ANNEX III TO THE DPA - TECHNICAL AND ORGANIZATIONAL MEASURES
AIKIT RESEARCH, S.A.

Last updated: April 2026

This Annex III forms an inseparable part of the Data Processing Agreement (DPA) entered into between the Client (Controller) and AIKIT RESEARCH, S.A. (Processor) and describes the technical and organizational measures adopted by AIKIT RESEARCH, S.A. to ensure a level of security appropriate to the risk of the processing, in accordance with Article 32 of Regulation (EU) 2016/679 (GDPR).

1. CONFIDENTIALITY

1.1. Physical access control

The data centers hosting the Client's information are operated by certified cloud providers with physical access controls, 24/7 surveillance and visitor logging. AIKIT RESEARCH, S.A. does not host the Client's information on its own premises.

1.2. Logical access control

- Strong user authentication through individual credentials and multi-factor authentication (MFA) on accounts with access to systems that process the Client's information.
- Password complexity and rotation policies.
- Automatic session lock-out after a period of inactivity.
- Encryption of corporate devices (endpoints) on which the Client's information is stored.
- Administrative access under Zero-Trust principles.

1.3. Authorization control

- Role-based access control (RBAC) model applying the principle of least privilege.
- Periodic review (at least annually) of access rights.
- Logging of access to systems that process the Client's information.
- Immediate revocation of access upon termination of the employment or contractual relationship of authorized personnel.

1.4. Segregation (multi-tenant)

The platform is designed with logical segregation of data between clients. Each Client's information is isolated by means of unique identifiers and access controls at the application and storage layers.

1.5. Environment segregation

The development, pre-production and production environments are segregated. The Client's data is processed exclusively in the production environment.

1.6. Encryption

- Encryption in transit: TLS 1.3 in all communications between the Client and the platform, as well as between the internal components of the service.
- Encryption at rest: AES-256 or equivalent for the Client's data stored on a persistent basis, including backups.
- Centralized management of keys and secrets with a rotation

policy.

2. INTEGRITY

2.1. Transfer control

- Encrypted communications via HTTPS/TLS.
- Web Application Firewall (WAF) against malicious traffic.
- Filtering and threat protection for corporate email.
- EDR/Antivirus solutions on corporate endpoints.

2.2. Input control

- Activity logging (audit trail) with a unique user identifier for relevant actions on the Client's data.
- Timestamping and retention of logs for the period necessary for security and compliance purposes.

2.3. Secure development

- Secure Software Development Lifecycle (SDLC) practices.
- Peer code review prior to deployment to production.
- Automated analysis of dependencies and vulnerabilities within the continuous integration pipeline.
- Versioned infrastructure as code (IaC).
- Automated testing.

3. AVAILABILITY AND RESILIENCE

3.1. Hosting and architecture

- Certified cloud infrastructure (Microsoft Azure and providers in accordance with Annex II) with geographic redundancy within the EEA in the standard deployment.
- Continuous monitoring and automatic alerts for availability and performance.
- Protection against denial of service (CDN + bot management).

3.2. Recovery

- Automated backups at a frequency appropriate to the risk.
- Encryption of backups (AES-256 or equivalent).
- Periodic recovery testing.
- Documented continuity and recovery plan.

4. REVIEW PROCEDURES

4.1. Data protection management

- Data protection contact point: admin@aikit.io.
- Review of the technical and organizational measures at least annually.
- Periodic staff training on data protection and information security.
- Performance of Data Protection Impact Assessments (DPIA) where appropriate, in accordance with Article 35 of the GDPR.

4.2. Vulnerability management

- Automated vulnerability scans.
- Periodic penetration tests (pentests), at least annually, carried out by independent third parties.

- Public Vulnerability Disclosure Policy.

4.3. Incident response

- Centralized management of logs and alerts (SIEM).
- Capability to immediately block compromised accounts.
- Documented incident response procedure, with the involvement of Management and the technical team.
- Notification to the Client of security breaches without undue delay and, in any event, within seventy-two (72) hours of becoming aware of them, in accordance with the DPA.

4.4. Privacy by design / by default

- Application of the principles of privacy by design and by default in the development of new features.
- Data minimization: the platform processes only the data necessary to provide the service.

4.5. Sub-processor management

- Prior review and due diligence of sub-processors.
- Execution of processor agreements with sub-processors, replicating the obligations set out in this DPA.
- Execution of international transfer safeguards (Standard Contractual Clauses, EU-U.S. DPF) where appropriate.

5. ORGANIZATION

5.1. Internal policies

AIKIT RESEARCH, S.A. maintains a system of internal policies including, among others, an Information Security Policy, a Data Protection Policy and an Artificial Intelligence Policy.

5.2. Personnel

All personnel of AIKIT RESEARCH, S.A. and its external collaborators are subject to contractual confidentiality obligations and to the security standards set out in the internal protocols.

5.3. No-training commitment

AIKIT RESEARCH, S.A. does NOT use the Client's personal data, the Inputs or the Outputs to train its own or third-party artificial intelligence models, nor for any purpose other than that strictly necessary to perform the service.

6. UPDATING OF THE MEASURES

AIKIT RESEARCH, S.A. reviews and updates the technical and organizational measures of this Annex where justified by changes in technology, in the identified risks, in the applicable legislation or in industry best practices. Updates may not reduce the level of protection provided for.

CONTACT

Data protection contact: admin@aikit.io
Operational matters: admin@aikit.io
Incident reporting: admin@aikit.io

==========
End of document - Annex III to the DPA: Technical and Organizational Measures
==========