eAlicia.com Security Terms

Information Security Management System – ISMS

Document:	EAIT100_20251124_ISMS_eAlicia_Security_Terms_2.0.0
Version:	2.0.0
Issue date:	November 24, 2025
Responsible:	RunCall Systems, SL
State	Approved
Confidentiality	Public

The information contained in this document may contain inaccuracies due to typographical errors and/or updates to the various services described. For the most up-to-date information on the products/solutions listed, please visit our website www.ealicia.com .

Version control

Version	Date	Author	Change Description
1.0	2025/06/01	RunCall Systems, SL	Initial creation of the document.
2.0	2025/11/20	RunCall Systems, SL	Major review and restructuring of Section 8.

Content

Glossary and Definitions:

As used in this document, the following terms shall have the meanings set forth below:

- *“eAlicia” means “SaaS eAlicia private cloud”, and/or any of its respective accesses, as applicable (individually or collectively).*
- *“Confidential Information”, hereinafter “CFI”, has the meaning given to that term, including other similar terms with similar intent, according to the Supplier's agreement with eAlicia.*
- *“Client**”**, hereinafter “CLIENT**”**, means any client who uses or will use the service provided by this platform, as applicable.*
- *“Personal Data”, hereinafter “PSDT”, has the meaning given to that term, including other similar terms with similar intent, by applicable data protection and/or privacy law.*

1 Physical site and environmental security

The security measures in place at the VODAFONE SPAIN-owned data centre, where the servers are located, are established security areas/zones, and it is where the PSDT, as well as the rest of the information classified as Confidential, will be stored, are as follows:

- ISO/IEC 27001:2013 | Information Security Management
- ENS (high level) | National Security Scheme
- GDPR | General Data Protection Regulation
- ISO 9001:2015 | International Quality Management System
- ISO 22301:2012 | Business continuity management
- ISO/IEC 27017:2015 | Information security for cloud services
- ISO 14001:2015 | Environmental Management
- ISO 50001 | Energy management system
- High-sensitivity smoke detection and an industry-recognized data centre fire suppression system
- Electronically locked doors
- Electronic access card reading system
- Access management, documentation and history of authorized users
- The exterior of the building has a reinforced concrete structure and no windows.
- There is on-site security personnel available 24 hours a day, 7 days a week, 365 days a year.
- Security service at Reception, with mandatory registration for all visitors, with validation of the corresponding entry authorization.
- Anti-theft alarm system
- Building surveillance management system with CCTV, and of its different rooms, with internal and external monitoring, with infrared cameras for horizontal and vertical motion detection
- Biometric scanners

2 Availability control

The measures taken to ensure that the CFI or PSDT are protected against accidental destruction or loss of data are described below:

- Access to the rack cabinet using a numeric code.
- The room where the rack containing all the electronic and communications equipment is located is equipped with multiple air conditioning units to ensure an optimal temperature for the operation of this equipment.
- A double power line is available
- UPS
- There is dual internet access with dual operators and a guaranteed bandwidth of 500/500 MB.
- Fortinet FG100F firewalls, redundant and HA, with multiple layers and independent security policies for each VLAN and/or service
- Redundant communication switches
- Fibber optic connectivity
- Network segmentation with VLANs
- The systems are redundant, as are the servers, which have RAID array configurations.

The immutable backups are stored on various NAS devices within the data centre itself. In addition to these, a second copy is made in an alternative geographical location.

3 Network-level security

Measures have been deployed to prevent unauthorized access to the data processing environment and to prevent potential attackers from compromising the provider's network. These security measures include technologies in the following categories:

- Fortinet FG100D perimeter firewalls, redundant and HA, always updated with the latest version, and VPN-based access controls to protect private service networks and back- end servers.
- Advanced detection/prevention of persistent threats
- Denial of service protection
- Data loss prevention
- Mobile device management
- Web application security
- Continuous infrastructure security monitoring, with PRTG
- Periodic review of security risks by internal employees and external auditors, including vulnerability audits and pentesting (penetration testing of systems)
- Role-based access control, implemented in accordance with the principle of least privilege

Remote access protected by two-factor authentication tokens or multi-factor authentication.

4 Server characteristics

eAlicia's servers are specifically configured for the secure handling of Sensitive Information (SII) and Personal Data. They incorporate features such as redundant servers with RAID arrays and fiber optic connectivity to ensure availability and performance. Furthermore, robust defences have been implemented to protect against intrusions, including patch management procedures, antivirus and antimalware solutions, and encryption of all data in transit and backup media.

