

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

единый обязательный документ экосистемы CasaSRM

Редакция №2

Дата проекта: 19 июля 2026 года

Официальный сайт: <https://CasaSRM.com>

ПРОЕКТ РЕДАКЦИИ №2. Не публиковать до подтверждения размещения основной базы персональных данных на территории Республики Казахстан, внесения номера, даты и органа государственной регистрации ИП, подготовки юридически выверенной версии на казахском языке и финальной проверки юристом Республики Казахстан.

Статус документа

Заменяет отдельные политики конфиденциальности и обработки персональных данных; согласие субъекта остается отдельным действием. Настоящая редакция является единственным публичным источником соответствующей темы после публикации.

ПРОЕКТ РЕДАКЦИИ №2. Не публиковать до подтверждения размещения основной базы персональных данных на территории Республики Казахстан, внесения номера, даты и органа государственной регистрации ИП, подготовки юридически выверенной версии на казахском языке и финальной проверки юристом Республики Казахстан.

1. Статус документа

Эта Политика является единственным авторитетным документом пакета по категориям, целям, основаниям, операциям, правам субъектов и организационным правилам обработки персональных данных. Другие документы содержат только необходимое краткое уведомление и ссылку сюда.

Оператор собственных данных аккаунта: ИП «ONLINE-PAY». При обработке рабочих данных по поручению бизнеса роли сторон определяются Соглашением о поручении обработки персональных данных.

CasaSRM — торговый клиент для продавцов, кассиров, кладовщиков и локальных администраторов, доступный как веб-версия, Android- и Windows-приложение. Casa Control — защищенный веб-кабинет владельца бизнеса для создания и настройки аккаунта, бизнеса, магазинов, складов, сотрудников, прав, тарифов и иных глобальных параметров. CasaSRM.com — официальный сайт экосистемы и место приобретения подписки.

Документ применяется с учетом Цифрового кодекса Республики Казахстан от 9 января 2026 года № 255-VIII и Закона Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V, включая требования к подтверждаемому согласию, минимизации данных, локализации базы, трансграничной передаче, безопасности и правам субъекта цифровых данных.

2. Принципы

Обработка ведется законно, добросовестно, прозрачно, только для определенных целей и в минимально необходимом объеме. Обеспечиваются точность, ограничение срока хранения, конфиденциальность, контролируемый доступ и подотчетность. Несовместимое повторное использование требует нового основания.

3. Категории и субъекты

Субъекты: владельцы бизнеса, пользователи Casa Control, продавцы и иные сотрудники CasaSRM, посетители CasaSRM.com, представители контрагентов и лица, чьи данные законно внесены бизнесом.

Категории: идентификационные и контактные данные; учетная запись, роль и принадлежность к бизнесу; данные устройства и сессии; журнал действий и безопасности; настройки; сведения о подписке, счете и статусе платежа; сообщения поддержки; Cookie/аналитические идентификаторы; рабочие записи, внесенные бизнесом. Специальные категории и биометрия не собираются без отдельной необходимости и законного основания.

4. Цели и основания

Цели: создание аккаунта, аутентификация, предоставление и синхронизация функций, управление доступом, поддержка, безопасность, резервное восстановление, исполнение договора, оплата, бухгалтерское и обязательное хранение, защита прав, предотвращение злоупотреблений. Основания: подтверждаемое согласие; договор и действия до его заключения; обязанность по закону; иные прямо предусмотренные законом основания.

5. Операции и источники

Допустимые операции: сбор, запись, систематизация, хранение, уточнение, использование, передача уполномоченному получателю, блокирование, обезличивание, удаление и уничтожение. Источники: субъект, его работодатель/владелец бизнеса, устройство, журналы системы и подключенные провайдеры.

6. Согласие

Когда требуется согласие, фиксируются оператор и его ИИН; субъект; срок или период; перечень данных; цели; сведения о передаче третьим лицам; наличие либо отсутствие трансграничной передачи; наличие либо отсутствие распространения в общедоступных источниках; способ и время акцепта; версия текста.

Согласие не объединяется с необязательной рекламой. Отзыв направляется Оператору. В течение пятнадцати рабочих дней обработка на основании согласия прекращается, если отсутствует другое законное основание, либо субъекту направляется мотивированный отказ.

