

ПРИЛОЖЕНИЕ №3

Соглашение об обработке и защите персональных данных

к Договору № ____ о подключении охранного агентства к цифровой платформе QOR

г. _____

« ____ » _____ 2026 года

ТОО «QOR.KZ», БИН 260440024350, в лице первого руководителя Левина Игоря Александровича, действующего на основании Устава, далее — «Оператор», с одной стороны, и

_____, БИН/ИИН _____, в лице _____, действующего на основании _____, далее — «Охранное агентство», с другой стороны,

совместно именуемые «Стороны», утвердили настоящее Приложение №3 — Соглашение об обработке и защите персональных данных.

1. Общие положения

1.1. Настоящее Соглашение определяет порядок передачи, обработки, хранения, использования, защиты, ограничения доступа, удаления и возврата персональных данных, передаваемых Оператором Охранному агентству в рамках работы цифровой платформы QOR.

1.2. Настоящее Соглашение является неотъемлемой частью Договора № ____ о подключении охранного агентства к цифровой платформе QOR.

1.3. Настоящее Соглашение применяется ко всем персональным данным, сведениям об объектах, тревожным обращениям, геолокационным данным, контактными данным и иной информации, которую Охранное агентство получает через QOR, S-OMS, API, личный кабинет, уведомления, телефонный канал, электронную почту, мессенджеры или иные каналы взаимодействия с Оператором.

1.4. Оператор передаёт Охранному агентству персональные данные только в объёме, необходимом для обработки тревожных обращений, организации реагирования, связи с Пользователем, взаимодействия с объектом, отчётности, рассмотрения жалоб и исполнения Договора.

1.5. Охранное агентство обязуется использовать полученные персональные данные исключительно для целей настоящего Соглашения и Договора.

1.6. Охранному агентству запрещается использовать персональные данные Пользователей QOR для самостоятельных продаж, рекламы, переманивания

клиентов, создания собственной клиентской базы, передачи третьим лицам или иных целей, не связанных с обработкой конкретного тревожного обращения.

1.7. Стороны обязуются соблюдать требования законодательства Республики Казахстан о персональных данных, конфиденциальной информации, информационной безопасности и охранной деятельности.

2. Термины и определения

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

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

2.3. Пользователь — физическое лицо, использующее QOR, тревожную кнопку, мобильное приложение, подключённое устройство, корпоративное подключение или иной сервис QOR.

2.4. Оператор — ТОО «QOR.KZ», обеспечивающее работу цифровой платформы QOR и передающее Охранному агентству данные в рамках Договора.

2.5. Охранное агентство — партнёрская организация, подключённая к QOR и обрабатывающая персональные данные для обработки тревожных обращений и оказания охранных услуг.

2.6. QOR — цифровая платформа оперативной помощи и поддержки, включающая мобильное приложение, сайт, личные кабинеты, тревожную кнопку, S-OMS, уведомления, API-интеграции и иные цифровые инструменты.

2.7. S-OMS — операционный модуль управления охранными процессами, объектами, постами, сменами, персоналом, маршрутами, инцидентами, статусами и отчётами.

2.8. Тревожное обращение — сигнал, заявка, сообщение, нажатие тревожной кнопки, автоматическое событие или иное обращение, созданное через QOR.

2.9. Геолокационные данные — сведения о местоположении Пользователя, устройства, объекта или точки создания тревожного обращения.

2.10. Конфиденциальная информация — любые сведения, полученные Сторонами в рамках Договора и настоящего Соглашения, включая персональные данные, сведения об объектах, тревожные обращения, статусы, отчёты, технические данные, коммерческие условия и внутренние регламенты.

2.11. Инцидент безопасности — любое событие, связанное с утратой, разглашением, несанкционированным доступом, изменением, копированием, передачей, удалением, повреждением или иным неправомерным использованием персональных данных.

3. Роли Сторон при обработке персональных данных

3.1. Оператор организует работу платформы QOR, получает согласия Пользователей, определяет цели и порядок обработки персональных данных в рамках платформы и передаёт Охранному агентству данные для исполнения Договора.

