Политика конфиденциальности

Silence environment

Дата вступления в силу: 13.01.2026

ОПРЕДЕЛЕНИЯ

Провайдер: Silence AI (далее -«Провайдер», «мы», «нас», «наш»), юридическое лицо, зарегистрированное в соответствии с законодательством Республики Казахстан.

Пользователь: Физическое или юридическое лицо (далее -«Пользователь», «вы», «ваш»), использующее Экосистему Silence Environment.

Экосистема: Программная платформа Silence Environment, включающая компоненты Ollama + LLM, SLNC-Code и SitHub.

Персональные данные: Любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу.

---

1. ВВЕДЕНИЕ И ПРИНЦИПЫ

1.1 Цель настоящей Политики

Настоящая Политика конфиденциальности (далее -«Политика») описывает принципы и практики обработки данных при использовании Экосистемы Silence Environment. Политика является неотъемлемой частью Условий предоставления услуг и должна читаться совместно с ними.

1.2 Принцип «Конфиденциальность по замыслу» (Privacy by Design)

Экосистема построена на архитектурном принципе минимизации сбора данных. Конфиденциальность не является дополнительной функцией -это фундаментальная характеристика архитектуры системы.

1.3 Применимое законодательство

Настоящая Политика разработана с учётом:

- Закона Республики Казахстан «О персональных данных и их защите»
- Общего регламента по защите данных ЕС (GDPR) -для пользователей из Европейского Союза
- Других применимых норм о защите данных в юрисдикции Пользователя

1.4 Контроллер и процессор данных

Для персональных данных, обрабатываемых в связи с подпиской:

- **Контроллер данных (Data Controller):** Silence AI
- Мы определяем цели и средства обработки информации о подписке

Для данных, обрабатываемых в Экосистеме:

- **Контроллер данных:** Пользователь (вы контролируете свой код и данные разработки)
- **Процессор данных:** Неприменимо -мы не обрабатываем ваши данные разработки

---

2. АРХИТЕКТУРНЫЕ ГАРАНТИИ КОНФИДЕНЦИАЛЬНОСТИ

2.1 Основной принцип изоляции данных

Исходный код Пользователя обрабатывается исключительно на локальной инфраструктуре Пользователя. Архитектура Экосистемы спроектирована таким образом, чтобы предотвратить передачу исходного кода на серверы Провайдера.

2.2 Техническая реализация изоляции

Ollama + LLM:

- Работает полностью автономно
- Не содержит функций сетевой передачи данных
- Все вычисления производятся локально

SLNC-Code:

- Работает полностью автономно
- Не содержит функций передачи кода на внешние серверы
- Интегрируется только с локальной LLM

SitHub:

- Единственный компонент, осуществляющий связь с серверами Провайдера
- Передаёт только данные, указанные в разделе 3.2
- Модуль сканирования изолирован от сетевых функций

2.3 Что это означает на практике

Провайдер не имеет технической возможности получить доступ к:

- Исходному коду, хранящемуся в Экосистеме
- Результатам сканирования безопасности
- Истории коммитов и изменений кода
- Именам файлов и структуре проектов

Важное уточнение: Данная гарантия действует при условии правильной эксплуатации Экосистемы в соответствии с технической документацией и при отсутствии действий Пользователя по ручной передаче данных во внешние сервисы.

---

3. ИНФОРМАЦИЯ, КОТОРУЮ МЫ СОБИРАЕМ

3.1 Информация о подписке (обязательная)

Для предоставления услуг мы собираем следующую информацию:

Корпоративная информация:

- Название организации (для корпоративных подписок)
- Контактный email для связи
- Страна регистрации (для соблюдения применимых законов)

Информация о лицензии:

- Хеш лицензионного ключа (необратимое криптографическое преобразование)
- Дата активации подписки
- Дата истечения подписки
- Статус подписки (активна/неактивна/приостановлена)

Платёжная информация:

- Платёжные реквизиты обрабатываются сторонними платёжными процессорами
- Провайдер не хранит полные данные банковских карт
- Мы храним только информацию о типе платёжного метода и последних четырёх цифрах карты (для идентификации платежей)