7. Роли бизнеса и Оператора

Владелец бизнеса определяет законность внесения данных своих сотрудников, клиентов и контрагентов, выдает роли и отвечает за их актуальность. Оператор обрабатывает такие данные только по документированным инструкциям, обеспечивает общие меры защиты, помогает реализовывать права субъектов и не использует рабочие данные для собственных рекламных целей.

8. Локализация и трансграничная передача

Хранение персональных данных в электронной базе обеспечивается на территории Республики Казахстан. Резервные копии и реплики, содержащие персональные данные, подчиняются тому же требованию, если закон не допускает иное.

Трансграничная передача осуществляется только при разрешенном законом основании, требуемом уровне защиты и предварительном раскрытии субъекту. Категория получателя, страна, цель и набор данных документируются. До подтверждения локализации промышленная обработка персональных данных запрещена.

9. Получатели и обработчики

Доступ ограничен ролью. Передача возможна хостингу, провайдерам аутентификации, сообщений, платежей, поддержки и безопасности; государственным органам — только при законном требовании; новому правообладателю — при законной передаче обязательств и предварительном уведомлении. Актуальный реестр обработчиков поддерживается Оператором.

10. Безопасность и нарушения

Меры включают многофакторную защиту административного доступа, принцип наименьших привилегий, шифрование каналов, управление секретами, журналирование, резервное копирование, тесты восстановления, управление уязвимостями и обучение персонала.

При обнаружении нарушения безопасности персональных данных Оператор регистрирует событие, ограничивает последствия, сохраняет доказательства и уведомляет уполномоченный орган в течение одного рабочего дня с момента обнаружения, если обязанность применима. Субъекты уведомляются в порядке, установленном законом и оценкой риска.

11. Сроки, удаление и уничтожение

Единственный авторитетный график сроков содержится в Политике хранения и удаления данных. По достижении цели данные удаляются или уничтожаются, если закон, неисполненное обязательство, спор или защита прав не требуют ограниченного дальнейшего хранения. Удаление аккаунта не означает уничтожение обязательных бухгалтерских и аудиторских записей.

12. Права субъекта

Субъект вправе знать о наличии и источнике данных; получить доступ; потребовать исправления, блокирования, ограничения обработки, удаления или уничтожения; отозвать согласие; получить сведения о передаче; потребовать человеческого пересмотра значимого автоматизированного решения; обжаловать действия.

13. Обращения, контроль и изменения

Запросы направляются на leonix.tech.io@gmail.com после разумной проверки личности и полномочий. Все запросы и ответы регистрируются без избыточного раскрытия данных. Существенное изменение целей, категорий или трансграничной передачи требует пересмотра основания и, когда необходимо, нового согласия.

Контакты и реквизиты

Оператор / Правообладатель: ИП «ONLINE-PAY»

Владелец: Тарасенко Максим Андреевич

ИИН: 030218551187

Адрес: ул. Заводская, 36, г. Петропавловск, 150000, Республика Казахстан

Телефон: +7 776 140 73 12

Официальный сайт: <https://CasaSRM.com>

Email: leonix.tech.io@gmail.com

Telegram: @LeonixTM

WhatsApp: <https://chat.whatsapp.com/CnQnmpCrJCb2gS1GM3Q3YO?s=cl&p=a&mlu=3>

Часы поддержки: ежедневно, 12:00–19:00 (время г. Петропавловска)

Номер, дата и орган государственной регистрации ИП должны быть добавлены до публикации.

История изменений

Редакция №2 от 19 июля 2026 года — первая публикация. Редакция №2 от 19 июля 2026 года — обязательные элементы согласия, локализация, цифровые права, уведомление об инциденте и единое владение правилами.

Архитектура хранения и синхронизации данных

1. Обязательный казахстанский контур персональных данных

ИП «ONLINE-PAY» организует на территории Республики Казахстан авторитетную электронную базу персональных данных (далее — Реестр ПД РК). Реестр ПД РК должен содержать полный актуальный набор персональных данных, необходимый для подтверждения учетной записи, принадлежности пользователя к бизнесу, выданных ролей и доступов, истории согласий, обращений субъектов и иных операций, для которых законодательство требует локального хранения. Локальная копия только регистрационных данных на компьютере владельца бизнеса не заменяет Реестр ПД РК, если персональные данные сотрудников, клиентов, контактов, журналов или поддержки остаются исключительно в зарубежном облаке.