3.2. Охранное агентство получает персональные данные от Оператора и обрабатывает их в целях обработки тревожных обращений, организации реагирования, связи с Пользователем, взаимодействия с объектом и исполнения Договора.

3.3. В части данных, полученных от Оператора через QOR, Охранное агентство обязуется действовать строго в пределах целей, определённых настоящим Соглашением, Договором, SLA и регламентами QOR.

3.4. Если Охранное агентство самостоятельно собирает дополнительные персональные данные у Пользователя вне QOR, такое Охранное агентство самостоятельно отвечает за законность такого сбора, наличие согласий, цели обработки, хранение и защиту таких данных.

3.5. Охранное агентство не вправе расширять цели обработки данных, полученных через QOR, без письменного согласия Оператора и законного основания.

4. Категории персональных данных

4.1. Оператор может передавать Охранному агентству следующие категории персональных данных Пользователя:

ФИО;
номер телефона;
адрес электронной почты, если он необходим для связи;
адрес проживания;
адрес объекта;
текущая геолокация;
последняя известная геолокация;
точность геолокации;
время получения координат;
тип тревожного обращения;
комментарий Пользователя;
источник тревожного обращения;
время создания обращения;
время принятия обращения;
статусы обращения;
история изменения статусов;
данные доверенных лиц;

информация об объекте;
подъезд, этаж, вход, ориентиры и иные данные доступа;
фото, видео, аудио, документы и иные вложения, переданные Пользователем;
корпоративная привязка;
данные устройства;
идентификатор устройства;
технические сведения, необходимые для обработки обращения;
иная информация, необходимая для исполнения Договора.

4.2. Оператор не передаёт Охранному агентству данные, не относящиеся к обработке тревожного обращения или исполнению Договора, если иное не предусмотрено отдельным соглашением, согласием Пользователя или законодательством.

4.3. Охранное агентство обязано немедленно уведомить Оператора, если получило избыточные данные, которые не требуются для обработки тревожного обращения.

5. Цели обработки персональных данных

5.1. Охранное агентство вправе обрабатывать персональные данные, полученные через QOR, только для следующих целей:

приём тревожного обращения;
проверка тревожного обращения;
связь с Пользователем;
связь с доверенными лицами, если это необходимо;
уточнение адреса, объекта или местоположения;
организация реагирования;
назначение ГБР;
выезд ГБР;
прибытие на объект или место обращения;
действия на месте в пределах охранной деятельности;
обновление статусов в QOR;
заккрытие тревожного обращения;
подготовка отчёта по обращению;
разбор ложной тревоги;
разбор спорного обращения;
рассмотрение жалобы;
взаимодействие с Оператором;
взаимодействие с корпоративным клиентом в пределах договора;
исполнение SLA;
исполнение Договора;
исполнение требований законодательства Республики Казахстан;
защита прав и законных интересов Оператора, Охранного агентства, Пользователя и третьих лиц.

5.2. Охранному агентству запрещается использовать персональные данные для следующих целей:

самостоятельная реклама;
продажа собственных услуг Пользователю без согласования с Оператором;
переманивание Пользователей QOR;
создание собственной базы клиентов на основании данных QOR;
передача третьим лицам;
публикация;
обучение сторонних систем без согласования;
аналитика вне целей Договора;
любые цели, не связанные с обработкой конкретного обращения и исполнением Договора.

6. Правовое основание передачи данных

6.1. Передача персональных данных Охранному агентству осуществляется на основании:

Публичной оферты QOR;
Пользовательского соглашения QOR;
Политики конфиденциальности QOR;
Согласия Пользователя на сбор и обработку персональных данных;
Согласия Пользователя на обработку геолокационных данных;
Согласия Пользователя на передачу тревожного обращения и данных партнёрам;
Договора между Оператором и Охранным агентством;
настоящего Соглашения;
иных документов QOR;
требований законодательства Республики Казахстан.

