

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

для сервиса VPN Port

Редакция от 5 августа 2026 года

Оператор сервиса: Frenz Company Limited

Настоящая Политика объясняет, какие персональные данные обрабатываются при использовании VPN Port, для каких целей они нужны, как защищаются, кому могут передаваться и какие права имеет Пользователь. Политика также разграничивает данные, необходимые для работы сервиса VPN Port, предоставляемого Frenz Company Limited (далее - «Компания»), и необязательные способы обработки.

1. Общие положения и сфера действия

1.1. Настоящая Политика обработки персональных данных и конфиденциальности (далее - «Политика») регулирует обработку данных сервисом VPN Port, предоставляемым Frenz Company Limited (далее - «Компания» или «Оператор»).

1.2. Политика применяется к Telegram-боту @vpn_portbot, сайту и базе знаний VPN Port, веб-интерфейсам, мини-приложениям, платежным страницам, каналам поддержки, программным интерфейсам и иным точкам доступа, находящимся под контролем Компании.

1.3. VPN Port предоставляет доступ к технологии виртуальной частной сети и связанным функциям, включая выдачу конфигураций или ключей доступа, выбор доступного сервера, управление подпиской, устройствами и настройками маршрутизации, если такие функции доступны в интерфейсе.

1.4. Политика распространяется на посетителей сайта, пользователей бота, плательщиков, получателей пробного доступа, участников реферальных программ и лиц, обращающихся в поддержку, далее совместно - «Пользователь».

1.5. Использование VPN Port подтверждает ознакомление Пользователя с Политикой. Когда применимое законодательство требует отдельного согласия, Компания запрашивает его явным способом. Отказ от необязательного согласия не ограничивает доступ к основной Услуге, если обработка не является технически или юридически необходимой.

1.6. Если Пользователь взаимодействует с Telegram, платежным сервисом, магазином приложений, сторонним VPN-клиентом или иным независимым сервисом, такой поставщик обрабатывает часть данных по собственным правилам. Настоящая Политика относится только к обработке, контролируемой Компанией.

2. Оператор и контакты

2.1. Оператором персональных данных является Frenz Company Limited, юридическое лицо, зарегистрированное в Таиланде под регистрационным номером 0835567027390.

2.2. Место государственной регистрации: 88/88, Mu 2, Rawai Sub-district, Mueang Phuket District, Phuket Province 83130, Thailand. Юридический адрес: 83130, Phuket Province, Mu 2, Rawai Sub-district, Mueang Phuket District.

2.3. Запросы о персональных данных направляются в Telegram-поддержку @vpnportsupport или через контакт, указанный в интерфейсе VPN Port, с темой «Privacy request / Запрос по персональным данным». Компания вправе запросить разумное подтверждение личности или владения учетной записью.

2.4. Для защиты данных Компания вправе запросить сведения, необходимые для подтверждения личности, владения учетной записью или связи с конкретной транзакцией. Не следует направлять в открытом чате полные реквизиты банковской карты, пароли или копии документов, если Компания прямо не запросила безопасный способ их передачи.

3. Термины

3.1. «Персональные данные» - информация, относящаяся к определенному или определяемому физическому лицу, включая электронные идентификаторы, контактные сведения, IP-адрес и данные об использовании сервиса, если они связаны с Пользователем.

3.2. «VPN» - технология создания защищенного сетевого соединения между устройством Пользователя и выбранной точкой выхода или иной сетевой инфраструктурой.

3.3. «Конфигурация» - ключ, ссылка, QR-код, файл, токен, параметры сервера или иной набор данных, необходимый для подключения к VPN Port через совместимый клиент.

3.4. «Интернет-трафик» - сетевые пакеты и содержимое соединений, которые устройство Пользователя передает через VPN-туннель.

3.5. «Технические данные соединения» - ограниченные служебные сведения, необходимые для установления, поддержания, защиты и диагностики VPN-соединения, без формирования истории посещенных ресурсов.

3.6. «Обработка» - любое действие с персональными данными, включая сбор, запись, хранение, использование, передачу, ограничение, обезличивание и удаление.

