REPLAYBOX / ПРАВОВЫЕ ДОКУМЕНТЫ

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИИ

Организационные и технические меры защиты данных и информации в ReplayBox.

Версия	**1.1**
Дата публикации	**24 сентября 2026 года**
Оператор	**ИП Струков Павел Николаевич**
ИНН / ОГРНИП	**771314210244 / 324774600166372**
Контакт	**support@replaybox.ru**

Актуальная веб-версия документа: https://replaybox.ru/legal/personal-data

1. Назначение и область действия

1.1. Настоящая Политика описывает организационные и технические подходы ИП Струкова Павла Николаевича (далее - «Оператор») к обработке и защите персональных данных и иной информации в ReplayBox.

1.2. Документ дополняет, но не заменяет Политику конфиденциальности. Цели, категории данных, правовые основания, сроки и права субъектов определяются Политикой конфиденциальности: https://replaybox.ru/legal/privacy.

1.3. Политика распространяется на сайт, личный кабинет, серверную часть, программу ReplayBox, базы данных, объектное хранилище, электронную почту и административные средства.

1.4. Публикуемая редакция не раскрывает пароли, ключи, адреса внутренних систем, схемы защиты и иные сведения, которые могли бы снизить безопасность.

1.5. Основой мер являются требования законодательства Российской Федерации, оценка возможного вреда и актуальных угроз.

2. Ответственность и управление

2.1. Оператор организует обработку, утверждает документы, определяет доступы и контролирует исполнение требований.

2.2. Лица, допущенные к обработке, получают только необходимые полномочия и обязуются соблюдать конфиденциальность.

2.3. Административный доступ предоставляется индивидуально и может быть отозван при изменении обязанностей или выявлении риска.

2.4. Оператор учитывает используемые информационные системы, категории данных, поставщиков и места хранения.

2.5. Существенные изменения обработки оцениваются до ввода соответствующей функции в эксплуатацию.

3. Категории защищаемой информации

3.1. Оператор защищает:

- данные учётных записей;
- данные авторизации, сессий и восстановления доступа;
- идентификаторы установок приложения и антифрод-сведения;
- пользовательские видеозаписи, звук, превью, заметки и метаданные;
- жалобы и результаты модерации;
- обращения в поддержку;
- технические журналы и сведения о событиях безопасности;
- договорные, платёжные и бухгалтерские сведения, если платные функции подключены;
- ключи, конфигурации и иную служебную информацию Оператора.

3.2. По режиму доступа информация подразделяется на:

- общедоступную - законно опубликованные сведения и материалы;
- пользовательскую ограниченного доступа - данные учётной записи и материалы по непубличной ссылке;
- конфиденциальную - персональные данные, секреты доступа и служебные сведения;
- критическую служебную - ключи, пароли, резервные коды и конфигурации безопасности.

3.3. Присвоение публичного режима материалу не делает общедоступными пароль, email, токены и иные связанные данные, если это прямо не предусмотрено и не имеет законного основания.

4. Принципы защиты

4.1. Оператор применяет:

- законность и ограничение целей;
- минимизацию собираемых данных;
- разделение пользовательского и административного доступа;
- предоставление минимально необходимых прав;
- защиту на всём жизненном цикле;
- своевременное обновление и устранение уязвимостей;
- контролируемое привлечение поставщиков;
- регистрацию значимых событий;
- ограничение сроков хранения;
- готовность к реагированию на инциденты.

4.2. Меры выбираются с учётом объёма и характера данных, доступных технологий, стоимости реализации и вероятного вреда субъектам.

5. Сбор и передача данных

5.1. Сбор осуществляется через формы сайта, личный кабинет, программу, загрузку файлов, обращения и технические запросы.

5.2. При сборе через интернет первичная запись и хранение данных граждан Российской Федерации выполняются с использованием баз данных в Российской Федерации.

5.3. Передача между Пользователем и Сервисом выполняется по защищённому соединению, если соответствующая технология поддерживается.