6.2. Оператор несёт ответственность за получение согласий Пользователей в зоне своей платформы.

6.3. Охранное агентство несёт ответственность за обработку данных после их получения и за действия своих сотрудников, представителей, подрядчиков и иных лиц, получивших доступ к данным через Охранное агентство.

7. Порядок передачи данных

7.1. Передача данных Охранному агентству осуществляется через защищённые и согласованные каналы QOR.

7.2. Каналами передачи могут быть:

личный кабинет QOR;
S-OMS;
мобильное приложение;
веб-интерфейс;
API;
push-уведомления;
SMS;

email;
телефонный канал;
мессенджер;
иные каналы, согласованные Сторонами.

7.3. Основным каналом обработки тревожных обращений является QOR/S-OMS, если иной канал не согласован Сторонами.

7.4. Передача данных через мессенджеры, email или телефон допускается только в случаях, когда это необходимо для обработки обращения, временной технической поддержки, резервного сценария или согласовано Сторонами.

7.5. Охранное агентство обязано обеспечить, чтобы данные, полученные через резервные каналы, не сохранялись вне необходимости и не передавались неуполномоченным лицам.

8. Доступ сотрудников Охранного агентства

8.1. Доступ к персональным данным Пользователей могут получать только сотрудники Охранного агентства, которым такие данные необходимы для исполнения служебных обязанностей.

8.2. Охранное агентство обязано назначить ответственного за доступы и обработку персональных данных.

8.3. Охранное агентство обязано вести перечень сотрудников, имеющих доступ к QOR, S-OMS, API, карточкам тревожных обращений и данным Пользователей.

8.4. Охранное агентство обязано обеспечить:

индивидуальные учётные записи сотрудников;
запрет передачи логинов и паролей;
своевременное удаление доступов уволенных сотрудников;
ограничение прав по роли;
доступ только по служебной необходимости;
контроль действий сотрудников;
инструктаж по персональным данным и конфиденциальности.

8.5. Охранное агентство несёт ответственность за все действия, совершённые через учётные записи своих сотрудников.

8.6. Если сотрудник Охранного агентства утратил полномочия, уволен, отстранён или больше не должен иметь доступ к QOR, Охранное агентство обязано немедленно заблокировать его доступ либо уведомить Оператора для блокировки доступа.

9. Обязанности Охранного агентства по защите данных

9.1. Охранное агентство обязуется принимать необходимые организационные, технические и правовые меры для защиты персональных данных.

9.2. Охранное агентство обязуется:

обрабатывать данные только в целях Договора;
ограничить доступ к данным;
не передавать данные третьим лицам без законного основания;
не публиковать данные;
не копировать данные вне необходимости;
не хранить данные в личных телефонах сотрудников без служебной необходимости;
не пересылать данные через личные аккаунты сотрудников;
не использовать данные для рекламы;
не использовать данные для самостоятельных продаж;
не создавать несанкционированные копии баз;
не выгружать данные массово без согласования с Оператором;
не подключать несанкционированные программы, боты, парсеры или автоматические инструменты;
не предоставлять доступ к QOR лицам, не уполномоченным Охранным агентством;
соблюдать парольную политику;
немедленно сообщать об инцидентах безопасности;
проводить инструктаж сотрудников;
соблюдать требования настоящего Соглашения.

9.3. Охранное агентство обязано обеспечить, чтобы все его сотрудники, имеющие доступ к данным QOR, были ознакомлены с требованиями конфиденциальности и персональных данных.

10. Запрещённые действия с персональными данными

10.1. Охранному агентству запрещается:

использовать данные Пользователей QOR вне целей Договора;
копировать базу Пользователей QOR;
выгружать данные из QOR без согласования;
передавать данные своим партнёрам, подрядчикам или третьим лицам без письменного согласия Оператора;
использовать данные для рассылок;
звонить Пользователям с рекламными предложениями вне конкретного тревожного обращения;
переманивать Пользователей на прямые договоры в обход QOR;
публиковать данные о тревожных обращениях;
размещать фото, видео, адреса, имена или обстоятельства обращений в социальных сетях;
использовать данные в обучающих материалах без обезличивания и согласования;
передавать данные сотрудникам, которым они не нужны для работы;
хранить данные в незащищённых файлах, личных мессенджерах, личных облаках или личных устройствах;

продавать, обменивать или иным образом коммерчески использовать данные; совершать иные действия, нарушающие законодательство, Договор или настоящее Соглашение.