3.7. «Обработчик» - поставщик, который обрабатывает данные от имени Компании. Отдельные поставщики могут действовать как самостоятельные операторы в части платежей, собственной платформы или обязательных юридических функций.

4. Принципы и правовые основания

4.1. Компания обрабатывает данные законно, добросовестно и прозрачно; для определенных целей; в минимально необходимом объеме; с учетом точности, ограниченных сроков хранения и соответствующих мер безопасности.

4.2. Основным основанием обработки является необходимость заключить или исполнить договор с Пользователем: создать учетную запись, выдать Конфигурацию, активировать подписку, обеспечить подключение, учесть устройства и оказать поддержку.

4.3. Отдельные операции выполняются для соблюдения требований закона, налогового и бухгалтерского учета, ответа на законные требования органов власти, предотвращения мошенничества, защиты инфраструктуры, Пользователей и прав Компании.

4.4. Когда применимое право допускает обработку для законных интересов или защиты прав, Компания оценивает необходимость и соразмерность такой обработки и не использует это основание вопреки преобладающим правам Пользователя.

4.5. Согласие применяется для маркетинговых сообщений, необязательной аналитики или иных операций, для которых оно требуется законом. Согласие можно отозвать; отзыв не влияет на законность предшествующей обработки и не прекращает обработку на ином законном

основании.

4.6. Компания не продает персональные данные Пользователей и не формирует рекламные профили на основании истории сайтов, посещенных через VPN Port.

5. Какие данные обрабатываются

5.1. Данные Telegram и учетной записи: Telegram ID, username, отображаемое имя, язык, фотография профиля и иные сведения, переданные Telegram в соответствии с настройками Пользователя и техническими правилами платформ.

5.2. Контактные данные: адрес электронной почты, номер телефона или иной контакт, если Пользователь добровольно сообщил его для поддержки, восстановления доступа, получения документов или связи по спорной операции.

5.3. Данные подписки: выбранный тариф, срок, дата активации и окончания, статус, число разрешенных устройств, доступные регионы или серверы, история продлений, пробный период, бонусы и реферальные начисления, если соответствующие функции используются.

5.4. Платежные данные: сумма, валюта, дата, статус платежа, идентификатор транзакции, способ оплаты, сведения о возврате или споре. Полные реквизиты банковской карты, как правило, обрабатываются платежным провайдером и не поступают Компании.

5.5. Данные Конфигурации и управления доступом: уникальный идентификатор подписки или ключа, назначенный сервер, протокол, срок действия, число активных устройств, состояние Конфигурации, факты выдачи, перевыпуска, блокировки и отзыва.

5.6. Технические данные: IP-адрес, необходимый для установления соединения и защиты сервиса; дата и время технического события; выбранная точка выхода; версия клиента и операционной системы, если передается; тип устройства; код ошибки; показатели нагрузки; объем переданных данных, если он нужен для тарифа, ограничения злоупотреблений или диагностики.

5.7. Данные сайта и интерфейса: IP-адрес, браузер, устройство, язык, приблизительный регион, cookie, идентификаторы сессии, просмотренные страницы базы знаний, события интерфейса и сведения о переходах, если такая аналитика включена.

5.8. Данные поддержки: текст переписки, приложенные файлы и скриншоты, сведения об устройстве, диагностические данные, история действий поддержки и оценка качества обслуживания.

5.9. Данные о согласиях и юридических действиях: версия документов, дата и способ принятия, настройки уведомлений, запросы на удаление, обращения, претензии и доказательства исполнения обязательств.

6. Интернет-трафик и правило «без журналов активности»

6.1. Для работы VPN интернет-трафик технически проходит через сетевую инфраструктуру и выбранную точку выхода. Такая передача является частью оказания Услуги и не означает намеренного изучения содержимого соединений Компанией.

6.2. VPN Port не ведет постоянный журнал посещенных сайтов, поисковых запросов, содержимого сообщений, содержимого передаваемых файлов или DNS-запросов, привязанный к конкретному Пользователю.

