Для закупок

Опросник по безопасности с готовыми ответами

Честные ответы на вопросы, которые чаще всего задают при проверке безопасности в компании. Если чего-то нет, мы так и пишем: «Нет».

Статус ответа: Да | Частично | Нет | Справка

Общее

Справка

Где хранятся данные?

Серверы и зашифрованные резервные копии находятся в Финляндии. Google/Firebase, AI-провайдер и некоторые другие субобработчики могут обрабатывать данные в США и других странах (Политика конфиденциальности).

Да

Раскрыт ли список субобработчиков?

Да: Google/Firebase, LiveKit, хостинг-провайдер и AI-провайдер (только для AI-функций). См. раздел 6 DPA.

Да

Есть ли соглашение об обработке данных (DPA)?

Шаблон на странице /dpa. Подписанный экземпляр можно получить по запросу (после регистрации юридического лица).

Нет

Есть ли сертификаты ISO 27001 / SOC 2?

Нет. Меры открыто описаны на странице /security и в этом опроснике.

Доступ и права

Да

Как аутентифицируются пользователи панели HR?

Firebase Authentication (e-mail и пароль). Хранение и проверка пароля выполняются Google/Firebase.

Нет

Есть ли многофакторная аутентификация (MFA)?

В панели HR пока нет.

Да

Есть ли доступ на основе ролей и прав?

Да: участникам команды выдаются отдельные права на вакансии, профиль, интервью и другое. Роль проверяется по базе при каждом запросе.

Да

Как разделены данные разных компаний?

Компания видит только отклики, экзамены и интервью по своим вакансиям.

Справка

Могут ли сотрудники платформы просматривать данные клиентов?

Только аккаунты с ролью администратора (для модерации и поддержки). Роль проверяется по базе.

Защита данных

Да

Шифруются ли данные при передаче?

Да: весь трафик идёт по HTTPS; в API включены заголовки безопасности (Helmet).

Частично

Шифруются ли данные при хранении?

Чувствительные поля шифруются на уровне полей AES-256-GCM: имя, e-mail, телефон, дата рождения и ссылки в резюме; переписка и сообщения в поддержку; телефон для интервью. Остальные поля (например, текст вакансии) хранятся открыто для поиска.

Справка

Как управляются ключи шифрования?

Ключи хранятся в окружении сервера, поддерживается ротация. При потере ключа зашифрованные данные не восстановить, поэтому копия ключа защищается отдельно.

Да

Есть ли резервные копии?

Да: зашифрованные, в отдельном хранилище, в Финляндии. Их состояние отслеживается на публичной странице статуса. Удалённые данные могут оставаться в копиях около 30 дней.

Да

Определены ли сроки хранения?

Да: видео экзаменов и откликов удаляется автоматически через 14 дней; видео, не привязанное к отклику, — через 6 часов.

Да

Можно ли удалить данные пользователя?

Да: кандидат удаляет аккаунт, персональные данные обезличиваются. Удаление данных компании выполняется по запросу.

Безопасность приложения

Да

Проверяются ли входящие данные?

Да: строгая проверка схемы, неизвестные поля отклоняются.

Да

Есть ли ограничение частоты запросов?

Да: по всему API, с более строгими лимитами для чувствительных операций.

Да

Как ограничен CORS?

Только списком одобренных адресов.

Да

Есть ли процесс сообщения об уязвимостях?

Да: страница /security и /.well-known/security.txt. Денежной программы вознаграждений нет.

Эксплуатация и устойчивость

Да

Есть ли мониторинг?

Да: сервисы проверяются каждые 5 минут; результаты и история инцидентов — на публичной странице статуса.

Да

Есть ли обязательство уведомлять о нарушениях?

Да: по DPA, без необоснованной задержки и, по возможности, в течение 72 часов.

Частично

Есть ли план аварийного восстановления с RTO/RPO?

Восстановление из резервной копии возможно; формального обязательства по RTO/RPO и письменного плана восстановления пока нет.

Конфиденциальность и AI

Да

Фиксируется ли согласие?

Да: сохраняются дата принятия и версия документа; при существенных изменениях согласие запрашивается повторно.

Да

Принимает ли AI решения о кандидатах?

Нет. AI только помогает; решение о найме или отказе принимает человек (условия для компаний, раздел 6).

Да

Как обрабатываются запросы субъектов данных (доступ, исправление, удаление)?

Через support@sizinkaryera.life; кандидат во многих случаях может сделать это сам в приложении.

Ответы верны на указанную дату и описывают текущее состояние Sizin Karyera. Если нужен другой формат (CAIQ, SIG и т. д.), пришлите нам вопросы.

Обновлено: 2026-11-21