10.2. Нарушение любого запрета настоящего раздела считается существенным нарушением Договора.

11. Хранение персональных данных Охранным агентством

11.1. Охранное агентство вправе хранить полученные персональные данные только в течение срока, необходимого для обработки тревожного обращения, отчётности, рассмотрения жалоб, исполнения Договора или выполнения требований законодательства.

11.2. Если данные доступны в QOR/S-OMS, Охранное агентство не должно создавать отдельные копии данных без необходимости.

11.3. Если создание копии данных необходимо для обработки обращения, Охранное агентство обязано обеспечить защиту такой копии.

11.4. После завершения цели обработки Охранное агентство обязано удалить или обезличить данные, если дальнейшее хранение не требуется по закону, Договору, спору, расследованию инцидента или защите прав Сторон.

11.5. Оператор вправе запросить у Охранного агентства подтверждение удаления или обезличивания данных.

12. Передача данных третьим лицам

12.1. Охранное агентство не вправе передавать персональные данные Пользователей третьим лицам без письменного согласия Оператора, если такая передача не требуется законодательством или непосредственной обработкой тревожного обращения.

12.2. Если передача данных третьему лицу необходима для исполнения закона, Охранное агентство обязано уведомить Оператора, если такое уведомление не запрещено законодательством.

12.3. Если Охранное агентство привлекает подрядчиков, субподрядчиков или внешних специалистов, которые могут получить доступ к данным QOR, такое привлечение допускается только при письменном согласии Оператора.

12.4. Охранное агентство несёт ответственность за действия привлечённых лиц как за свои собственные действия.

12.5. Подрядчики Охранного агентства должны принять на себя обязательства по конфиденциальности и защите данных не ниже уровня, предусмотренного настоящим Соглашением.

13. Обработка данных в мобильных устройствах и мессенджерах

13.1. Охранное агентство обязано ограничить использование личных мобильных телефонов сотрудников для обработки персональных данных Пользователей QOR.

13.2. Передача данных через мессенджеры допускается только в случаях, когда это необходимо для обработки обращения или согласовано Сторонами.

13.3. При использовании мессенджеров запрещается:

создавать несанкционированные группы с данными Пользователей;
пересылать данные лицам, не участвующим в обработке обращения;
сохранять данные в личных архивах;
публиковать данные;
использовать данные после завершения обращения;
пересылать данные на личные аккаунты сотрудников без необходимости.

13.4. Охранное агентство обязано удалять данные из временных каналов связи после завершения цели обработки, если дальнейшее хранение не требуется.

14. Обработка данных в бумажной форме

14.1. Если Охранное агентство распечатывает или фиксирует персональные данные на бумажном носителе, оно обязано обеспечить защиту таких документов.

14.2. Бумажные документы с персональными данными должны храниться в местах с ограниченным доступом.

14.3. Запрещается оставлять документы с персональными данными в открытом доступе, транспортных средствах, местах общего пользования, на стойках, рабочих столах без контроля или у неуполномоченных лиц.

14.4. После достижения цели обработки бумажные документы должны быть уничтожены способом, исключающим восстановление данных, если дальнейшее хранение не требуется законом или Договором.

15. Информационная безопасность

15.1. Охранное агентство обязано обеспечить минимальные меры информационной безопасности при работе с QOR.

15.2. Минимальные меры включают:

использование индивидуальных учётных записей;
запрет передачи паролей;
использование сложных паролей;
своевременное изменение паролей при подозрении на компрометацию;

ограничение доступа по ролям;
блокировку устройств при отсутствии сотрудника;
запрет доступа с незащищённых устройств;
обновление программного обеспечения;
использование антивирусной защиты при необходимости;
контроль доступа сотрудников;
удаление доступов уволенных сотрудников;
уведомление Оператора об инцидентах;
запрет массовой выгрузки данных без согласования.

