Політика інформаційної безпеки: CB Automation

Версія: 1.5.0

Видавець: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «КОНСАЛТИНГ УА-РО»

1. МЕТА, СФЕРА ЗАСТОСУВАННЯ ТА ПРАВОВА БАЗА

Ця Політика інформаційної безпеки встановлює обов'язковий базовий рівень безпеки, протоколи обробки даних та суворі межі відповідальності для Органів з сертифікації («Клієнт»), що використовують додаток CB Automation.

Розгортаючи та експлуатуючи це програмне забезпечення, Клієнт визнає, що CB Automation є корпоративною системою комплаєнсу, розробленою для обробки даних виключно відповідно до інформації, введеної Клієнтом та його уповноваженим персоналом.

Відповідність нормативним вимогам (ЄС та Україна):

Загальний регламент захисту даних ЄС (GDPR):

Відповідно до GDPR, Клієнт діє як єдиний

Контролер даних

(та Обробник даних, якщо використовує власний хостинг). ТОВ «КОНСАЛТИНГ УА-РО» виступає виключно як постачальник програмного забезпечення. Ми не відстежуємо, не перевіряємо та не керуємо особистими або 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 повну законодавчу відповідальність за отримання згоди від своїх кінцевих споживачів та забезпечення точності зареєстрованих даних.

2. ЗАСТЕРЕЖЕННЯ ПРО НУЛЬОВУ ВІДПОВІДАЛЬНІСТЬ ТА ПРИЙНЯТТЯ РИЗИКІВ

Для захисту цілісності програмного забезпечення та встановлення чітких операційних меж, ТОВ «КОНСАЛТИНГ УА-РО» діє за політикою **Суворої Нульової Відповідальності** щодо втрати даних, їх пошкодження або юридичних спорів, що виникають через помилки користувача.

2.1. Спори з кінцевими споживачами та ланцюг відповідальності

Кінцеві споживачі Клієнта отримуватимуть сертифікати, згенеровані цим Додатком. Якщо кінцевий споживач стикається з юридичними, фінансовими або акредитаційними проблемами через неправильно виданий, помилково призупинений або неналежним чином зареєстрований (у базі IAF) сертифікат, абсолютна юридична відповідальність лежить на Клієнті (Органі з сертифікації). ТОВ «КОНСАЛТИНГ УА-РО» прямо відмовляється від будь-якої відповідальності за претензії третіх осіб, втрату акредитації або фінансові збитки, що виникли внаслідок використання або неправильного використання згенерованих документів Клієнтом.

2.2. Анулювання відповідальності постачальника (Катастрофічна помилка користувача)

ТОВ «КОНСАЛТИНГ УА-РО» бере на себе **НУЛЬОВУ ВІДПОВІДАЛЬНІСТЬ** за будь-які катастрофічні події, включаючи, але не обмежуючись, очищення баз даних, видалення таблиць, пошкодження послідовності сертифікатів або збої синхронізації API IAF CERTSEARCH, якщо Клієнт або його персонал:

Не читає документацію:

Виконує дії без попереднього ознайомлення з офіційними Посібниками користувача, Інструкціями зі швидкого старту та Довідниками з API.

Ігнорує відеоуроки:

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

Оминає протоколи підтримки:

Намагається внести високоризиковані модифікації в базу даних (наприклад, виконання прямих SQL-запитів, ручне видалення кореневих папок додатка або примусове скидання системи)

без

попередньої реєстрації офіційного запиту в службу підтримки на https://support.consulting-ua.eu, звернення в онлайн-чат або написання листа на електронну пошту підтримки.

Нехтує резервним копіюванням:

Не створює щоденні SQL-дампи та щотижневі резервні копії файлової системи, як того вимагає План відновлення після катастроф.

3. ОБОВ'ЯЗКОВІ ПРОТОКОЛИ БЕЗПЕКИ ДЛЯ КЛІЄНТА

Для забезпечення відповідності принципам ISO 27001 та місцевому законодавству, Клієнт повинен дотримуватися наступних технічних протоколів:

Управління доступом на основі ролей (RBAC):

Привілеї Супер-Адміністратора повинні надаватися лише уповноваженому IT-персоналу. Аудиторам та технічним експертам слід надавати лише ті дозволи, які необхідні для виконання їхніх обов'язків, через інтерфейс admin/staff.php.

Безпека інфраструктури:

У разі використання власного хостингу Клієнт зобов'язаний захистити серверне середовище за допомогою стандартних міжмережевих екранів, fail2ban (або аналогічних систем запобігання вторгненням), ModSecurity (WAF), а також забезпечити шифрування SSL/TLS для всього веб-трафіку.

Перевірка даних AI-сканера:

Модуль Google Cloud Vision AI є допоміжним інструментом. Персонал Клієнта юридично зобов'язаний візуально перевіряти всі вилучені штучним інтелектом дані (коди ЄДРПОУ, юридичні адреси) з офіційними державними реєстрами перед збереженням профілю клієнта.

4. РЕАГУВАННЯ НА ІНЦИДЕНТИ ТА ЕСКАЛАЦІЯ ДО ПІДТРИМКИ

Перш ніж вчиняти будь-які дії, які можуть змінити структурну цілісність бази даних (наприклад, видалення великого масиву заявок, зміна кореневих налаштувань або модифікація основних PHP-файлів), Клієнт ПОВИНЕН:

Зупинити операції.

Відкрити Пріоритетний тікет на

https://support.consulting-ua.eu

Дочекатися задокументованого дозволу від інженерів ТОВ «КОНСАЛТИНГ УА-РО». Невиконання цього алгоритму ескалації повністю звільняє постачальника від будь-якої відповідальності за подальший простій або втрату даних.