

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

цифровой платформы QOR

Редакция №1.0

Дата публикации: «__» _____ 2026 года

Территория действия: Республика Казахстан

1. Общие положения

1.1. Настоящая Политика конфиденциальности определяет порядок сбора, обработки, хранения, использования, передачи, защиты и удаления персональных данных Пользователей цифровой платформы QOR.

1.2. Оператором платформы QOR является ТОО «QOR.KZ», БИН 260440024350, далее — «Оператор».

1.3. Настоящая Политика применяется к:

мобильному приложению QOR;
сайту QOR;
личному кабинету Пользователя;
тревожной кнопке;
сервисам уведомлений;
службе поддержки;
партнёрским сервисам;
корпоративным подключениям;
подключённым устройствам;
API-интеграциям;
иным цифровым инструментам QOR.

1.4. Использование платформы QOR означает согласие Пользователя с настоящей Политикой, если такое согласие выражено через регистрацию, акцепт документов, оплату подписки, использование приложения, нажатие тревожной кнопки или иное действие, предусмотренное документами QOR.

1.5. Если Пользователь не согласен с настоящей Политикой, он обязан прекратить использование платформы QOR.

1.6. Настоящая Политика является частью комплекта документов QOR и применяется совместно с Публичной офертой, Пользовательским соглашением, Согласием на сбор и обработку персональных данных, Согласием на обработку геолокации, Правилами использования тревожной кнопки и иными документами Оператора.

2. Термины и определения

2.1. Персональные данные — сведения, относящиеся к определённомu или определяемому Пользователю, зафиксированные на электронном, бумажном или ином материальном носителе.

2.2. Обработка персональных данных — любое действие или совокупность действий с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, изменение, дополнение, использование, передачу, распространение, обезличивание, блокирование и уничтожение.

2.3. Пользователь — физическое лицо, использующее платформу QOR.

2.4. Оператор — ТОО «QOR.KZ», осуществляющее сбор, обработку, хранение и защиту персональных данных в рамках работы платформы QOR.

2.5. Партнёр — юридическое лицо, индивидуальный предприниматель, специалист или организация, подключённые к платформе QOR для оказания отдельных услуг Пользователям.

2.6. Охранное агентство — партнёрская организация, оказывающая охранные услуги самостоятельно в пределах своего договора, лицензии, зоны покрытия и регламентов.

2.7. Тревожное обращение — обращение, сигнал, заявка или действие Пользователя, направленное через QOR и указывающее на необходимость оперативной помощи, поддержки, реагирования или связи.

2.8. Геолокация — данные о местоположении Пользователя, полученные через устройство, операционную систему, GPS, мобильную сеть, интернет, Wi-Fi, Bluetooth, подключённое устройство или иной технический канал.

2.9. Доверенное лицо — лицо, контактные данные которого Пользователь добавил в платформу QOR для уведомлений, связи или экстренного информирования.

2.10. Корпоративный клиент — юридическое лицо или индивидуальный предприниматель, подключающий к QOR сотрудников, клиентов, жителей, арендаторов, посетителей, объекты или иные группы пользователей.

3. Принципы обработки персональных данных

3.1. Оператор обрабатывает персональные данные в целях работы платформы QOR, исполнения договоров, обработки тревожных обращений, предоставления доступа к сервисам, обеспечения безопасности, технической поддержки и выполнения требований законодательства Республики Казахстан.

3.2. Оператор обрабатывает персональные данные только в объёме, необходимом для конкретных целей обработки.

3.3. Оператор принимает организационные и технические меры для защиты персональных данных от несанкционированного доступа, утраты, изменения, распространения, блокирования, уничтожения и иных неправомерных действий.

3.4. Оператор ограничивает доступ к персональным данным по ролям и служебной необходимости.

3.5. Оператор не продаёт персональные данные Пользователей третьим лицам.