Правовое основание (для пользователей из ЕС):

- Исполнение договора (GDPR, статья 6(1)(b))

3.2 Технические данные от SitHub (автоматические)

При проверке лицензии и запросе обновлений SitHub передаёт:

Данные аутентификации:

- Хеш лицензионного ключа
- Криптографический токен сессии (временный)

Технические метаданные:

- Временная метка запроса (дата и время в формате UTC)
- Версия установленного SitHub (например, "2.1.3")
- Хеш идентификатора установки (необратимое преобразование уникального ID)
- IP-адрес (автоматически записывается сервером, используется для предотвращения злоупотреблений)

Правовое основание:

- Законные интересы Провайдера в предотвращении мошенничества и обеспечении безопасности (GDPR, статья 6(1)(f))

Период хранения: 90 дней

3.3 Техническая телеметрия (опциональная)

Если вы явно согласитесь, мы можем собирать дополнительную техническую информацию для улучшения качества услуг:

Информация об использовании:

- Частота запросов обновлений
- Статистика загрузки обновлений безопасности
- Время последнего успешного обновления

Отчёты об ошибках:

- Трассировки стека (stack traces) без исходного кода
- Сообщения об ошибках
- Информация о системном окружении (ОС, версия, архитектура)
- Логи системных вызовов (без пользовательских данных)

Важно: Отчёты об ошибках проходят автоматическую фильтрацию для удаления любых фрагментов кода или конфиденциальных данных перед отправкой.

Правовое основание:

- Согласие (GDPR, статья 6(1)(a))
- Вы можете отозвать согласие в любое время в настройках SitHub

3.4 Информация, которую мы НЕ собираем

Мы явно **не собираем, не обрабатываем и не храним**:

Исходный код:

- Код в репозиториях
- Содержимое файлов
- Фрагменты кода

- Комментарии в коде

Результаты анализа:

- Результаты сканирования безопасности
- Обнаруженные уязвимости в вашем коде
- Отчёты о качестве кода

Метаданные разработки:

- Имена файлов и каталогов
- Структура проектов
- История коммитов
- Сообщения коммитов
- Информация о ветках

Информация о пользователях:

- Имена разработчиков
- Email-адреса разработчиков
- Структура команд
- Права доступа внутри организации

Учётные данные:

- Пароли
- API-ключи
- Токены доступа
- SSH-ключи
- Сертификаты

---

4. ЦЕЛИ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ

4.1 Управление подпиской

Цель: Предоставление доступа к Экосистеме и обновлениям

Обрабатываемые данные:

- Информация о подписке (раздел 3.1)
- Статус лицензии

Правовое основание:

- Исполнение договора (GDPR, статья 6(1)(b))
- Для РК: согласие на обработку персональных данных при заключении договора

Действия:

- Проверка активности лицензии
- Обработка продлений подписки
- Отправка уведомлений о статусе подписки
- Предоставление доступа к обновлениям безопасности

4.2 Доставка обновлений безопасности

Цель: Обеспечение актуальности баз данных уязвимостей

Обрабатываемые данные:

- Хеш лицензионного ключа
- Версия SitHub
- Временные метки запросов

Правовое основание:

- Исполнение договора (GDPR, статья 6(1)(b))

Действия:

- Аутентификация запросов обновлений
- Передача баз данных уязвимостей
- Передача патчей безопасности
- Мониторинг работоспособности службы обновлений

4.3 Улучшение качества услуг

Цель: Разработка и улучшение баз данных безопасности

Обрабатываемые данные:

- Техническая телеметрия (только если вы дали согласие)
- Анонимные отчёты об ошибках

Правовое основание:

- Согласие (GDPR, статья 6(1)(a))

Действия:

- Исследование новых угроз и уязвимостей
- Улучшение точности обнаружения уязвимостей
- Разработка новых сигнатур безопасности
- Устранение ошибок в компонентах Экосистемы

Источники информации: Результаты анализа угроз, проведенного подразделением Thret Hunters компании Silence AI. **НЕ** ваш код.

