CB HACCP Smart Engine: Information Security & Data Sovereignty Policy

Version: 1.5.0

Publisher: CONSULTING UA-RO LIMITED LIABILITY COMPANY

1. Data Isolation & Sovereignty Consulting UA-RO LLC ensures that your proprietary process flow diagrams, recipes, and Hazard Analysis matrices are strictly protected. For users of the **Standalone Enterprise License**, the database environment is completely partitioned. Your data never leaves your corporate infrastructure and is never used to train global AI models.

2. Encryption Standards All data in transit between your local machines and the haccp.consulting-ua.eu server is secured using industry-standard TLS 1.3 encryption. Scheduled database backups are encrypted at rest using AES-256 standards to prevent unauthorized access in the event of hardware compromise.

3. Immutable Audit Trails (FSSC 22000 Compliance) To meet strict international certification standards, the CB HACCP Engine employs an immutable Closed-Loop CAPA system. Once a Critical Control Point (CCP) breach is recorded, the ensuing corrective action is permanently stamped with the user's ID and timestamp. Records cannot be retroactively altered or deleted by standard users, ensuring total legal defensibility during external audits.

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.

4. 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.

4.1. 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.

4.2. 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.

5. 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 AI module is an assistive tool. The Client's staff is legally mandated to visually verify all AI-extracted data 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.