3.6. Передача персональных данных партнёрам допускается только для целей работы платформы QOR, обработки тревожного обращения, оказания услуги, технической поддержки, оплаты, корпоративного подключения, исполнения договора или выполнения требований законодательства.

4. Категории собираемых данных

4.1. Оператор может собирать и обрабатывать следующие данные Пользователя:

ФИО;
номер телефона;
адрес электронной почты;
дату рождения, если она требуется для конкретного сервиса;
адрес проживания;
адрес объекта;
адрес работы или места нахождения объекта, если он указан Пользователем;
данные доверенных лиц;
историю тревожных обращений;
типы тревожных обращений;
геолокационные данные;
данные устройства;
IP-адрес;
данные операционной системы;
данные браузера;
идентификаторы устройства;
push-токены;
язык интерфейса;
настройки приложения;
историю входов;
историю действий в личном кабинете;
историю статусов обращений;
переписку со службой поддержки;
записи звонков, если такая функция подключена и Пользователь уведомлён;
фотографии, комментарии, вложения и иные материалы, загруженные Пользователем;
данные об оплатах в объёме, доступном Оператору;
технические логи;
иную информацию, которую Пользователь добровольно предоставляет через платформу QOR.

4.2. При корпоративном подключении Оператор может обрабатывать:

название организации;
подразделение Пользователя;
роль Пользователя в корпоративном подключении;
статус подключения;
служебный номер телефона;
служебный email;
привязку к объекту;
привязку к группе пользователей;
историю обращений по корпоративному подключению;
информацию, необходимую корпоративному администратору для управления доступом.

4.3. При подключении объектов Оператор может обрабатывать:

адрес объекта;
тип объекта;
схему объекта, если она предоставлена;
контакты ответственных лиц;
точки доступа;
посты охраны;
режим работы объекта;
историю тревожных событий по объекту;
данные, необходимые для взаимодействия с охранным агентством или корпоративной службой безопасности.

5. Геолокационные данные

5.1. QOR может использовать геолокацию Пользователя для работы тревожной кнопки и связанных функций.

5.2. Геолокация может использоваться:

для определения местоположения Пользователя при тревожном обращении;
для передачи координат оператору, диспетчеру, охранным агентству или иному партнёру;
для выбора доступного партнёра;
для фиксации истории тревожного обращения;
для отображения статуса реагирования;
для повышения точности обработки обращения;
для проверки нахождения Пользователя в зоне покрытия.

5.3. Геолокация может передаваться партнёру только в объёме, необходимом для обработки обращения или оказания услуги.

5.4. Точность геолокации зависит от устройства Пользователя, операционной системы, качества связи, GPS-сигнала, интернета, настроек энергосбережения, разрешений приложения и иных технических факторов.

5.5. При отключении геолокации отдельные функции QOR могут работать некорректно или стать недоступными.

6. Данные доверенных лиц

6.1. Пользователь может добавить в QOR доверенных лиц для уведомлений, связи и экстренного информирования.

6.2. Пользователь обязан получить согласие доверенного лица на указание его данных в QOR.

6.3. Оператор может обрабатывать следующие данные доверенного лица:

ФИО или имя контакта;
номер телефона;
email, если он указан;
статус связи с Пользователем;
настройки уведомлений;
историю направленных уведомлений.

6.4. Данные доверенных лиц используются только для целей, связанных с уведомлением, связью, обработкой тревожного обращения и обеспечением функций QOR.

6.5. Пользователь вправе удалить доверенное лицо из аккаунта.

7. Данные несовершеннолетних

7.1. Использование QOR несовершеннолетними допускается в порядке, предусмотренном законодательством Республики Казахстан и документами QOR.

7.2. Если аккаунт создаётся для несовершеннолетнего, Оператор вправе запросить согласие законного представителя.

7.3. Законный представитель несёт ответственность за достоверность данных несовершеннолетнего, настройку аккаунта, указание доверенных лиц и использование функций платформы.

7.4. Оператор вправе ограничить отдельные функции для несовершеннолетнего Пользователя, если это требуется для безопасности, соблюдения закона или корректной работы сервиса.

