# Политика защиты данных

ИП Руденко Вячеслав Сергеевич, ИНН 743805184150, адрес: 198261, г. Санкт-Петербург, Ленинский проспект, дом 43, кв. 556, e-mail: support@veruna.io.

## 1. Цели и принципы

Цель Политики — обеспечить защиту персональных данных при их обработке Оператором. Принципы: законность, минимизация, целевое ограничение, точность, ограничение хранения, конфиденциальность и целостность.

## 2. Категории данных и субъектов

Категории субъектов: пользователи Сервиса, заявители обращений, плательщики. Категории данных: учётные, платёжные, технические, переписка.

## 3. Сроки хранения и удаление

Аккаунты — до удаления / 3 года неактивности; логи — 12 месяцев; финансовые документы — 5 лет; маркетинговые рассылки — до отзыва согласия. Применяется soft-delete с последующим физическим удалением по регламенту.

## 4. Доступ и контроль

Ролевая модель доступа (RBAC); многофакторная аутентификация (MFA) для административных учётных записей и для доступа к продуктивным базам данных; пересмотр прав доступа не реже 1 раза в квартал; журналирование административных действий; хранение секретов в защищённом хранилище (vault); принцип наименьших привилегий.

## 5. Безопасность

Шифрование трафика TLS; пароли в виде hash+salt; своевременные обновления ПО; резервное копирование; мониторинг аномалий; тестовые среды без продуктивных ПДн или с обезличиванием.

Оператором разработаны и поддерживаются в актуальном состоянии модель угроз безопасности персональных данных и оценка вреда субъектам ПДн в соответствии с ч. 2 ст. 18.1 Федерального закона № 152-ФЗ. Внутренний аудит мер защиты ПДн проводится не реже 1 раза в год; по итогам аудита формируется отчёт и план устранения выявленных недостатков.

## 6. Подрядчики и обработчики

До подключения подрядчика проводится проверка местонахождения данных, заключается договор поручения/обработки (ч. 3 ст. 6 ФЗ-152), при необходимости — соглашение о защите данных (DPA); согласовываются процедуры реагирования на инциденты; перечень и условия периодически пересматриваются.

## 7. Инциденты и уведомления

При выявлении инцидента, повлёкшего неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, Оператор:

(1) уведомляет Роскомнадзор о факте инцидента в течение 24 часов через специализированный сервис на сайте РКН (https://pd.rkn.gov.ru) — в объёме, предусмотренном ч. 3.1 ст. 21 ФЗ-152;

(2) предоставляет в Роскомнадзор результаты внутреннего расследования инцидента, включая сведения о лицах, действия которых стали причиной инцидента, в течение 72 часов;

(3) уведомляет затронутых субъектов ПДн без неоправданной задержки доступными каналами связи (e-mail, уведомление в Личном кабинете).

Ведётся реестр инцидентов; по итогам каждого инцидента проводится анализ причин и принимаются меры по предотвращению повторов. Тестирование плана реагирования на инциденты безопасности персональных данных проводится не реже 1 раза в год.

## 8. Обучение и оффбординг

Обязательный тренинг по безопасности для лиц, допущенных к обработке ПДн; отзыв доступов при прекращении сотрудничества; контроль возврата/уничтожения носителей информации.

## 9. Пересмотр

Пересмотр Политики — ежегодно или при существенных изменениях процессов/законодательства. Ответственный: ИП Руденко В.С.

*Дата: 24.06.2026. Версия 1.0*