15.3. Оператор вправе устанавливать дополнительные требования информационной безопасности.

15.4. Если Охранное агентство не может выполнить отдельные требования, оно обязано уведомить Оператора до начала обработки данных.

16. Инциденты безопасности

16.1. Охранное агентство обязано немедленно уведомить Оператора о любом инциденте безопасности.

16.2. Инцидентами безопасности считаются:

утрата персональных данных;
несанкционированный доступ;
разглашение данных;
ошибочная передача данных;
отправка данных неверному получателю;
компрометация аккаунта;
утрата устройства с доступом к QOR;
увольнение сотрудника с сохранённым доступом;
подозрение на копирование данных;
массовая выгрузка данных без основания;
кибератака;
вредоносное программное обеспечение;
утечка логина, пароля, API-ключа или токена;
иное событие, создающее риск для данных.

16.3. Уведомление об инциденте должно содержать:

дату и время выявления;
описание инцидента;
категории затронутых данных;
примерное количество затронутых лиц, если известно;
причину инцидента, если известна;
принятые меры;
ответственное лицо;
дальнейший план устранения последствий.

16.4. Охранное агентство обязано принять срочные меры для ограничения последствий инцидента.

16.5. Оператор вправе временно ограничить доступ Охранного агентства к QOR до устранения риска.

16.6. Охранное агентство обязано содействовать Оператору в расследовании инцидента.

17. Проверки и аудит

17.1. Оператор вправе проверять соблюдение Охранным агентством требований настоящего Соглашения.

17.2. Проверка может проводиться в форме:

- запроса документов;
- запроса перечня сотрудников с доступом;
- запроса подтверждения удаления данных;
- проверки логов QOR;
- проверки действий пользователей Охранного агентства;
- анализа инцидентов;
- анализа жалоб;
- запроса внутренних регламентов;
- опроса ответственных лиц;
- иных разумных контрольных действий.

17.3. Охранное агентство обязано предоставить запрошенные сведения в течение ____ рабочих дней с даты запроса Оператора.

17.4. Если проверка выявила нарушение, Оператор вправе потребовать устранения нарушения и предоставления плана корректирующих действий.

17.5. При существенном нарушении Оператор вправе ограничить доступ Охранного агентства к QOR или расторгнуть Договор.

18. Права Оператора

18.1. Оператор вправе:

- передавать Охранному агентству данные в необходимом объеме;
- ограничивать состав передаваемых данных;
- устанавливать правила доступа;
- устанавливать требования информационной безопасности;
- проверять соблюдение настоящего Соглашения;
- запрашивать документы и пояснения;
- требовать удаления данных;

требовать подтверждения удаления данных;
ограничивать доступ при нарушениях;
блокировать учётные записи сотрудников Охранного агентства;
отзывать API-ключи и токены;
приостанавливать передачу тревожных обращений;
требовать возмещения ущерба;
расторгнуть Договор при существенном нарушении.

19. Обязанности Оператора

19.1. Оператор обязуется:

передавать Охранному агентству данные только для целей Договора;
не передавать заведомо избыточные данные без необходимости;
обеспечить технические роли и доступы в QOR в пределах возможностей платформы;
принимать меры по защите данных в зоне своего контроля;
информировать Охранное агентство о существенных изменениях требований к обработке данных;
рассматривать уведомления Охранного агентства об инцидентах;
содействовать в урегулировании вопросов, связанных с правами Пользователей.

20. Права Охранного агентства

20.1. Охранное агентство вправе:

получать данные, необходимые для обработки тревожных обращений;
запрашивать уточнение данных по конкретному обращению;
использовать данные для реагирования и отчётности;
предлагать Оператору изменения в порядке передачи данных;
уведомлять Оператора о недостаточности или избыточности передаваемых данных;
запрашивать технические разъяснения по доступам, ролям и обработке данных.