8. Цели обработки персональных данных

8.1. Оператор обрабатывает персональные данные для следующих целей:

регистрация Пользователя;
создание аккаунта;
идентификация Пользователя;
предоставление доступа к платформе QOR;
подключение подписки;
обработка оплаты;
управление тарифами;
работа тревожной кнопки;
обработка тревожных обращений;
передача тревожного обращения партнёрам;
связь с Пользователем;
уведомление доверенных лиц;
отображение статусов обращений;
ведение истории обращений;
техническая поддержка;
рассмотрение жалоб и претензий;
защита прав Оператора, Пользователя, партнёров и третьих лиц;
предотвращение мошенничества;
расследование нарушений;
обеспечение информационной безопасности;
улучшение качества сервиса;
аналитика работы платформы;
подготовка обезличенной статистики;
корпоративное администрирование;
исполнение договоров с Пользователями, партнёрами и корпоративными клиентами;
выполнение требований законодательства и компетентных органов.

8.2. Оператор может использовать обезличенные данные для аналитики, улучшения продукта, оценки качества работы партнёров, расчёта нагрузки, развития зон покрытия и подготовки управленческой отчётности.

8.3. Обезличенные данные не должны позволять прямо определить конкретного Пользователя без использования дополнительной информации.

9. Основания обработки персональных данных

9.1. Персональные данные обрабатываются на основании:

согласия Пользователя;
Публичной оферты;
Пользовательского соглашения;
заключённого договора;
корпоративного подключения;
необходимости обработки тревожного обращения;
необходимости защиты прав и законных интересов Оператора, Пользователя, партнёров и третьих лиц;

требований законодательства Республики Казахстан;
запросов компетентных органов в случаях, предусмотренных законом.

9.2. Пользователь вправе отказаться от предоставления отдельных данных, если такие данные не являются обязательными для конкретной функции.

9.3. Если данные необходимы для работы определённой функции, отказ от их предоставления может привести к невозможности использования такой функции.

10. Передача данных партнёрам

10.1. Оператор может передавать персональные данные партнёрам в объёме, необходимом для работы QOR и оказания услуг.

10.2. Получателями данных могут быть:

охранные агентства;
операторы и диспетчеры;
корпоративные клиенты;
корпоративные администраторы;
юридические партнёры;
психологические партнёры;
страховые партнёры;
платёжные провайдеры;
банки;
операторы связи;
поставщики SMS, push и email-уведомлений;
хостинг-провайдеры;
поставщики облачной инфраструктуры;
разработчики и технические подрядчики;
службы поддержки;
аналитические и антифрод-сервисы;
иные лица, участвующие в работе платформы QOR.

10.3. При тревожном обращении Оператор вправе передать партнёру данные, необходимые для обработки события:

ФИО Пользователя;
номер телефона;
адрес объекта;
текущую геолокацию;
тип тревоги;
комментарий Пользователя;
данные доверенных лиц;
статусы обращения;
технические данные, необходимые для обработки события.

10.4. Партнёры обязаны использовать данные только для целей, в связи с которыми такие данные были переданы.

10.5. Партнёры, получающие доступ к персональным данным, должны соблюдать требования конфиденциальности, информационной безопасности и применимого законодательства.

11. Передача данных корпоративному клиенту

11.1. Если Пользователь подключён к QOR через корпоративного клиента, Оператор может передавать корпоративному клиенту ограниченный объём данных, необходимый для администрирования подключения.

11.2. Корпоративному клиенту могут быть доступны:

ФИО Пользователя;
номер телефона;
статус подключения;
статус подписки в рамках корпоративного тарифа;
привязка к объекту или группе;
факт создания тревожного обращения;
статус обработки обращения;
отчёт по обращению в пределах корпоративного договора и согласия Пользователя.

11.3. Состав данных, доступных корпоративному клиенту, определяется договором между Оператором и корпоративным клиентом, настройками платформы, согласием Пользователя и требованиями законодательства.