4.4 Соблюдение законодательства

Цель: Выполнение юридических обязательств

Обрабатываемые данные:

- Информация о подписке
- Платёжные записи

Правовое основание:

- Юридическое обязательство (GDPR, статья 6(1)(c))
- Для РК: требования налогового и бухгалтерского законодательства

Действия:

- Хранение платёжных записей (7 лет -требование налогового законодательства)
- Ответы на судебные запросы
- Предоставление информации регулирующим органам (только при наличии законного основания)
- Предотвращение мошенничества

4.5 Предотвращение злоупотреблений

Цель: Защита от мошенничества и нарушений Условий

Обрабатываемые данные:

- IP-адреса запросов
- Частота запросов обновлений
- Паттерны использования

Правовое основание:

- Законные интересы (GDPR, статья 6(1)(f))
- Наши законные интересы: предотвращение мошенничества, защита от злоупотреблений лицензиями

Действия:

- Выявление подозрительной активности
- Блокировка скомпрометированных лицензий
- Предотвращение несанкционированного распространения

---

5. ХРАНЕНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

5.1 Данные, хранимые Провайдером

На серверах Провайдера хранятся только:

Тип данных	Местонахождение	Шифрование	Срок хранения
Информация о подписке	Республика Казахстан	AES-256	Период действия + 1 год
Платёжные записи	Обработчик платежей	Соответствует PCI DSS	7 лет (требование закона)
Хеши лицензионных ключей	Республика Казахстан	Bcrypt	Период действия + 1 год
Журналы запросов	Республика Казахстан	TLS 1.3 при передаче	90 дней
Базы данных безопасности	Республика Казахстан (зеркала в ЕС)	Не требуется (публичная информация)	Постоянно (продукт)

5.2 Данные, хранимые на инфраструктуре Пользователя

Исключительно на вашей инфраструктуре:

- Весь исходный код
- Результаты сканирования безопасности
- История коммитов
- Метаданные репозиториев
- Информация о пользователях и правах доступа
- Загруженные базы данных уязвимостей

Ответственность: Пользователь самостоятельно обеспечивает хранение, резервное копирование и безопасность этих данных.

5.3 Меры технической безопасности

Провайдер применяет следующие меры для защиты данных, хранимых на наших серверах:

Шифрование:

- **В состоянии покоя:** AES-256 для баз данных с конфиденциальной информацией
- **При передаче:** TLS 1.3 (минимум TLS 1.2 не принимается)
- **Хеширование:** Bcrypt для лицензионных ключей (необратимое преобразование)

Контроль доступа:

- Многофакторная аутентификация для административного доступа
- Принцип минимальных привилегий для сотрудников
- Журналирование всех административных действий

- Регулярный аудит прав доступа

Сетевая безопасность:

- Межсетевые экраны на периметре
- Системы обнаружения вторжений (IDS/IPS)
- DDoS-защита
- Регулярное сканирование на уязвимости

Мониторинг и реагирование:

- 24/7 мониторинг безопасности
- Автоматические оповещения о подозрительной активности
- План реагирования на инциденты
- Регулярные учения по безопасности

5.4 Аудит безопасности

- Ежегодный независимый аудит безопасности сторонней фирмой
- Регулярное тестирование на проникновение
- Публикация сводных отчётов (без раскрытия уязвимостей)

5.5 Уведомление об инцидентах

В случае инцидента безопасности, затрагивающего ваши данные:

- **Уведомление Пользователей:** в течение 72 часов с момента обнаружения
- **Уведомление регуляторов (для пользователей из ЕС):** в течение 72 часов (требование GDPR)
- **Уведомление регуляторов РК:** в соответствии с законодательством о персональных данных

---

6. ПЕРЕДАЧА И РАСКРЫТИЕ ДАННЫХ

6.1 Внутреннее использование

Доступ к данным Пользователей имеют только сотрудники Провайдера, которым это необходимо для выполнения служебных обязанностей:

- Администраторы систем (для обслуживания инфраструктуры)
- Служба поддержки (для решения технических проблем)
- Бухгалтерия (для обработки платежей)

Все сотрудники подписывают соглашения о конфиденциальности.