5.4. Аналитические технологии активируются только после отдельного согласия, кроме обязательных технических средств.

5.5. Токены подтверждения и восстановления не должны передаваться в аналитические системы. Параметры чувствительных ссылок исключаются из адресов, направляемых в аналитику.

5.6. Оператор не запрашивает пароль по электронной почте и не требует сообщать полный номер карты или код безопасности.

6. Защита учётных записей и сессий

6.1. Пароли хранятся в виде криптографических хешей с использованием алгоритма, предназначенного для защиты паролей.

6.2. Сессионные, проверочные и восстановительные токены хранятся в виде хешей, когда хранение открытого значения не требуется для доставки.

6.3. Сессии имеют ограниченный срок действия и могут быть отозваны.

6.4. Для подключения приложения применяются одноразовые коды, ограниченные по времени, и криптографическое подтверждение установки.

6.5. Оператор ограничивает частоту чувствительных запросов и применяет средство защиты от автоматизированных регистраций.

6.6. Пользователь обязан использовать уникальный пароль, защищать устройство и незамедлительно сообщать о компрометации.

7. Защита пользовательских материалов

7.1. Видеофайлы и превью размещаются в приватном объектном хранилище.

7.2. Доступ к опубликованному материалу предоставляется через уникальный непредсказуемый токен ссылки и с учётом настройки видимости.

7.3. Публичная ссылка может быть передана получателем третьим лицам, поэтому Пользователь обязан контролировать её передачу.

7.4. Оператор ограничивает административный просмотр целями поддержки, безопасности, модерации, исполнения запроса или закона.

7.5. Для незавершённых загрузок устанавливается отдельный срок жизни. Завершённые материалы удаляются по сроку тарифа или команде Пользователя.

7.6. Оператор не использует содержание пользовательских видео для рекламного профилирования или обучения собственных моделей.

8. Криптографическая и секретная информация

8.1. Секреты приложения и инфраструктуры не включаются в общедоступный код и правовые документы.

8.2. Временное содержимое очереди сервисных писем шифруется до отправки и удаляется после завершения обработки.

8.3. Закрытый ключ установки программы создаётся и хранится на устройстве Пользователя; Оператор получает открытый ключ и его цифровой отпечаток.

8.4. Ключи и пароли поставщиков хранятся отдельно от общедоступных материалов и доступны ограниченному кругу лиц.

8.5. При подозрении на компрометацию секрет отзывается или заменяется в разумный срок.

9. Управление доступом

9.1. Доступ предоставляется по ролям и задачам.

9.2. Администратору может быть доступна информация о пользователях, материалах и жалобах в объёме, необходимом для поддержки и модерации.

9.3. Действия с повышенными полномочиями по возможности регистрируются и подлежат проверке.

9.4. Общие учётные записи административного доступа не используются, если технически доступна индивидуальная идентификация.

9.5. После прекращения полномочий доступ подлежит отзыву.

10. Журналирование и мониторинг

10.1. Оператор может регистрировать дату, время, адрес запроса, User-Agent, результат операции, техническую ошибку и идентификатор события.

10.2. Журналы используются для диагностики, безопасности и расследования инцидентов, а не для скрытого профилирования.

10.3. Доступ к журналам ограничивается. Срок хранения определяется Политикой конфиденциальности и необходимостью расследования.

10.4. Сведения журналов минимизируются и не должны включать пароли, полные платёжные реквизиты или открытые токены.

10.5. Выявленные аномалии могут привести к временному ограничению сессии или установки с возможностью обращения в поддержку.

11. Разработка и эксплуатация

11.1. Изменения программы проходят проверку в объёме, соразмерном риску.

11.2. Используемые зависимости и базовые компоненты обновляются с учётом известных уязвимостей и совместимости.

11.3. Доступ к производственной среде отделяется от обычной пользовательской работы.

11.4. Конфигурации проверяются перед публикацией, чтобы исключить случайное раскрытие ключей и служебных данных.

11.5. Ошибки не должны раскрывать Пользователю внутренние секреты или данные другого лица.