21. Обязанности Охранного агентства

21.1. Охранное агентство обязуется:

обрабатывать данные только в целях Договора;
соблюдать конфиденциальность;
ограничивать доступ к данным;
назначить ответственного за обработку данных;
вести контроль сотрудников с доступом;
не передавать данные третьим лицам без основания;
не использовать данные для рекламы и продаж;
не создавать несанкционированные копии;
не выгружать данные массово без согласования;
удалять данные после достижения цели обработки;
уведомлять об инцидентах безопасности;
содействовать проверкам Оператора;

обеспечить обучение сотрудников;
возмещать ущерб, причинённый нарушением настоящего Соглашения.

22. Обработка запросов Пользователей

22.1. Если Пользователь обращается к Охранному агентству с запросом о персональных данных, полученных через QOR, Охранное агентство обязано перенаправить такой запрос Оператору или согласовать ответ с Оператором.

22.2. Охранное агентство не вправе самостоятельно изменять, удалять или предоставлять Пользователю данные из QOR, если это не предусмотрено функционалом платформы, Договором или письменным указанием Оператора.

22.3. Если запрос Пользователя касается действий Охранного агентства, Охранное агентство обязано предоставить Оператору необходимые сведения для подготовки ответа.

22.4. Охранное агентство обязано содействовать Оператору при реализации прав Пользователя на доступ, уточнение, удаление, ограничение обработки или отзыв согласия.

23. Удаление и возврат данных после прекращения Договора

23.1. После прекращения Договора Охранное агентство обязано прекратить обработку персональных данных, полученных через QOR, если дальнейшая обработка не требуется по закону, спору, отчётности или защите прав Сторон.

23.2. Охранное агентство обязано по требованию Оператора:

вернуть данные;
удалить данные;
обезличить данные;
подтвердить удаление;
ограничить доступ к архивным данным.

23.3. Если Охранное агентство обязано хранить отдельные данные по закону, оно должно обеспечить их защиту и использовать только для законной цели хранения.

23.4. Доступ Охранного агентства к QOR, S-OMS, API и иным системам подлежит прекращению после расторжения Договора, если иное не согласовано Сторонами.

24. Конфиденциальность

24.1. Все персональные данные, тревожные обращения, геолокационные данные, сведения об объектах и статусы являются конфиденциальной информацией.

24.2. Охранное агентство обязано сохранять конфиденциальность полученной информации.

24.3. Обязанность конфиденциальности действует в течение срока действия Договора и 5 лет после его прекращения, если более длительный срок не установлен законодательством или отдельным соглашением.

24.4. Если информация относится к персональным данным, обязанность защиты действует в течение всего срока обработки и хранения таких данных.

25. Ответственность Охранного агентства

25.1. Охранное агентство несёт ответственность за:

незаконную обработку данных;
использование данных вне целей Договора;
передачу данных третьим лицам без основания;
разглашение данных;
утрату данных;
несанкционированное копирование данных;
действия своих сотрудников;
действия своих подрядчиков;
несвоевременное уведомление об инциденте;
неудаление данных после достижения цели обработки;
нарушение конфиденциальности;
причинение ущерба Оператору, Пользователю или третьим лицам.

25.2. В случае нарушения настоящего Соглашения Охранное агентство обязано возместить Оператору документально подтверждённый ущерб, включая расходы на урегулирование претензий, восстановление данных, юридическое сопровождение, выплаты Пользователям и иные расходы, вызванные нарушением.

25.3. Если нарушение Охранного агентства повлекло претензии Пользователей, партнёров, государственных органов или третьих лиц к Оператору, Охранное агентство обязано содействовать Оператору в урегулировании таких претензий.

25.4. Нарушение режима персональных данных является существенным нарушением Договора и может повлечь немедленное ограничение доступа или расторжение Договора.

26. Ответственность Оператора

26.1. Оператор несёт ответственность за обработку персональных данных в зоне своего контроля.