6.2 Сторонние обработчики данных

Мы используем следующие категории сторонних обработчиков:

Платёжные процессоры:

- Для обработки платежей по подписке
- Соответствуют стандарту PCI DSS
- Примеры: Stripe, PayPal, Kaspi.kz (для клиентов из РК)
- Имеют собственные политики конфиденциальности

Хостинг-провайдеры:

- Для размещения серверов обновлений
- Местонахождение: Республика Казахстан (основные серверы), ЕС (зеркала для клиентов из ЕС)
- Работают в соответствии с соглашениями об обработке данных (DPA)

Службы мониторинга и безопасности:

- Для обеспечения работоспособности и безопасности инфраструктуры
- Доступ ограничен техническими метаданными (логи, метрики)
- Не имеют доступа к информации о подписках

Важно: Все сторонние обработчики:

- Подписывают соглашения об обработке данных (DPA)
- Соблюдают принцип минимизации доступа
- Не используют данные для собственных целей

6.3 Передачи в правоохранительные органы

Мы можем раскрывать информацию правоохранительным или регулирующим органам:

Когда это требуется:

- По судебному приказу
- По повестке в суд
- При наличии юридического обязательства в соответствии с применимым законодательством

Процедура:

- Проверка законности запроса юридическим отделом
- Предоставление только минимально необходимой информации
- Уведомление Пользователя (если это не запрещено судебным приказом)
- Документирование всех запросов для отчёта о прозрачности

Что НЕ может быть предоставлено:

- Исходный код (так как мы его не храним)
- Результаты сканирования (так как они хранятся локально у Пользователя)

6.4 Передачи при реорганизации бизнеса

В случае слияния, поглощения или продажи бизнеса:

- Информация о подписках может быть передана правопреемнику
- Пользователи будут уведомлены за 30 дней
- Правопреемник обязан соблюдать настоящую Политику
- У Пользователей будет возможность прекратить подписку с возвратом пропорциональной части оплаты

6.5 Что мы НИКОГДА не делаем

Провайдер **никогда** не будет:

- Продавать данные Пользователей третьим лицам
- Сдавать данные в аренду для маркетинговых целей
- Монетизировать данные помимо оплаты подписки
- Передавать данные брокерам данных
- Использовать данные для таргетированной рекламы

---

7. МЕЖДУНАРОДНЫЕ ПЕРЕДАЧИ ДАННЫХ

7.1 Местонахождение серверов

Основные серверы: Республика Казахстан

7.2 Передачи из ЕС в Казахстан (для пользователей из ЕС)

Правовое основание для передачи: Провайдер использует **Стандартные договорные оговорки (Standard Contractual Clauses, SCC)**, утверждённые Решением Европейской Комиссии 2021/914.

Дополнительные меры защиты:

- Шифрование данных при передаче (TLS 1.3)
- Шифрование данных в состоянии покоя (AES-256)
- Ограниченный доступ к данным
- Регулярный аудит безопасности

Доступ SCC:

- Стандартные договорные оговорки доступны для ознакомления по запросу
- Отправьте запрос на: info@silence.codes
- SCC автоматически включаются в Соглашение об обработке данных (DPA) для корпоративных клиентов из ЕС

7.3 Что передаётся международно

При использовании из-за пределов Казахстана передаются:

- Информация о подписке (для управления лицензией)
- Запросы на загрузку обновлений безопасности
- Базы данных безопасности (загружаются к вам)

Что НЕ передаётся:

- Исходный код (остаётся на вашей локальной инфраструктуре)
- Результаты сканирования (обрабатываются локально)
- Информация о разработчиках (управляется локально)

7.4 Локализация данных для клиентов из РК

Для клиентов, находящихся в Республике Казахстан, все данные хранятся на серверах в РК в соответствии с требованиями законодательства о локализации данных (если применимо).