До промышленного запуска должны быть документально зафиксированы: оператор казахстанского центра обработки данных; адрес площадки; ответственное лицо; перечень коллекций Реестра ПД РК; схема шифрования и управления ключами; резервное копирование в Казахстане; сроки восстановления; контроль целостности; порядок удаления; результаты теста восстановления. Доступ владельца бизнеса к данным осуществляется через Casa Control по

ролям и не означает свободного доступа ИП «ONLINE-PAY» к содержимому всех арендаторов.

2. Firebase Authentication

Firebase Authentication используется как внешний сервис аутентификации. Он может обрабатывать идентификатор пользователя, email или номер телефона, технические идентификаторы, сведения о провайдере входа, времени входа, токенах и событиях безопасности. По опубликованным условиям Google обработка данных Firebase Authentication привязана к инфраструктуре за пределами Казахстана, включая США. Поэтому такая обработка является трансграничной, раскрывается субъекту до регистрации и учитывается в согласии. Пароли в открытом виде ИП «ONLINE-PAY» не получает и не хранит.

3. Cloud Firestore

Cloud Firestore используется как оперативная база синхронизации CasaSRM и Casa Control. Фактический неизменяемый регион базы проекта kassa-srm, проверенный через Firebase CLI 19 июля 2026 года, — europe-west3 (Франкфурт, Германия). Firestore не имеет региона размещения в Казахстане. В нем допускается хранение данных только после классификации каждой коллекции, определения законного основания и подтверждения наличия полной требуемой записи в Реестре ПД РК.

Предпочтительная модель: в Firestore используются tenant_id, business_id, store_id, user_id и иные псевдонимные идентификаторы; прямые идентификаторы и подтверждающие документы находятся в Реестре ПД РК; разрешение идентификаторов выполняется защищенным серверным API. Если в Firestore передаются имена, телефоны, email, клиентские карточки, комментарии, чеки с идентификаторами, IP-адреса, журналы действий либо иные персональные данные, это отдельно включается в перечень трансграничной передачи и согласие.

4. Cloud Functions, Hosting, Crash- и push-сервисы

Серверные функции проекта в текущей конфигурации исполняются в регионе europe-west1. Firebase Hosting и связанные сети доставки контента могут обслуживать запросы глобально. Firebase Cloud Messaging, средства журналирования, диагностики сбоев и аналитики подключаются только после внесения в реестр обработчиков, оценки необходимости, настройки минимизации и обновления пользовательского уведомления. Содержание уведомления не должно раскрывать кассовые, платежные или персональные сведения на экране блокировки.

5. Поток регистрации и выдачи доступа

При регистрации Casa Control создает техническую учетную запись в Firebase Authentication и запись статуса в Firestore. Проверенные реквизиты владельца, контактные данные, согласие, роль, принадлежность к бизнесу и история выдачи/отзыва доступа записываются в Реестр ПД РК. Владелец бизнеса вправе приглашать сотрудников и назначать разрешенные роли, но не вправе обходить минимальные требования, просматривать пароли или выдавать права другого арендатора. Любое назначение, расширение, приостановление и отзыв роли журналируется с request_id, временем, инициатором и результатом.

6. Синхронизация и разрешение конфликтов

Серверный API является источником бизнес-истины. Локальное хранилище Windows/Android является зашифрованным офлайн-кэшем и очередью исходящих операций, а не самостоятельной базой полномочий. Каждая операция содержит tenant_id, business_id, store_id, user_id, версию, идемпотентный ключ и отметку времени. После восстановления связи сервер повторно проверяет роль, лицензию, версию объекта и допустимость операции. Конфликт не разрешается молча: денежные и складские операции журналируются и обрабатываются по доменному правилу; персональные данные сверяются с Реестром ПД РК.

7. Запреты

Запрещается хранить в Firestore, локальном кэше, журналах или аналитике пароли, секретные ключи, полные данные платежных карт, коды подтверждения после использования, необработанные документы личности без отдельного законного основания, а также избыточное содержимое чеков и обращений. Запрещено использовать производственные персональные данные в тестовых проектах. Экспорт, резервные копии и административные выгрузки наследуют классификацию исходных данных.

Детальный реестр категорий данных

Учетная запись и доступ

- Данные: имя, email и/или телефон, UID, статус подтверждения, язык, роль, бизнес и магазин, события приглашения, выдачи и отзыва доступа.
- Цели: регистрация, вход, управление полномочиями, безопасность и поддержка.
- Источники: субъект, владелец бизнеса, система аутентификации.
- Системы: Реестр ПД РК; ограниченная оперативная запись Firebase Authentication/Firestore; локальный токен и минимальный кэш на устройстве.
- Получатели: уполномоченный владелец бизнеса, ИП «ONLINE-PAY» в пределах служебной необходимости, Google как обработчик соответствующего Firebase-сервиса.