11.4. Корпоративный клиент не вправе использовать данные Пользователя вне целей подключения к QOR, обеспечения безопасности, администрирования сервиса и исполнения договора.

12. Передача данных государственным органам

12.1. Оператор может передавать персональные данные государственным органам, судам, правоохранительным органам и иным компетентным органам в случаях, предусмотренных законодательством Республики Казахстан.

12.2. Передача данных осуществляется в объёме, необходимом для исполнения законного запроса, судебного акта, требования уполномоченного органа или защиты прав и законных интересов Оператора, Пользователя, партнёров и третьих лиц.

13. Международная передача данных

13.1. При использовании отдельных технических сервисов, облачной инфраструктуры, аналитических инструментов, сервисов уведомлений или подрядчиков персональные данные могут передаваться за пределы Республики Казахстан, если такая передача необходима для работы платформы QOR.

13.2. Оператор принимает меры для того, чтобы международная передача данных осуществлялась с учётом требований законодательства Республики Казахстан, договорных обязательств и мер защиты данных.

13.3. Пользователь соглашается, что отдельные технические элементы платформы могут работать с использованием инфраструктуры и сервисов, расположенных в разных юрисдикциях, если это требуется для стабильной работы QOR.

14. Хранение персональных данных

14.1. Персональные данные хранятся в течение срока, необходимого для достижения целей обработки, исполнения договоров, работы платформы, рассмотрения обращений, защиты прав Оператора и выполнения требований законодательства.

14.2. Сроки хранения могут отличаться в зависимости от категории данных:

данные аккаунта — в течение срока использования аккаунта;
данные подписки и оплат — в течение срока, необходимого для бухгалтерского, налогового и юридического учёта;
история тревожных обращений — в течение срока, установленного внутренними регламентами Оператора, договорами и требованиями законодательства;
технические логи — в течение срока, необходимого для безопасности, диагностики и расследования инцидентов;
данные поддержки — в течение срока, необходимого для рассмотрения обращений и защиты прав сторон;
обезличенная аналитика — без ограничения срока, если она не позволяет определить Пользователя.

14.3. После достижения целей обработки данные удаляются, обезличиваются или архивируются, если дальнейшее хранение не требуется по закону, договору, спору, расследованию инцидента или защите прав Оператора.

15. Защита персональных данных

15.1. Оператор принимает технические, организационные и правовые меры для защиты персональных данных.

15.2. К таким мерам могут относиться:

разграничение прав доступа;
использование ролей и уровней доступа;
парольная защита;
двухфакторная аутентификация для административных доступов, если она подключена;
логирование действий;
ограничение доступа сотрудников и подрядчиков;
договоры о конфиденциальности;

шифрование каналов передачи данных;
резервное копирование;
контроль технических уязвимостей;
внутренние регламенты обработки данных;
проверка действий администраторов;
ограничение доступа по служебной необходимости.

15.3. Оператор не может гарантировать абсолютную защиту от всех возможных рисков, включая кибератаки, сбои внешней инфраструктуры, действия третьих лиц и ошибки Пользователя.

15.4. Пользователь обязан самостоятельно принимать меры защиты своего устройства, номера телефона, пароля, email, SIM-карты и иных средств доступа.

16. Доступ сотрудников и подрядчиков

16.1. Доступ к персональным данным предоставляется только тем сотрудникам, операторам, диспетчерам, подрядчикам и партнёрам, которым такой доступ необходим для выполнения служебных или договорных обязанностей.

16.2. Доступ может предоставляться для:

обработки тревожных обращений;
технической поддержки;
работы с оплатами;
рассмотрения претензий;
администрирования аккаунтов;
обеспечения безопасности;
разработки и сопровождения платформы;
аудита качества;
исполнения договоров.

16.3. Лица, получающие доступ к персональным данным, обязаны соблюдать конфиденциальность и использовать данные только в разрешённых целях.

