные биллинга, метаданные соединения, данные поддержки, идентификаторы, связанные с Telegram, аналитические сигналы, статус KYC, риск-сигналы и иная сервисная информация.

11.2.2. Отдельные технические поставщики, обеспечивающие работу определённых компонентов Сервиса, могут видеть ограниченные данные аккаунта, биллинга, использования и журналирования, необходимые для функционирования соответствующих технических решений.

11.3. Международные передачи данных

11.3.1. Поскольку Сервис может использовать поставщиков и инструменты, расположенные в различных странах, данные могут обрабатываться и передаваться за пределы страны Пользователя или страны, из которой осуществляется доступ к Сервису.

11.3.2. Уровень защиты данных в таких юрисдикциях может отличаться от уровня защиты в стране Пользователя. В применимых случаях Провайдер стремится использовать разумные договорные, технические и организационные меры, а также иные допустимые законом механизмы для защиты данных при трансграничной передаче.

11.4. Ограничения на использование данных третьими лицами

11.4.1. Провайдер стремится привлекать контрагентов, которые обязуются использовать данные только для оказания соответствующих услуг Провайдеру либо в иных случаях, прямо допускаемых законом или их собственной ролью в обработке.

11.4.2. Конкретный состав таких поставщиков и сервисов может изменяться без предварительного уведомления Пользователя.

12. БЕЗОПАСНОСТЬ ДАННЫХ И АВТОМАТИЗИРОВАННЫЕ ПРОВЕРКИ

12.1. Технические и организационные меры

12.1.1. Провайдер принимает разумные технические и организационные меры для защиты данных от несанкционированного доступа, утраты, изменения, раскрытия или уничтожения с учётом характера данных, структуры Сервиса и уровня риска.

12.1.2. Такие меры могут включать шифрование при передаче, разграничение доступа, аутентификацию, журналирование административных действий, сегментацию инфраструктуры, резервирование, мониторинг событий безопасности, использование антифрод-инструментов и иные меры, соразмерные текущим потребностям Сервиса.

12.2. Ограничения и риски

12.2.1. Передача данных через интернет и использование распределённой технической инфраструктуры объективно сопряжены с определёнными рисками. Провайдер не гарантирует абсолютную безопасность среды передачи данных, но стремится принимать меры, соразмерные рискам.

12.3. Автоматизированные сигналы и оценка риска

12.3.1. Провайдер вправе использовать автоматизированные сигналы, поведенческие правила, обнаружение аномалий, риск-скоринг, фрод-флаги и иные средства технической оценки активности Пользователей в целях безопасности, противодействия злоупотреблениям, защиты инфраструктуры и управления доступом к отдельным функциям.

12.3.2. Такие механизмы могут повлечь временную заморозку аккаунта, ограничение отдельных функций, инициирование проверки, запрос KYC, задержку предоставления доступа к ограниченным доменам или направление запроса на дополнительное рассмотрение.

12.3.3. Если применимое право предоставляет Пользователю дополнительные гарантии в отношении решений, основанных исключительно на автоматизированной обработке, Провайдер стремится обеспечить надлежащие процедуры, включая возможность дополнительного рассмотрения с участием человека, если это требуется.

12.4. Инциденты безопасности

12.4.1. При выявлении инцидентов безопасности Провайдер вправе принимать необходимые меры, включая ограничение доступа, проведение внутренних проверок, взаимодействие с поставщиками и компетентными органами, а также иные меры, направленные на минимизацию последствий и предотвращение повторения.

13. ПРАВА ПОЛЬЗОВАТЕЛЯ

13.1. Общие положения

13.1.1. Пользователь обладает правами в отношении своих данных в объёме, предусмотренном применимым правом о защите данных.

13.2. Возможные права

13.2.1. В зависимости от применимого права Пользователь может обладать правом на информацию об обработке, доступ к данным, исправление, удаление, ограничение обработки, переносимость данных, возражение против обработки, отзыв согласия, подачу жалобы в надзорный орган, а также правом не подвергаться решению, основанному исключительно на автоматизированной обработке, если такое право предусмотрено законом.

13.3. Порядок подачи запросов

13.3.1. Для реализации указанных прав Пользователь вправе направить запрос на privacy@x2proxy.com или через иные официальные каналы связи, указанные в Сервисе. Провайдер вправе запросить дополнительную информацию, необходимую для идентификации Пользователя и предотвращения несанкционированного раскрытия данных.

13.4. Сроки рассмотрения запросов

13.4.1. Провайдер рассматривает запросы по вопросам конфиденциальности без необоснованной задержки и, как правило, стремится ответить в течение 30 календарных дней, если иной срок не установлен применимым правом.

13.4.2. Если запрос является сложным, объёмным, повторяющимся или требует дополнительной верификации, срок ответа может быть продлён в пределах, допускаемых применимым правом. При необходимости Пользователь уведомляется о таком продлении.

13.5. Ограничения на исполнение запросов

13.5.1. Провайдер вправе полностью или частично отказать в исполнении запроса либо ограничить объём предоставляемой информации, если это допускается законом, нарушает права третьих лиц, создаёт угрозу безопасности Сервиса, препятствует расследованию либо если соответствующие данные должны быть сохранены по юридическим, комплаенс-, биллинговым основаниям, основаниям предотвращения мошенничества или безопасности.

14. ИЗМЕНЕНИЯ ПОЛИТИКИ

14.1. Право на внесение изменений

14.1.1. Провайдер вправе обновлять настоящую Политику с учётом развития Сервиса, изменения его функциональности, внедрения новых технологий, а также изменений способов оплаты, коммуникаций, аналитики, законодательства и требований безопасности.

14.2. Вступление изменений в силу

14.2.1. Обновлённая версия вступает в силу с даты, указанной в такой версии, либо с момента публикации, если иное не предусмотрено применимым правом.

14.2.2. В отношении существенных изменений Провайдер вправе использовать уведомления в интерфейсе, по электронной почте, в официальных мессенджерах или через иные доступные каналы связи.

14.2.3. Если для определённой категории обработки или коммуникации требуется новое согласие, Провайдер запрашивает его отдельно и не рассматривает продолжение использования Сервиса как универсальную замену такого согласия, если это запрещено законом.

15. КОНТАКТЫ

15.1. Каналы связи

15.1.1. По вопросам конфиденциальности, обработки данных, реализации прав и иным вопросам конфиденциальности Пользователь вправе обращаться на privacy@x2proxy.com.

15.1.2. По общим вопросам использования Сервиса Пользователь вправе обращаться к Провайдеру через официальную электронную почту, форму поддержки, встроенную систему обращений, официальный Telegram или иные мессенджеры, указанные в интерфейсе Сервиса или на официальных ресурсах.

15.1.3. Провайдер вправе обновлять перечень доступных каналов связи по мере развития Сервиса.

15.2. Коммуникации с Пользователем

15.2.1. Провайдер вправе направлять Пользователю сервисные, технические, платёжные уведомления, уведомления по вопросам безопасности, KYC, ограниченных доменов, поддержки и иные обязательные сообщения по электронной почте, через личный кабинет, Telegram, мессенджеры и иные доступные каналы.

15.2.2. Маркетинговые и промо-коммуникации могут направляться в объёме и на основаниях, допускаемых законом. Пользователь вправе отказаться от маркетинговых сообщений, однако такой отказ не влияет на получение обязательных сервисных уведомлений.

15.3. Электронная форма взаимодействия

15.3.1. Пользователь соглашается с тем, что взаимодействие с Провайдером по вопросам, связанным с Сервисом и настоящей Политикой, может осуществляться в электронной форме.