

# **Information Security Policy: CB Automation**

**Version:** 1.5.0

**Publisher:** CONSULTING UA-RO LIMITED LIABILITY COMPANY

## **1. PURPOSE, SCOPE & LEGAL FRAMEWORK**

This Information Security Policy establishes the mandatory security baseline, data handling protocols, and strict liability boundaries for Certification Bodies (the "Client") utilizing the CB Automation App.

By deploying and operating this software, the Client acknowledges that CB Automation is an enterprise compliance engine designed to process data strictly according to the inputs provided by the Client and their authorized staff.

### **Regulatory Alignment (EU & Ukraine):**

#### **EU General Data Protection Regulation (GDPR):**

Under GDPR, the Client acts as the sole

#### **Data Controller**

(and Data Processor, if self-hosting). CONSULTING UA-RO LLC acts exclusively as the software vendor. We do not monitor, audit, or govern the personal or corporate data you input into the system.

#### **Ukrainian Legislation:**

In accordance with the Law of Ukraine "On Personal Data Protection" (Закон України «Про захист персональних даних»), the Client is the "Owner of the personal data base" (Володілець бази персональних даних). The Client bears absolute statutory responsibility for obtaining consent from their end-customers and ensuring the accuracy of the registered data.

## **2. ZERO LIABILITY CLAUSE & ASSUMPTION OF RISK**

To protect the integrity of the software and establish clear operational boundaries, CONSULTING UA-RO LLC operates under a **Strict Zero Liability** policy regarding data loss, data corruption, or legal disputes arising from user error.

### **2.1. End-Customer Disputes and Chain of Blame**

The Client's end-customers will receive certificates generated by this App. If an end-customer faces legal, financial, or accreditation issues due to an incorrectly issued,

mistakenly suspended, or improperly reported certificate, the absolute legal liability rests with the Client (the Certification Body). CONSULTING UA-RO LLC explicitly disclaims any liability for third-party claims, loss of accreditation, or financial damages resulting from the Client's use or misuse of the generated documents.

## **2.2. Voiding of Vendor Responsibility (Catastrophic User Error)**

CONSULTING UA-RO LLC assumes **ZERO LIABILITY** for any catastrophic events, including but not limited to wiped databases, emptied tables, corrupted certificate sequences, or IAF CERTSEARCH API synchronization failures, if the Client or their staff:

### **Fails to Read Documentation:**

Executes actions without first consulting the official User Guides, Quick Start Manuals, and API References.

### **Ignores Video Tutorials:**

Bypasses mandatory training materials provided at consulting-ua.eu.

### **Bypasses Support Protocols:**

Attempts high-risk database modifications (e.g., executing raw SQL queries, manually deleting root application folders, or forcing system resets)

*without*

first registering a formal support ticket at <https://support.consulting-ua.eu>, engaging the live chat, or emailing support.

### **Neglects Backups:**

Fails to maintain daily SQL dumps and weekly file system backups as mandated by the Disaster Recovery Plan.

## **3. MANDATORY SECURITY PROTOCOLS FOR THE CLIENT**

To ensure compliance with ISO 27001 principles and local laws, the Client must enforce the following technical protocols:

### **Role-Based Access Control (RBAC):**

Super-Admin privileges must be restricted to authorized IT personnel only. Auditors and Technical Experts must only be granted the specific permissions required for their roles via the admin/staff.php interface.

### **Infrastructure Security:**

If self-hosted, the Client must secure the server environment using industry-standard firewalls, fail2ban (or similar intrusion prevention), ModSecurity (WAF), and enforce SSL/TLS encryption for all web traffic.

### **AI Scanner Verification:**

The Google Cloud Vision AI module is an assistive tool. The Client's staff is legally mandated to visually verify all AI-extracted data (EDRPOU codes, legal addresses) against official state registries before saving the client profile.

## **4. INCIDENT RESPONSE & SUPPORT ESCALATION**

Before taking any action that could alter the structural integrity of the database (e.g., deleting a massive batch of applications, altering root settings, or modifying the core PHP files), the Client MUST:

Halt operations.

Open a Priority Ticket at

<https://support.consulting-ua.eu>

Wait for documented clearance from CONSULTING UA-RO LLC engineers. Failure to follow this escalation path fully absolves the vendor of any responsibility for the resulting downtime or data loss.