26.2. Оператор не несёт ответственность за действия Охранного агентства, его сотрудников, подрядчиков, представителей и иных лиц, получивших доступ к данным через Охранное агентство.

26.3. Оператор не несёт ответственность за утечку, разглашение, незаконное использование или утрату данных после их получения Охранным агентством, если такая утечка, разглашение, использование или утрата произошли по вине Охранного агентства.

27. Санкции за нарушение Соглашения

27.1. При нарушении настоящего Соглашения Оператор вправе применить одну или несколько мер:

письменное предупреждение;
требование устранить нарушение;
требование предоставить план корректирующих действий;
временное ограничение доступа к данным;
блокировка отдельных сотрудников Охранного агентства;
отзыв API-ключей;
ограничение передачи тревожных обращений;
приостановление подключения к QOR;
расторжение Договора;
предъявление требования о возмещении ущерба;
иные меры, предусмотренные Договором и законодательством.

27.2. Применение санкций не освобождает Охранное агентство от обязанности устранить нарушение, возместить ущерб и обеспечить дальнейшую защиту данных.

28. Форс-мажор и внешние угрозы

28.1. Стороны освобождаются от ответственности за нарушение настоящего Соглашения, если оно вызвано обстоятельствами непреодолимой силы, которые Сторона не могла разумно предотвратить.

28.2. Форс-мажор не освобождает Охранное агентство от обязанности принять разумные меры по защите данных и уведомить Оператора об инциденте безопасности.

28.3. Кибератака, вредоносное программное обеспечение или внешний взлом не освобождают Охранное агентство от ответственности, если нарушение стало возможным из-за несоблюдения разумных мер информационной безопасности.

29. Срок действия Соглашения

29.1. Настоящее Соглашение вступает в силу с даты его подписания Сторонами либо с даты начала передачи персональных данных Охранному агентству.

29.2. Настоящее Соглашение действует в течение всего срока действия Договора.

29.3. Положения о конфиденциальности, защите данных, ответственности, удалении данных, запрете использования данных вне целей Договора и урегулировании

инцидентов продолжают действовать после прекращения Договора до полного исполнения соответствующих обязательств.

30. Изменение Соглашения

30.1. Настоящее Соглашение может быть изменено по соглашению Сторон.

30.2. Изменения оформляются дополнительным соглашением, новой редакцией приложения или иным способом, согласованным Сторонами.

30.3. Если изменения вызваны требованиями законодательства, информационной безопасности, изменением платформы QOR или требованиями защиты данных, Оператор вправе инициировать обновление настоящего Соглашения.

31. Разрешение споров

31.1. Все споры по настоящему Соглашению Стороны стремятся урегулировать путём переговоров.

31.2. До обращения в суд Сторона обязана направить другой Стороне письменную претензию.

31.3. Срок рассмотрения претензии составляет ____ рабочих дней с даты получения.

31.4. При невозможности урегулирования спора в досудебном порядке спор подлежит рассмотрению в суде по месту нахождения Оператора, если иное не согласовано Сторонами или не установлено законодательством Республики Казахстан.

32. Заключительные положения

32.1. Настоящее Соглашение регулируется законодательством Республики Казахстан.

32.2. Настоящее Соглашение является неотъемлемой частью Договора № ____ о подключении охранного агентства к цифровой платформе QOR.

32.3. В случае противоречия между настоящим Соглашением и Договором по вопросам обработки персональных данных приоритет имеют положения настоящего Соглашения, если иное прямо не указано в Договоре.

32.4. Недействительность отдельного положения настоящего Соглашения не влечёт недействительность остальных положений.

32.5. Стороны подтверждают, что обладают полномочиями на подписание настоящего Соглашения и принимают на себя обязательства по защите персональных данных.

33. Подписи Сторон

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: _____

Подпись: _____

М.П.

Охранное агентство

Наименование: _____

БИН/ИИН: _____

Руководитель: _____

Юридический адрес: _____

Телефон: _____

Email: _____

Лицензия/разрешение: _____

Подпись: _____

М.П.