**Security Addendum**

DE software & control takes security of its information system very seriously. Therefore DE software & control has implemented several security measures and will maintain them during the term of the subscription schedule at least with the following minimum standards.

**1. Infrastructure and Encapsulation**

1.1 DE software & control will ensure the application executes within a fully encapsulated and isolated container environment. This architecture will follow container isolation principles. DE software & control will implement process isolation and namespace separation to prevent unauthorized lateral movement within the infrastructure.

1.3 DE software & control will conduct regular integrity checks of the container images to protect against Malicious Code. DE software & control will remediate any deviations from the authorized baseline at no cost to Customer.

**2. Geographic Data Residency and AI Processing**

2.1 DE software & control warrants that all data processing, including the inference and execution of models by LLM Providers, takes place only on physical servers located within the European Economic Area (EEA).

2.2 DE software & control will not redirect data traffic or processing to any location outside the EEA without Customer's prior written consent.

2.3 DE software & control will use dedicated Enterprise API endpoints for all model interactions with LLM Providers. DE software & control will verify that these endpoints follow European data residency for transit and processing.

2.4 DE software & control will maintain a current list of all AI sub-processors and their server locations as described in the list of sub-processors.

**3. AI Data Policy and Minimization**

3.1 DE software & control will contractually ensure that LLM providers do not use Customer Content to train, improve, or fine-tune their models.

3.2 DE software & control will implement automated data minimization using "Edge Processing." DE software & control will pre-process large files locally before any external API transmission. DE software & control will use industry-standard libraries to extract data locally, e.g.:

- ffmpeg to extract specific frames from video files; and
- poppler to extract text snippets from documents.

3.3 DE software & control will transmit only relevant data fragments to LLM Provider's APIs.

3.4 DE software & control will encrypt all data in transit between the environment and LLM Provider's API endpoints using Transport Layer Security (TLS) 1.3 or higher.

**4. Multi-Tenancy and Access Control**

4.1 DE software & control will implement a multi-tenancy architecture where each Customer is assigned a unique, immutable tenantId. DE software & control will ensure logical data separation. Database queries must be scoped by the tenantId to prevent cross-tenant data leakage.

4.3 DE software & control will provide a Role-Based Access Control (RBAC) system supporting at least “Admin”, “Editor”, and “Viewer” roles. DE software & control will enforce the principle of least privilege (PoLP) across all application layers.

4.4 DE software & control will provide a "Delete Organization" feature. This allows the "Admin" to trigger the complete and irreversible erasure of all tenant data at any time.

**5. Vulnerability Management and Security**

5.1 DE software & control will follow a vulnerability management program, including automated scans of images and the application stack at least weekly.

5.2 If the DE software & control identifies Vulnerabilities, the DE software & control will remediate them within these timeframes:

- Critical (CVSS 9.0-10.0): Within 48 business hours.
- High (CVSS 7.0-8.9): Within 7 business days.
- Medium/Low: Within the next regular patch cycle, not to exceed 30 days.

**6. Audit Rights and Compliance**

Customer’s right to audit DE software & control’s compliance with the technical and organizational measures and the security standards set forth in this Security Addendum shall be governed exclusively by, and is subject to, the audit procedures and conditions stipulated in Section 3 (Audit) of the Data Processing Agreement (DPA) entered into between the Parties.