6.3. Компания не использует содержимое интернет-трафика для рекламы, составления профиля интересов или продажи данных третьим лицам.

6.4. Отдельные сетевые сведения могут кратковременно обрабатываться в оперативной памяти или технических компонентах ровно в объеме, необходимом для маршрутизации, шифрования, предотвращения атак и поддержания соединения. Такая обработка не предназначена для создания истории интернет-активности.

6.5. Для безопасности и диагностики могут формироваться ограниченные технические журналы без содержимого трафика, например факты ошибки, перегрузки, превышения числа устройств, подозрительной автоматизации, атаки или нарушения правил использования.

6.6. Заявление об отсутствии журналов активности не означает абсолютную анонимность. Сайты, приложения, рекламные сети, операционная система, интернет-провайдер и сторонние клиенты могут использовать собственные cookie, идентификаторы, вход в аккаунт, цифровой отпечаток устройства или иные способы распознавания Пользователя.

6.7. Некоторые протоколы, приложения или сайты могут передавать данные вне VPN-туннеля из-за настроек устройства, split tunneling, системных ограничений, утечек DNS, IPv6, WebRTC или ошибок стороннего клиента. Пользователь отвечает за корректную настройку совместимого приложения и устройства.

6.8. Если Компания получает обязательное и юридически действительное требование компетентного органа, она предоставляет только те данные, которыми фактически располагает и которые обязана раскрыть по применимому закону. Компания не обязуется создавать отсутствующую историю интернет-активности.

7. Цели обработки

7.1. Создание и обслуживание учетной записи, связывание ее с Telegram или иным интерфейсом, проверка статуса и предоставление доступа к VPN Port.

7.2. Формирование, выдача, обновление, перевыпуск и отзыв Конфигураций, назначение серверов, управление устройствами, сроком подписки и доступными функциями.

7.3. Маршрутизация сетевого трафика и техническое обеспечение VPN-соединения, включая балансировку нагрузки, устойчивость, диагностику и восстановление работы.

7.4. Обработка платежей, учет покупок и возвратов, предотвращение двойных начислений, мошенничества и злоупотребления платежными средствами.

7.5. Предоставление поддержки, разбор ошибок подключения, восстановление доступа, обработка претензий и связь по вопросам сервиса.

7.6. Защита учетных записей, серверов и сетей, выявление атак, спама, сканирования, перегрузки, перепродажи доступа и иных нарушений Пользовательского соглашения.

7.7. Соблюдение юридических обязанностей, бухгалтерский и налоговый учет, защита прав в суде или ином разбирательстве, исполнение законных требований органов власти.

7.8. Анализ надежности и качества сервиса на агрегированном или обезличенном уровне, планирование емкости, оценка работы интерфейсов и исправление ошибок.

7.9. Направление сервисных уведомлений о подписке, платежах, изменениях Конфигурации, безопасности, технических работах и существенных изменениях документов.

7.10. Направление рекламных и информационных сообщений только при наличии требуемого согласия или иного законного основания и с возможностью отказаться от таких сообщений.

8. Источники данных

8.1. Компания получает данные непосредственно от Пользователя при запуске бота, оплате, настройке, обращении в поддержку, заполнении формы или ином взаимодействии.

8.2. Часть данных передается Telegram, платежными системами, магазинами приложений, партнерами реферальной программы или другими платформами в соответствии с их правилами и выбором Пользователя.

8.3. Технические данные формируются автоматически серверами, приложениями, средствами мониторинга, защиты и аналитики при использовании VPN Port.

8.4. Компания может получать сведения из общедоступных источников или от поставщиков противодействия мошенничеству, если это необходимо для проверки спорной операции, безопасности или исполнения закона.

8.5. Компания не просит Пользователя раскрывать содержание интернет-активности. Для диагностики Пользователь может добровольно предоставить скриншоты, журналы стороннего клиента или адрес проблемного ресурса; такие материалы обрабатываются только для поддержки и связанных юридических целей.

9. Cookie, аналитика и уведомления

9.1. Сайт и веб-интерфейсы могут использовать строго необходимые cookie для сессии, безопасности, языка и сохранения настроек.

