Розумний рушій CB HACCP: Політика інформаційної безпеки та суверенітету даних Версія: 1.5.0
Видавець: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «КОНСАЛТИНГ ЮА-РО»

1. Ізоляція та суверенітет даних ТОВ «КОНСАЛТИНГ ЮА-РО» гарантує суворий захист ваших пропрієтарних блок-схем процесів, рецептур та матриць аналізу небезпек. Для користувачів Автономної корпоративної ліцензії (Standalone Enterprise License) середовище бази даних є повністю розділеним. Ваші дані ніколи не залишають вашу корпоративну інфраструктуру і не використовуються для навчання глобальних моделей штучного інтелекту.

2. Стандарти шифрування Усі дані, що передаються між вашими локальними комп'ютерами та сервером haccp.consulting-ua.eu, захищені за допомогою галузевого стандарту шифрування TLS 1.3. Резервні копії баз даних, що створюються за розкладом, шифруються у стані спокою за стандартом AES-256 для запобігання несанкціонованому доступу у разі компрометації обладнання.

3. Незмінні контрольні журнали (Відповідність FSSC 22000) Для відповідності суворим міжнародним стандартам сертифікації, рушій CB HACCP використовує незмінну систему CAPA замкнутого циклу. Після фіксації порушення Критичної контрольної точки (ККТ), подальша коригувальна дія назавжди позначається ідентифікатором користувача та часовою міткою. Записи не можуть бути змінені заднім числом або видалені звичайними користувачами, що забезпечує повний юридичний захист під час зовнішніх аудитів.

Нормативно-правова відповідність (ЄС та Україна):

Загальний регламент ЄС про захист даних (GDPR): Відповідно до GDPR, Клієнт діє як єдиний Контролер даних (і Обробник даних, якщо використовується власний хостинг). ТОВ «КОНСАЛТИНГ ЮА-РО» виступає виключно як постачальник програмного забезпечення. Ми не здійснюємо моніторинг, аудит або управління особистими чи корпоративними даними, які ви вводите в систему.

Законодавство України: Відповідно до Закону України «Про захист персональних даних», Клієнт є «Володільцем бази персональних даних». Клієнт несе абсолютну законодавчу відповідальність за отримання згоди від своїх кінцевих клієнтів та забезпечення точності зареєстрованих даних.

4. ПОЛОЖЕННЯ ПРО НУЛЬОВУ ВІДПОВІДАЛЬНІСТЬ ТА ПРИЙНЯТТЯ РИЗИКІВ Щоб захистити цілісність програмного забезпечення та встановити чіткі операційні межі, ТОВ «КОНСАЛТИНГ ЮА-РО» діє згідно з політикою Суворої нульової відповідальності (Strict Zero Liability) щодо втрати даних, пошкодження даних або юридичних суперечок, що виникають через помилки користувача.

4.1. Суперечки з кінцевими клієнтами та ланцюг відповідальності Кінцеві клієнти Клієнта отримуватимуть сертифікати, згенеровані цим Додатком. Якщо кінцевий клієнт стикається з юридичними, фінансовими чи акредитаційними проблемами через

неправильно виданий, помилково призупинений або неналежним чином зареєстрований сертифікат, абсолютна юридична відповідальність лежить на Клієнті (Органі з сертифікації). ТОВ «КОНСАЛТИНГ ЮА-РО» прямо відмовляється від будь-якої відповідальності за претензії третіх осіб, втрату акредитації або фінансові збитки, що виникли внаслідок використання або неналежного використання Клієнтом згенерованих документів.

4.2. Анулювання відповідальності постачальника (Катастрофічна помилка користувача) ТОВ «КОНСАЛТИНГ ЮА-РО» не несе ЖОДНОЇ ВІДПОВІДАЛЬНОСТІ за будь-які катастрофічні події, включаючи, але не обмежуючись цим, видалення баз даних, очищення таблиць, пошкодження послідовностей сертифікатів або збої синхронізації IAF CERTSEARCH API, якщо Клієнт або його персонал:

Не читає документацію: Виконує дії без попереднього ознайомлення з офіційними Посібниками користувача, Короткими інструкціями (Quick Start Manuals) та Довідниками API.

Ігнорує відеоуроки: Оминає обов'язкові навчальні матеріали, надані на сайті consulting-ua.eu.

Порушує протоколи підтримки: Здійснює спроби модифікації бази даних з високим ступенем ризику (наприклад, виконання необроблених SQL-запитів, ручне видалення кореневих тек додатку або примусове скидання системи) без попередньої реєстрації офіційного запиту в службу підтримки на сайті

https://support.consulting-ua.eu

, звернення в онлайн-чат або електронного листа до служби підтримки.

Нехтує резервним копіюванням: Не створює щоденні SQL-дампи та щотижневі резервні копії файлової системи, як це вимагається Планом відновлення після катастроф (Disaster Recovery Plan).

5. ОБОВ'ЯЗКОВІ ПРОТОКОЛИ БЕЗПЕКИ ДЛЯ КЛІЄНТА Для забезпечення відповідності принципам ISO 27001 та місцевому законодавству, Клієнт повинен дотримуватися наступних технічних протоколів:

Керування доступом на основі ролей (RBAC): Привілеї Super-Admin повинні надаватися виключно уповноваженому IT-персоналу. Аудиторам та Технічним експертам повинні надаватися лише ті специфічні дозволи, які необхідні для їхніх ролей, через інтерфейс

admin/staff.php

.

Безпека інфраструктури: У разі використання власного хостингу, Клієнт повинен захистити серверне середовище, використовуючи галузеві стандарти брандмауерів, fail2ban (або аналогічні системи запобігання вторгненням), ModSecurity (WAF), а також забезпечити шифрування SSL/TLS для всього вебтрафіку.

Перевірка сканером ШІ: Модуль штучного інтелекту є допоміжним інструментом. Персонал Клієнта юридично зобов'язаний візуально перевіряти всі дані, витягнуті за допомогою ШІ, звіряючи їх з офіційними державними реєстрами перед збереженням профілю клієнта.

6. РЕАГУВАННЯ НА ІНЦИДЕНТИ ТА ЕСКАЛАЦІЯ ПІДТРИМКИ Перш ніж вживати будь-яких дій, які можуть змінити структурну цілісність бази даних (наприклад, видалення великого масиву заявок, зміна кореневих налаштувань або модифікація основних PHP-файлів), Клієнт ЗОБОВ'ЯЗАНИЙ:

Зупинити операції.

Відкрити пріоритетний запит (Priority Ticket) на сайті

https://support.consulting-ua.eu

.

Дочекатися задокументованого дозволу від інженерів ТОВ «КОНСАЛТИНГ ЮА-РО».

Недотримання цього шляху ескалації повністю звільняє постачальника від будь-якої відповідальності за подальший час простою або втрату даних.