---

8. ПРАВА СУБЪЕКТОВ ДАННЫХ

8.1 Применимость прав

Права, описанные в этом разделе, применяются:

- **Для всех Пользователей:** базовые права в соответствии с законодательством РК
- **Для Пользователей из ЕС:** расширенные права в соответствии с GDPR
- **Для Пользователей из других юрисдикций:** права в соответствии с применимым законодательством

8.2 Право на доступ (GDPR, статья 15)

Вы имеете право получить:

- Подтверждение, обрабатываем ли мы ваши персональные данные
- Копию ваших персональных данных
- Информацию о целях обработки, категориях данных, получателях
- Срок хранения данных
- Информацию о ваших правах

Как реализовать:

- Отправьте запрос на: info@silence.codes
- Мы ответим в течение 30 дней (GDPR) или 15 дней (законодательство РК)

- Предоставим данные в структурированном, общеупотребительном формате (JSON или PDF)

8.3 Право на исправление (GDPR, статья 16)

Вы имеете право исправить неточные персональные данные:

- Исправление контактной информации
- Обновление названия организации
- Корректировка платёжных реквизитов

Как реализовать:

- Войдите в личный кабинет и обновите информацию
- Или отправьте запрос на: info@silence.codes

8.4 Право на удаление / «Право быть забытым» (GDPR, статья 17)

Вы имеете право запросить удаление ваших персональных данных в следующих случаях:

- Данные больше не нужны для целей обработки
- Вы отзываете согласие (для обработки на основе согласия)
- Данные обрабатывались незаконно
- Удаление требуется для соблюдения юридического обязательства

Ограничения:

- Мы не можем удалить данные, если их хранение требуется законом (например, платёжные записи -7 лет)
- Мы не можем удалить данные, необходимые для исполнения договора (пока подписка активна)

Как реализовать:

- Отправьте запрос на: info@silence.codes
- Мы удалим данные в течение 30 дней (за исключением данных с законодательными требованиями хранения)

8.5 Право на ограничение обработки (GDPR, статья 18)

Вы можете запросить ограничение обработки ваших данных:

- Пока проверяется точность данных (по вашему запросу)
- Если обработка незаконна, но вы не хотите удаления
- Если данные нужны вам для юридических целей

Как реализовать:

- Отправьте запрос на: info@silence.codes с указанием причины

8.6 Право на переносимость данных (GDPR, статья 20)

Вы имеете право получить свои данные в структурированном, машиночитаемом формате:

- Данные, которые вы предоставили нам
- Обработка которых основана на согласии или договоре
- Обработка которых осуществляется автоматизированными средствами

Форматы: JSON, CSV, XML

Как реализовать:

- Отправьте запрос на: info@silence.codes
- Укажите предпочтительный формат

8.7 Право на возражение (GDPR, статья 21)

Вы имеете право возразить против обработки, основанной на законных интересах:

- Например, против обработки для предотвращения мошенничества

Мы прекратим обработку, если не сможем продемонстрировать преобладающие законные основания.

Как реализовать:

- Отправьте запрос на: info@silence.codes с указанием причины возражения

8.8 Право на отзыв согласия (GDPR, статья 7(3))

Если обработка основана на согласии, вы можете отозвать согласие в любое время:

- Например, для технической телеметрии

Отзыв не влияет на законность обработки до отзыва.

Как реализовать:

- В настройках SitHub: отключите опцию "Отправка телеметрии"
- Или отправьте запрос на: info@silence.codes

8.9 Право на жалобу в надзорный орган

Для пользователей из ЕС: Вы имеете право подать жалобу в надзорный орган по защите данных вашей страны.

Для пользователей из РК: Вы можете обратиться в уполномоченный орган по защите прав субъектов персональных данных Республики Казахстан.

8.10 Сроки ответа на запросы

Тип запроса	Срок ответа (GDPR)	Срок ответа (РК)
Доступ к данным	30 дней	15 дней
Исправление	30 дней	15 дней
Удаление	30 дней	15 дней
Другие запросы	30 дней	15 дней

Сроки могут быть продлены на 2 месяца (GDPR) при сложных запросах с обязательным уведомлением.