9.2. Необязательные аналитические cookie используются в соответствии с применимыми требованиями и, когда требуется, после выбора Пользователя в интерфейсе согласия.

9.3. Cookie сайта не используются Компанией для просмотра или записи содержимого трафика, проходящего через VPN-туннель.

9.4. Пользователь может ограничить cookie в настройках браузера, однако это способно нарушить работу отдельных функций сайта или платежного интерфейса.

9.5. Сервисные сообщения необходимы для исполнения договора и могут включать уведомления о платеже, окончании срока, безопасности, изменении сервера, работах или документах.

9.6. От рекламных сообщений можно отказаться через предусмотренную кнопку, команду бота, настройки или обращение в поддержку. Отказ не влияет на получение необходимых сервисных сообщений.

10. Кому передаются данные

10.1. Telegram и иные платформы доступа получают данные в соответствии с технической архитектурой их сервисов и собственными правилами.

10.2. Платежные провайдеры, банки и магазины приложений обрабатывают данные, необходимые для приема платежа, проверки, возврата, борьбы с мошенничеством и выполнения собственных обязанностей.

10.3. Поставщики серверов, дата-центров, облачной инфраструктуры, сетей доставки, DNS, защиты от атак, мониторинга и резервного копирования могут получать ограниченный доступ, необходимый для работы и безопасности VPN Port.

10.4. Поставщики поддержки, коммуникаций и аналитики получают только данные, необходимые для соответствующей функции, и обязуются соблюдать применимые требования конфиденциальности и безопасности.

10.5. Профессиональные консультанты, аудиторы, бухгалтеры, страховщики и юристы могут получать данные, когда это необходимо для законной деятельности и защиты прав Компании.

10.6. Компетентные органы получают данные при наличии законного требования, обязательного предписания, судебного акта или иной правовой обязанности. Компания вправе оспаривать чрезмерные или неправомерные требования, когда это допустимо.

10.7. При реорганизации, продаже бизнеса, актива или привлечении инвестиций данные могут передаваться потенциальному или фактическому правопреемнику при соблюдении конфиденциальности и сохранении обязательных прав Пользователя.

10.8. Компания не раскрывает данные другим лицам для их самостоятельного маркетинга без отдельного законного основания или согласия Пользователя.

11. Трансграничная обработка

11.1. Компания зарегистрирована в Таиланде и может использовать поставщиков и серверы в разных странах. Поэтому данные могут обрабатываться за пределами страны Пользователя и Таиланда.

11.2. Выбор Пользователем конкретной точки выхода означает, что сетевой трафик технически проходит через инфраструктуру в соответствующей или связанной юрисдикции.

11.3. При трансграничной передаче Компания применяет предусмотренные законом механизмы и оценивает характер данных, цели, договорные гарантии, меры безопасности и применимое право страны получателя.

11.4. Законы страны размещения сервера или поставщика могут отличаться и предоставлять государственным органам полномочия доступа к данным. Пользователь должен учитывать это при выборе региона подключения.

11.5. Если передача требует отдельного согласия, разрешения или дополнительных гарантий, Компания применяет соответствующий механизм до начала такой обработки, если иное не допускается законом.

12. Сроки хранения и удаление

12.1. Данные учетной записи, настройки и история подписки хранятся, пока учетная запись или договорные отношения активны, а после прекращения - обычно до 90 дней для завершения операций, предотвращения мошенничества и восстановления по обоснованному запросу.

12.2. Активные Конфигурации хранятся в течение срока подписки. После окончания или отзыва служебная связь с учетной записью удаляется или обезличивается, как правило, в течение 30 дней, если более длительный срок не требуется для безопасности или спора.

12.3. Ограниченные технические журналы ошибок и безопасности без содержания трафика обычно хранятся не более 30 дней. Записи, связанные с атакой, мошенничеством, спором или нарушением, могут храниться до завершения расследования и применимого срока защиты прав.

12.4. Компания не хранит постоянную историю посещенных сайтов и содержимого интернет-трафика Пользователя.