Main server configuration features for CFI and PSDT processing:

- Redundant servers, which have RAID array configurations
- Fibber optic connectivity
- Windows Server 2019 STD and Windows Server 2025 STD Operating System
- SQL SERVER 2019 Standard

Implemented defences for intrusion protection, antivirus and antimalware:

- Patch management procedures are implemented that prioritize security patches on the systems used to process CLIENT CFI or PSDT.
- Records of all audit, monitoring, and security activities are maintained for 120 days in a secure environment.
- Endpoint protection, and response capabilities are implemented.

Measures have been adopted to ensure that the CFI or PSDT cannot be read, copied, modified, or deleted without authorization during transmission or electronic transport, and that it is possible to verify and determine which agencies are intended to receive the transfer of CFI or STPS through data transmission facilities:

- All data (particularly sensitive PSDT) is encrypted in transit using the latest secure transmission protocols, Transport Layer Security (TLS) 1.3 with 2048-bit or higher RSA key exchange.
- Access to the reports is recorded.
- The backup media is encrypted.
- No removable storage is used.

5 Access control

This section describes the access control measures implemented on the servers to safeguard Confidential Information (CFI) and Personal Data (PSDT). Strict procedures are in place to prevent unauthorized use of data processing systems, including personal authentication and the use of strong passwords. Furthermore, it details the controls in place to ensure that only authorized personnel have access to the relevant data, and that any action on CFI or PSDT is logged and auditable.

Measures have been adopted to prevent data processing systems from being used without authorization:

- Personal and individual login when accessing the system or the corporate network.
- Password procedures require a minimum of 8 characters, including one uppercase letter, one lowercase letter, and one number. If a user account has five failed login attempts, it will be locked. All passwords expire after 90 days. After username and password verification, the application uses a session-based token authentication system.
- Remote access for maintenance requires two-factor authentication
- Automatic screen locks after a defined period of inactivity
- Password-protected screen locks
- All passwords are documented electronically and protected against unauthorized access through encryption.
- User accounts are audited twice a year

Controls have been activated to ensure that individuals entitled to use a data processing system have access only to the CFI or PSDT to which they have the right of access, and that such CFI or PSDT cannot be read, copied, modified, or deleted without authorization during processing or use, or after storage:

- User authentication is based on a username and a secure password.
- The data is stored encrypted at rest.
- All transactional records contain identifiers to distinguish customer records.
- The system's processing uses a role-based mechanism to tailor data access to specific users and roles.
- Access, insertion, and modification of data are recorded in log records or transactions.

Entry control measures are implemented to ensure that it is possible to verify and determine who has introduced, modified, or deleted CFI or PSDT into the data processing systems, should this occur:

- Use of user identification credentials
- Access to records is restricted to a defined set of roles
- Every entry has a date and time and includes identifiers for the resource or functionality being accessed.

Firewalls and intrusion prevention systems are implemented to prevent unauthorized access.

6 Software development controls

This document addresses the rigorous security measures implemented during software development to protect Confidential Information (CFI) and Personal Data (PSDTD). It details the principles considered in the improvements and changes, including the use of secure version control systems, code and dependency analysis, and the adoption of practices that mitigate vulnerabilities. Furthermore, it describes data separation controls, ensuring that information is processed independently in dedicated environments.

When improvements or changes are made, at the request of the CLIENT, that include software development, the following precepts will be taken into account:

- The source code is managed through a secure version control system.
- Secret data (such as passwords, API keys, etc.) is not stored in the source code.
- The source code is subjected to periodic static analysis (SAST).
- Software dependencies (such as code libraries, packages, modules, and frameworks) are subjected to software composition analysis (SCA).
- Development practices and testing methodologies (including the analysis techniques mentioned above) take into account common vulnerability vectors and up-to-date vulnerability databases.
- For example, OWASP Top 10, NIST NVD.

Separation Control: Measures have been deployed to ensure that CFI or PSDT collected for different purposes are processed separately.

- Three-tier systems are used to physically separate presentation, business processing, and storage.
- CUSTOMER data is stored in separate databases or logically separate architectures.
- Separation of duties is applied internally to ensure that functions pass change control processes.
- Development, testing, and production environments are maintained separately.
- All data routing for processing is controlled by automated rule engines.
- Processing and storage are performed on equipment owned by the Supplier.

7 Governance and security policies

This section focuses on how the organization establishes and maintains a robust security framework, through clear guidelines and defined responsibilities, to ensure regulatory compliance, proactive risk management, and continuous improvement of defences for sensitive information.

- Written information security policies and procedures, as well as incident response programs, are maintained and updated to comply, at a minimum, with (i) all applicable data protection laws and (ii) generally accepted industry standards for data protection, including ISO **27001:2013.**
- Drills to test information security procedures and incident response programs, at least once a year, keeping written reports of the results.
- There is staff responsible for determining, reviewing, and implementing security policies and measures.
- Allocation control: This is activated to ensure that, in the event of processing on behalf of CFI or PSDT, this data is processed strictly in accordance with the CLIENT's instructions.
    - Confidentiality agreements have been established for all individuals with access to the data.
    - Information privacy and security training is provided during onboarding and on a regular basis.
    - No third parties are used for data processing, except as described in the Agreements.
    - The privacy policy describes the rights and obligations of the agent and the CLIENT.