17. Права Пользователя

17.1. Пользователь вправе:

получать информацию об обработке своих персональных данных;
запрашивать уточнение данных;
изменять данные аккаунта;
запрашивать удаление данных;
отозвать согласие на обработку персональных данных;
отказаться от маркетинговых уведомлений;
запросить ограничение обработки в случаях, предусмотренных законом;
обратиться с жалобой к Оператору;

обратиться в уполномоченный орган или суд в случаях, предусмотренных законодательством.

17.2. Для реализации своих прав Пользователь направляет обращение Оператору через приложение, сайт, email, службу поддержки или иной официальный канал.

17.3. Оператор вправе запросить подтверждение личности Пользователя перед предоставлением информации, изменением данных, удалением данных или выполнением иного запроса.

17.4. Оператор вправе отказать в удалении или ограничении обработки данных, если дальнейшее хранение требуется для исполнения закона, договора, бухгалтерского учёта, расследования инцидента, защиты прав Оператора, рассмотрения претензии или разрешения спора.

18. Отзыв согласия

18.1. Пользователь вправе отозвать согласие на обработку персональных данных.

18.2. Отзыв согласия направляется через официальный канал связи Оператора.

18.3. После получения отзыва Оператор прекращает обработку данных, если дальнейшая обработка не требуется по закону, договору, судебному спору, расследованию инцидента, бухгалтерскому учёту, защите прав Оператора или иным законным основаниям.

18.4. Пользователь понимает, что отзыв согласия может привести к:

- невозможности использования аккаунта;
- отключению тревожной кнопки;
- невозможности передачи обращения партнёрам;
- невозможности обработки геолокации;
- отключению уведомлений;
- прекращению подписки;
- ограничению доступа к истории обращений;
- невозможности оказания отдельных услуг.

19. Cookies и технические идентификаторы

19.1. Сайт QOR и отдельные веб-сервисы могут использовать cookies, пиксели, локальное хранилище, технические идентификаторы и аналогичные технологии.

19.2. Такие технологии могут использоваться для:

- авторизации;
- сохранения настроек;
- аналитики;
- безопасности;

защиты от мошенничества;
улучшения интерфейса;
работы личного кабинета;
измерения качества сервиса.

19.3. Пользователь может ограничить использование cookies в настройках браузера, если такая возможность предусмотрена браузером.

19.4. Ограничение cookies может повлиять на работу сайта, личного кабинета и отдельных функций платформы.

20. Аналитика и улучшение сервиса

20.1. Оператор может использовать технические и обезличенные данные для анализа работы платформы.

20.2. Аналитика может использоваться для:

улучшения интерфейса;
устранения ошибок;
измерения нагрузки;
оценки качества обработки обращений;
развития зон покрытия;
проверки эффективности партнёров;
оптимизации уведомлений;
повышения стабильности платформы;
подготовки внутренней отчётности.

20.3. При использовании аналитики Оператор стремится применять обезличивание, агрегирование и ограничение доступа к данным.

21. Маркетинговые коммуникации

21.1. Оператор может направлять Пользователю маркетинговые сообщения только при наличии согласия Пользователя или иного законного основания.

21.2. Маркетинговые сообщения могут содержать:

информацию о тарифах;
акции;
промокоды;
предложения партнёров;
новости QOR;
информацию о новых функциях;
опросы качества сервиса.

21.3. Пользователь вправе отказаться от маркетинговых сообщений через настройки приложения, ссылку отказа, службу поддержки или иной доступный канал.

21.4. Отказ от маркетинговых сообщений не отменяет сервисные уведомления, связанные с безопасностью, тревожными обращениями, оплатой, подпиской, изменением документов и работой аккаунта.

22. Инциденты безопасности

22.1. При выявлении инцидента, связанного с персональными данными, Оператор принимает меры по ограничению последствий, расследованию причин и восстановлению защищённости данных.