12.5. Платежные, налоговые и бухгалтерские записи хранятся в течение срока, установленного применимым законодательством и требованиями платежных провайдеров.

12.6. Переписка поддержки обычно хранится до 3 лет после закрытия обращения, если более длительный срок не нужен для спора, безопасности или выполнения закона.

12.7. Cookie и необязательные аналитические идентификаторы хранятся в течение срока, указанного в соответствующем интерфейсе, и обычно не дольше 13 месяцев, если закон или техническая необходимость не требуют иного.

12.8. Резервные копии могут сохранять удаленные данные до 90 дней и удаляются по циклу перезаписи, если не введена законная блокировка удаления.

12.9. Агрегированные и необратимо обезличенные сведения могут храниться без ограничения срока, поскольку они больше не относятся к определяемому лицу.

13. Безопасность и инциденты

13.1. Компания применяет технические и организационные меры, соответствующие характеру данных и рискам: разграничение доступа, шифрование при передаче, управление секретами, резервное копирование, мониторинг, обновления, журналирование действий администраторов и договорные требования к поставщикам.

13.2. Доступ к данным предоставляется сотрудникам и подрядчикам по принципу необходимости и в пределах их функций.

13.3. Компания стремится разделять идентификаторы учетной записи, платежные сведения и техническую сетевую информацию и не объединять их в историю интернет-активности.

13.4. При инциденте Компания оценивает риск, принимает меры по локализации и восстановлению, документирует событие и уведомляет компетентный орган и затронутых лиц в случаях и сроки, предусмотренные законом.

13.5. Ни одна система не обеспечивает абсолютную безопасность. Пользователь обязан защищать Telegram-аккаунт, устройство, Конфигурацию и коды доступа, устанавливать обновления и не передавать ключ третьим лицам вне условий тарифа.

13.6. О подозрении на утечку Конфигурации, несанкционированный платеж или доступ необходимо без промедления сообщить в поддержку и, при необходимости, отозвать активные сеансы или перевыпустить ключ.

14. Права Пользователя

14.1. В зависимости от применимого законодательства Пользователь вправе запросить информацию об обработке и доступ к своим персональным данным.

14.2. Пользователь вправе потребовать исправления неточных данных, дополнения неполных сведений и обновления устаревшей информации.

14.3. Пользователь вправе потребовать удаление данных, если отсутствует законное основание для дальнейшего хранения, а также ограничение или прекращение отдельных операций в предусмотренных законом случаях.

14.4. Пользователь вправе отозвать согласие, возразить против обработки, основанной на соответствующем законном интересе, и отказаться от прямого маркетинга.

14.5. Если применимо, Пользователь вправе получить предоставленные им данные в структурированном машиночитаемом формате и запросить их передачу другому оператору, когда это технически осуществимо.

14.6. Пользователь вправе запросить разъяснение и пересмотр решения, принятого исключительно автоматизированным способом и создающего существенные юридические последствия, если такая обработка применяется.

14.7. Пользователь вправе подать жалобу в компетентный орган по защите данных или обратиться в суд в соответствии с применимым законодательством.

14.8. Права могут быть ограничены, если данные необходимы для исполнения договора, безопасности, налогового учета, расследования злоупотребления, защиты прав или выполнения обязательного требования закона.

14.9. Компания отвечает на подтвержденный запрос в срок, установленный применимым законом. Явно необоснованные или чрезмерно повторяющиеся запросы могут обрабатываться с учетом допускаемых законом ограничений.

15. Автоматизированная обработка

15.1. VPN Port автоматически выдает Конфигурации, назначает серверы, учитывает срок и число устройств, применяет лимиты и обрабатывает платежные статусы.

15.2. Автоматические средства могут выявлять необычную нагрузку, множество одновременных подключений, атаки, спам, перепродажу доступа и иные признаки нарушения.

15.3. Такие средства предназначены для работы и безопасности сервиса и не используются для оценки личности Пользователя по содержимому его интернет-активности.