Рабочие данные сотрудника

- Данные: имя или рабочий псевдоним, должность, роль, магазин, смены, назначенные задачи, действия в документах и журнал аудита.
- Цели: исполнение трудовых и торговых процессов, предотвращение злоупотреблений, разрешение споров.
- Владелец бизнеса отвечает за законность внесения данных своих сотрудников; ИП «ONLINE-PAY» обрабатывает их по поручению и для безопасности платформы.

Данные клиентов бизнеса

- Данные: имя, контакт, история продаж или возвратов, скидки и иные сведения только в объеме, который бизнес законно собирает для конкретной операции.
- Запрещено делать обязательными необязательные поля. Владелец бизнеса обязан самостоятельно получить необходимое согласие или иметь другое законное основание.
- ИП «ONLINE-PAY» не использует клиентскую базу бизнеса для собственной рекламы и не объединяет ее между арендаторами.

Платежи и подписка

- Данные: плательщик, сумма, валюта, тариф, период, идентификатор и статус транзакции, счет или чек, сведения о возврате. Полные реквизиты банковской карты не хранятся.
- Цели: заключение и исполнение договора, бухгалтерский и налоговый учет, возвраты и противодействие мошенничеству.

Устройство, безопасность и поддержка

- Данные: тип приложения и ОС, версия, device_id в минимальном объеме, IP-адрес, время входа, коды ошибок, request_id, события доступа, текст и вложения обращения.
- Цели: защита учетной записи, диагностика, исполнение SLA и расследование инцидентов.
- Пользователь не должен отправлять в поддержку пароли, ключи, полные платежные реквизиты и избыточные документы личности.

Веб-сайт и Cookie

- Данные: необходимые идентификаторы сессии и согласия; необязательная аналитика — только после отдельного выбора пользователя.
- Конкретные названия, поставщики, сроки и цели Cookie публикуются в живом реестре Cookie; отсутствующий в реестре необязательный трекер не должен загружаться.

Порядок реализации прав субъекта

Запрос принимается по официальному email, а после запуска соответствующей функции — через Casa Control. Запрос содержит достаточные сведения для поиска записи и описание требуемого действия; лишние персональные данные и копии документов не запрашиваются. Личность и полномочия проверяются соразмерным способом. Каждому запросу присваиваются номер, дата получения, ответственный и срок.

Оператор определяет, выступает ли он владельцем базы либо обработчиком по поручению конкретного бизнеса. В последнем случае запрос без промедления передается владельцу бизнеса, а субъекту сообщается маршрут. По запросу предоставляется понятная информация об источнике, целях, основании, составе, сроке, получателях, трансграничной передаче и автоматизированной обработке; выполняются исправление, блокирование, ограничение, удаление или отзыв согласия, если закон не требует сохранить конкретную запись.

При отзыве согласия обработка, основанная только на нем, прекращается в установленный законом срок; сохранение на ином основании документируется и объясняется субъекту. Удаление распространяется на активные системы, очереди и доступные копии по утвержденной процедуре; неизменяемая резервная копия выводится из обычного использования и очищается при штатной ротации. Отказ должен быть мотивированным, проверяемым и содержать способ обжалования.

Матрица ответственности

ИП «ONLINE-PAY» является владельцем базы и/или оператором для данных собственного аккаунта, подписки, безопасности сайта и прямой поддержки. Владелец бизнеса является владельцем базы своих сотрудников, клиентов и хозяйственных записей; ИП «ONLINE-PAY» выступает обработчиком в пределах Соглашения о поручении обработки персональных данных. Google и иные инфраструктурные поставщики являются привлеченными обработчиками в пределах их договоров. Название роли не отменяет обязанностей, прямо возложенных законом.

Контроль перед релизом

До 1 августа 2026 года должны быть завершены: ввод Реестра ПД РК; инвентаризация всех коллекций Firestore; фиксация региона; проверка правил безопасности и tenant-изоляции; запрет прямых клиентских записей в чужие коллекции; включение App Check там, где применимо; ротация ключей; тест экспорта, удаления и восстановления; оформление трансграничного согласия; актуализация реестра обработчиков.