22.2. К инцидентам безопасности могут относиться:

несанкционированный доступ;
утрата данных;
изменение данных;
утечка данных;
ошибка в правах доступа;
компрометация аккаунта;
кибератака;
технический сбой, затрагивающий безопасность данных.

22.3. Оператор вправе временно ограничить доступ к аккаунту, функции, партнёрскому сервису или административному интерфейсу при наличии риска для безопасности данных.

22.4. При необходимости Оператор уведомляет Пользователей, партнёров или компетентные органы в порядке, предусмотренном законодательством и внутренними регламентами.

23. Данные, предоставленные Пользователем о третьих лицах

23.1. Если Пользователь предоставляет Оператору данные третьих лиц, включая доверенные контакты, членов семьи, сотрудников, гостей, арендаторов или иных лиц, Пользователь подтверждает наличие законного основания для передачи таких данных.

23.2. Пользователь несёт ответственность за достоверность и законность передачи данных третьих лиц.

23.3. Оператор вправе удалить данные третьего лица по его обоснованному обращению, если дальнейшая обработка не требуется для исполнения закона, договора, безопасности или защиты прав сторон.

24. Данные, связанные с тревожными обращениями

24.1. История тревожных обращений может содержать сведения о времени, месте, типе обращения, статусах, операторах, партнёрах, комментариях, уведомлениях, действиях и результатах обработки события.

24.2. Такие данные могут храниться для:

подтверждения факта обращения;
разбора качества реагирования;
рассмотрения жалоб;
защиты прав Пользователя, Оператора и партнёров;
анализа ложных тревог;
расследования инцидентов;
исполнения договоров;
выполнения требований законодательства.

24.3. Доступ к истории тревожных обращений ограничивается ролями и служебной необходимостью.

24.4. Удаление истории тревожного обращения может быть ограничено, если данные необходимы для защиты прав сторон, расследования, отчётности или исполнения закона.

25. Данные подключённых устройств

25.1. QOR может работать с мобильными телефонами, смарт-часами, тревожными кнопками, датчиками, устройствами связи и иными техническими средствами.

25.2. При использовании подключённых устройств Оператор может обрабатывать:

идентификатор устройства;
тип устройства;
модель устройства;
статус подключения;
состояние батареи, если доступно;
статус сети;
время последней активности;
сигналы устройства;
технические ошибки;
события активации тревоги;
данные геолокации, если устройство их передаёт.

25.3. Пользователь отвечает за корректное использование устройства, его заряд, связь, настройки, физическую сохранность и своевременное обслуживание, если иное не предусмотрено отдельным договором.

26. Обновление Политики

26.1. Оператор вправе изменять настоящую Политику.

26.2. Новая редакция Политики вступает в силу с момента публикации на сайте, в приложении или ином официальном канале QOR, если иной срок не указан при публикации.

26.3. Продолжение использования QOR после публикации новой редакции означает согласие Пользователя с изменениями.

26.4. Если Пользователь не согласен с новой редакцией Политики, он обязан прекратить использование платформы QOR и вправе направить запрос на удаление аккаунта в установленном порядке.

27. Контакты по вопросам персональных данных

27.1. По вопросам обработки персональных данных Пользователь может обратиться к Оператору через официальный канал связи.

27.2. Обращение должно содержать:

ФИО Пользователя;
номер телефона, связанный с аккаунтом;
суть обращения;
документы или сведения, необходимые для идентификации, если они запрошены Оператором.

27.3. Оператор рассматривает обращения в сроки, установленные законодательством Республики Казахстан и внутренними регламентами Оператора.

28. Реквизиты Оператора

Оператор: ТОО «QOR.KZ»

БИН: 260440024350

Первый руководитель: Левин Игорь Александрович

Юридический адрес: M06F3A4, Карагандинская область, город Караганда, район имени Казыбек Би, пр. Бухар Жырау, ст-е 49/6

Телефон: +7 775 462 48 71

Email: _____

Сайт: _____

Банковские реквизиты: _____