15.4. Пользователь может обратиться в поддержку для проверки блокировки или иного существенного ограничения, если считает его ошибочным, за исключением случаев, когда раскрытие деталей создаст риск обхода мер безопасности.

16. Дети и несовершеннолетние

16.1. VPN Port предназначен для совершеннолетних и полностью дееспособных пользователей. Компания сознательно не предлагает платные услуги детям без участия законного представителя.

16.2. Лицо, не достигшее возраста самостоятельного согласия или заключения договора по применимому праву, не должно использовать VPN Port без разрешения и контроля законного представителя.

16.3. Если Компания узнает, что данные ребенка собраны без требуемого основания, она принимает разумные меры для прекращения обработки и удаления данных, если их хранение не требуется законом или безопасностью.

16.4. Родитель или законный представитель может направить запрос через контакты раздела 18 и должен подтвердить полномочия в объеме, необходимом для защиты ребенка и учетной записи.

17. Обязанности Пользователя

17.1. Пользователь обязан сообщать достоверные данные, не передавать чужие персональные данные без законного основания и не выдавать себя за другое лицо.

17.2. Пользователь обязан хранить Конфигурацию конфиденциально и не публиковать ключ, QR-код, ссылку или файл доступа в открытых источниках.

17.3. Для диагностики Пользователь должен по возможности скрывать на скриншотах пароли, платежные реквизиты, личную переписку и иную информацию, не относящуюся к проблеме.

17.4. Пользователь обязан соблюдать применимое законодательство при использовании VPN и не использовать сервис для противоправной обработки данных, скрытого наблюдения, атак или иных нарушений прав третьих лиц.

17.5. Если Пользователь предоставляет данные от имени организации, он подтверждает наличие полномочий и обязан информировать соответствующих лиц об обработке, когда это требуется законом.

18. Изменения, нормативная основа и контакты

18.1. Компания вправе обновлять Политику при изменении сервиса, поставщиков, технологий, рисков или законодательства. Новая редакция публикуется в VPN Port, на сайте или по иному доступному адресу.

18.2. Существенные изменения могут дополнительно сообщаться через Telegram, электронную почту или интерфейс до их вступления в силу, если это требуется законом или разумно с учетом характера изменения.

18.3. Политика применяется с учетом законодательства Таиланда, включая Закон о защите персональных данных В.Е. 2562 (2019), а также иных обязательных норм, применимых к конкретному Пользователю или операции.

18.4. Вопросы электронных транзакций, потребительских отношений и кибербезопасности регулируются, когда применимо, Законом об электронных транзакциях В.Е. 2544 (2001), Законом о защите прав потребителей В.Е. 2522 (1979), Законом о преступлениях, связанных с компьютерами, В.Е. 2550 (2007), применимыми нормами о защите детей и иными обязательными нормами законодательства Таиланда.

18.5. Если отдельное положение Политики противоречит обязательной норме закона, применяется такая норма, а остальные положения сохраняют силу.

18.6. Для реализации прав, жалобы или сообщения об инциденте используются реквизиты ниже.

Юридическое наименование	Frenz Company Limited
Регистрационный номер	0835567027390
Место государственной регистрации	88/88, Mu 2, Rawai Sub-district, Mueang Phuket District, Phuket Province 83130, Thailand
Юридический адрес	83130, Phuket Province, Mu 2, Rawai Sub-district, Mueang Phuket District
Сервис	VPN Port; Telegram-бот: @vpn_portbot
Контакты	Telegram-поддержка: @vpnportsupport или контакт, указанный в интерфейсе VPN Port
Тема обращения	Privacy request / Запрос по персональным данным

Приложение. Краткое уведомление для интерфейса

VPN Port обрабатывает данные Telegram-аккаунта, подписки, платежного статуса, Конфигурации, устройств, ограниченные технические события и обращения в поддержку для предоставления и защиты сервиса. VPN Port не ведет постоянный журнал посещенных сайтов или содержимого интернет-трафика, привязанный к Пользователю. Полные правила, сроки хранения, получатели данных и права Пользователя изложены в настоящей Политике.