11.6. Оператор поддерживает процедуры восстановления работоспособности и целостности в объёме, предусмотренном архитектурой Сервиса.

12. Поставщики и обработка по поручению

12.1. Поставщики привлекаются на основании договора и только в необходимом объёме.

12.2. Основные категории поставщиков:

- Timeweb Cloud - серверная инфраструктура и объектное хранение;
- ООО «Яндекс.Облако» - отправка сервисных писем;
- Cloudflare - защита форм через Turnstile;
- ООО «ЯНДЕКС» - аналитика после получения согласия.

12.3. Актуальные документы поставщиков: https://replaybox.ru/legal/personal-data#section-12.

12.4. Поставщикам устанавливаются требования конфиденциальности, безопасности, удаления и содействия при инцидентах в применимом объёме.

12.5. Перед подключением поставщика оцениваются место обработки, назначение, доступ к данным и наличие необходимых договорных условий.

13. Сроки хранения и уничтожение

13.1. Сроки для каждой цели определены Политикой конфиденциальности: https://replaybox.ru/legal/privacy.

13.2. По окончании срока активный доступ прекращается, а данные удаляются, уничтожаются или обезличиваются.

13.3. Автоматическое удаление применяется там, где это технически возможно; иные операции выполняются по установленной процедуре.

13.4. Если немедленное уничтожение невозможно, данные блокируются до завершения удаления.

13.5. Уничтожение подтверждается в случаях и форме, предусмотренных законодательством.

13.6. Данные, обязательные для бухгалтерского учёта, исполнения закона или разрешения спора, отделяются от активного профиля и хранятся только в необходимом объёме.

14. Реагирование на инциденты

14.1. Признаками инцидента могут быть неправомерный доступ, раскрытие, изменение, уничтожение, потеря доступности или компрометация секретов.

14.2. При инциденте Оператор:

- регистрирует сообщение;
- ограничивает дальнейшее воздействие;
- сохраняет необходимые технические сведения;
- определяет затронутые системы и данные;
- устраняет причину и последствия;
- оценивает возможный вред;

- уведомляет уполномоченный орган и субъектов в случаях и сроки, установленные законом;
- документирует результаты расследования.

14.3. Сообщение об инциденте направляется на support@replaybox.ru с темой «Безопасность».

14.4. Пользователь не должен публично раскрывать действующие ключи, токены или персональные данные при сообщении об уязвимости.

15. Права пользователей

15.1. Пользователь вправе получить сведения об обработке, потребовать уточнения, блокирования, прекращения или удаления данных в предусмотренных законом случаях.

15.2. Обращение направляется на support@replaybox.ru или по почтовому адресу Оператора.

15.3. До предоставления данных Оператор вправе проверить личность заявителя разумным и соразмерным способом.

15.4. Пользователь может управлять материалами и сессиями через доступные функции личного кабинета.

15.5. Подробный порядок реализации прав содержится в Политике конфиденциальности: https://replaybox.ru/legal/privacy.

16. Контроль и совершенствование

16.1. Оператор периодически проверяет соответствие фактической обработки документам и требованиям закона.

16.2. При изменении функций проводится оценка необходимости новых данных, срока хранения и согласий.

16.3. Лица с доступом знакомятся с требованиями конфиденциальности и безопасной обработки.

16.4. Выявленные нарушения устраняются, а документы и технические меры актуализируются.

16.5. Оператор может привлекать специалистов для проверки при условии конфиденциальности.

17. Заключительные положения

17.1. Политика действует с 20 сентября 2026 года.

17.2. Действующая редакция размещается по адресу https://replaybox.ru/legal/personal-data.

17.3. Архив редакций размещается по адресу https://replaybox.ru/legal/personal-data#versions.

17.4. Политика конфиденциальности: https://replaybox.ru/legal/privacy.

17.5. Поручение на обработку персональных данных: https://replaybox.ru/legal/data-processing.

17.6. Вопросы по защите информации направляются на support@replaybox.ru.