---

9. ФАЙЛЫ COOKIE И ТЕХНОЛОГИИ ОТСЛЕЖИВАНИЯ

9.1 Использование cookies

Провайдер использует минимальное количество cookies:

Строго необходимые cookies (не требуют согласия):

- Сессионный cookie для аутентификации в личном кабинете
- Cookie для сохранения языковых предпочтений
- Cookie для безопасности (CSRF-токены)

Срок действия: до конца сессии или 30 дней

Аналитические cookies (требуют согласия):

- Если включено: базовая аналитика использования веб-сайта (не SitHub)
- Используем собственное решение (не Google Analytics)
- Данные анонимизированы

9.2 Управление cookies

Вы можете:

- Отклонить необязательные cookies при первом посещении сайта
- Изменить настройки в любое время в настройках браузера
- Удалить существующие cookies через настройки браузера

9.3 Отсутствие отслеживания

Мы **НЕ используем:**

- Трекеры социальных сетей
- Рекламные трекеры
- Трекеры третьих сторон для профилирования

- Системы межсайтового отслеживания

---

10. ХРАНЕНИЕ ДАННЫХ

10.1 Сроки хранения

Тип данных	Срок хранения	Правовое основание
Информация о подписке	Период действия + 1 год	Возможные споры, возвраты
Платёжные записи	7 лет после транзакции	Налоговое законодательство РК, ЕС
Хеши лицензионных ключей	Период действия + 1 год	Предотвращение злоупотреблений
Журналы запросов обновлений	90 дней	Техническая поддержка, безопасность
Техническая телеметрия	1 год	Улучшение услуг
Отчёты об ошибках	2 года	Устранение ошибок

10.2 Удаление после истечения сроков

По истечении срока хранения:

1. Данные автоматически помечаются для удаления
2. Безвозвратное удаление происходит в течение 30 дней
3. Резервные копии перезаписываются в течение 90 дней
4. Логи удаления сохраняются для аудита

10.3 Досрочное удаление

Вы можете запросить досрочное удаление данных (кроме данных с законодательными требованиями хранения):

- Отправьте запрос на: info@silence.codes
- Укажите, какие данные вы хотите удалить
- Мы выполним запрос в течение 30 дней

---

11. КОНФИДЕНЦИАЛЬНОСТЬ ДЕТЕЙ

11.1 Возрастные ограничения

Экосистема не предназначена для использования лицами младше 18 лет:

- Это профессиональный инструмент разработки
- Это корпоративное программное обеспечение

- Мы не собираем сознательно данные от лиц младше 18 лет

11.2 Исключение: использование с согласия родителей

Лица в возрасте 16-18 лет могут использовать Экосистему с письменного согласия родителя или законного опекуна.

11.3 Обнаружение и удаление данных несовершеннолетних

Если мы обнаружим, что собрали данные от лица младше 16 лет:

- Мы немедленно удалим всю информацию
- Мы деактивируем учётную запись
- Мы уведомим контактное лицо (если доступно)

Для родителей: Если вы обнаружили, что ваш ребенок использует Экосистему без вашего согласия:

- Свяжитесь с нами: info@silence.codes
- Мы закроем учётную запись и удалим данные в течение 48 часов

---

12. ВАШИ ОБЯЗАННОСТИ ПО ЗАЩИТЕ ДАННЫХ

12.1 Обязанности Пользователя

Провайдер обеспечивает конфиденциальность на уровне архитектуры. Вы несёте ответственность за:

Безопасность инфраструктуры:

- Надлежащую конфигурацию межсетевых экранов
- Контроль доступа к серверам, на которых развёрнута Экосистема
- Регулярное обновление операционных систем
- Физическую безопасность оборудования

Предотвращение ручной передачи данных:

- Не загружайте код вручную во внешние облачные сервисы
- Не копируйте репозитории в публично доступные сервисы (GitHub, GitLab и т.д.)
- Обучайте разработчиков принципам безопасной работы

Управление пользователями:

- Контролируйте, кто имеет доступ к Экосистеме
- Используйте надёжные пароли и многофакторную аутентификацию
- Своевременно отзывайте доступ уволенных сотрудников

- Применяйте принцип минимальных привилегий

12.2 Ограничение ответственности Провайдера

Провайдер **не несёт ответственности** за утечки данных, вызванные:

- Действиями Пользователя или его сотрудников
- Компрометацией инфраструктуры Пользователя
- Неправильной конфигурацией безопасности на стороне Пользователя
- Вредоносным ПО на оборудовании Пользователя

12.3 Обработка персональных данных разработчиков

Если вы используете Экосистему для управления командой разработчиков:

- **Вы** являетесь контроллером данных ваших сотрудников
- Вы обязаны соблюдать применимое законодательство о защите данных
- Вы обязаны информировать сотрудников об обработке их данных
- Провайдер не имеет доступа к этим данным и не несёт ответственности за их обработку

---

13. ОТЧЁТ О ПРОЗРАЧНОСТИ

13.1 Обязательство по прозрачности

Провайдер привержен прозрачности в отношении:

- Запросов правоохранительных органов
- Инцидентов безопасности
- Изменений в практиках обработки данных

13.2 Уведомление об инцидентах безопасности

В случае нарушения безопасности данных:

- **Уведомление Пользователей:** в течение 72 часов с момента обнаружения
- **Содержание уведомления:**
  - Описание инцидента
  - Категории и количество затронутых данных
  - Возможные последствия
  - Принятые меры по устранению
  - Рекомендации для Пользователей
- **Способ уведомления:** email + уведомление в интерфейсе SitHub

13.3 Раскрытие запросов правоохранительных органов

Провайдер будет уведомлять Пользователей о запросах правоохранительных органов:

- За исключением случаев, когда уведомление запрещено судебным приказом
- С указанием характера запроса (без раскрытия деталей расследования)
- С предоставлением копии запроса (если это разрешено)

---

14. СОГЛАШЕНИЕ ОБ ОБРАБОТКЕ ДАННЫХ (DPA) ДЛЯ КОРПОРАТИВНЫХ КЛИЕНТОВ ИЗ ЕС

14.1 Применимость DPA

Для корпоративных клиентов из Европейского Союза, которые используют Экосистему для обработки персональных данных своих сотрудников, Провайдер предоставляет Соглашение об обработке данных (Data Processing Agreement, DPA).

14.2 Содержание DPA

DPA включает:

- Стандартные договорные оговорки (SCC) ЕС
- Описание предмета и срока обработки
- Характер и цели обработки
- Типы персональных данных
- Категории субъектов данных
- Обязанности и права контроллера и процессора

14.3 Запрос DPA

Чтобы запросить DPA:

- Отправьте запрос на: info@silence.codes
- Укажите название вашей организации и контактную информацию
- DPA будет предоставлен в течение 5 рабочих дней

14.4 Субпроцессоры

Список субпроцессоров (хостинг-провайдеры, платёжные системы) указывается в DPA. Пользователи будут уведомлены за 30 дней о добавлении новых субпроцессоров.

---

15. ИЗМЕНЕНИЯ В ПОЛИТИКЕ КОНФИДЕНЦИАЛЬНОСТИ

15.1 Право на изменение

Провайдер оставляет за собой право изменять настоящую Политику по следующим причинам:

- Изменения в применимом законодательстве
- Развитие функциональности Экосистемы
- Улучшение защиты прав Пользователей
- Изменения в практиках обработки данных

15.2 Уведомление об изменениях

Несущественные изменения (исправление опечаток, уточнение формулировок):

- Публикуются на веб-сайте с указанием новой даты вступления в силу

Существенные изменения (влияющие на права или изменяющие практики обработки):

- Email-уведомление за 30 дней до вступления в силу
- Уведомление в интерфейсе SitHub
- Публикация на веб-сайте с выделением изменений

15.3 Согласие с изменениями

Продолжая использовать Экосистему после вступления изменений в силу, вы подтверждаете согласие с обновлённой Политикой.

Если вы не согласны с изменениями:

- Вы имеете право прекратить использование Экосистемы
- При отмене в течение 14 дней после уведомления о существенных изменениях -пропорциональный возврат средств

---

16. КОНТАКТНАЯ ИНФОРМАЦИЯ

Вопросы о конфиденциальности? Вопросы по данной политике? Вопросы о том, какие данные мы храним?

Свяжитесь с нами:
Email: info@silence.codes

Настоящая Политика конфиденциальности разработана для обеспечения прозрачности наших практик обработки данных и защиты ваших прав. Экосистема Silence Environment построена на принципе минимизации сбора данных: мы собираем только информацию, необходимую для предоставления услуг, и никогда не получаем доступ к вашему исходному коду.