In the event that payment card data is processed by the CLIENT service, when processing or accessing cardholder data on behalf of eAlicia, the applicable credit card management standards of the issuer are met. eAlicia is aligned with the Payment Card Industry Data Services Standard (PCFIDSS) and will provide proof of compliance annually.

8 AI model security

8.1 Procedures with AI models

Purpose of the management model

This section describes and develops the technical, operational and regulatory compliance specifications of the **eAlicia platform**, developed and managed by **MST GROUP**.

The goal is to provide customers' security, technology, and compliance departments with a comprehensive description of the infrastructure, the artificial intelligence (AI) models used, the data protection mechanisms, the security measures, and the certifications applicable to the service.

8.1.1 Scope

The document covers the architectural design of eAlicia, its data processing methods (voice, text, and various types of files and images), the technologies used, security and privacy policies, and the ethical principles governing the use of AI within the framework of the **AI Act** and the **GDPR. It also includes a description of** *anonymization* mechanisms, auditing procedures, bias management, and human oversight of automated systems.

8.1.2 Functional objective of eAlicia

eAlicia is a quality platform focused on **intelligent auditing of customer interactions, used by companies that manage** their customer service directly or through **BPOs or contact centres.**

It allows for the **automatic and objective evaluation** of multi-channel interactions (phone calls, emails, chats, instant messages and social networks) using **generative and analytical AI models.**

The system generates **transcripts, summaries, performance indicators, and improvement recommendations,** both for agents and for service processes.

8.1.3 Corporate approach and regulatory compliance

The development of eAlicia has been carried out under a **security by design and compliance by default approach** (Security *& Compliance). by Design)*, ensuring that all phases—from data capture to results analysis—comply with applicable European and international regulations:

CERTIFICATIONS

- **GDPR** (General Data Protection Regulation).
- **ISO 27001** (Information Security Management System - ISMS).
- **ISO 22301** (Business Continuity Management System - BCMS).

COMPLIANCE WITH RECOMMENDATIONS

- **AI Act** (European Artificial Intelligence Act).
- **ENS** (National Security Scheme).

- **SOC 2 Type II** and **NIST SP 800-53** (systems control and audit standards).

8.1.4 Guiding principles of the platform

eAlicia is based on the following principles:

- **Privacy and confidentiality:** the connection is encrypted and critical data is treated under encryption, with strict access policies and minimum retention.
- **Transparency and auditability:** each automated process generates verifiable traceability.
- **Human oversight:** the decision generated by AI is validated by humans before being considered in audits or official reports.
- **Impartiality and absence of bias:** models are trained and validated with representative *datasets,* applying bias mitigation techniques.

Data sovereignty: All of eAlicia's infrastructure is deployed in private cloud environments located exclusively within European Union countries, guaranteeing full compliance with the principles of data residency and sovereignty. This approach ensures that all processed information remains within the European legal framework, strictly adhering to GDPR requirements, EDPB guidelines, and contractual obligations established with clients.

8.2 Technical Architecture

The **eAlicia platform** is based on a **SaaS model deployed on a private cloud** environment managed by **MST GROUP**, with physical infrastructure hosted in **VODAFONE and COLT data centres**. This configuration guarantees **geographic redundancy, low latency,** and **high availability** of critical services.

The architectural design is geared towards horizontal scalability, perimeter and logical security, and functional modularity, allowing the environment to be adapted to the technical, operational, and regulatory requirements of each client.

Each component of the solution is contained in Docker containers, which facilitates service isolation, environment portability, and deployment standardization. Container orchestration is managed through an internal control and administration layer, responsible for version control, deployments, monitoring, and dynamic scaling.

This modular and automated architecture allows:

- **Agile and controlled maintenance** of the environments.
- **Rapid replication** of configurations in development, pre-production, or production environments.
- **Effective isolation** between client instances, guaranteeing the **security and confidentiality** of information.

Overall, the adopted model provides a **resilient, flexible, and secure infrastructure,** aligned with best practices for **service-oriented *private cloud (SaaS)* architectures.**

8.2.1 Main components

a) Data acquisition layer

Responsible for receiving, validating, and storing input data (audio, text, and metadata). Supported channels include:

- Voice calls (WAV, MP3, OGG files).
- Textual transcripts.
- Digital interactions (emails, chats, social networks, instant messaging).
- PSDTF, DOCX, XLSX, etc. files.
- Image Files

Each flow is processed asynchronously **and encrypted from SFTP or APIs,** guaranteeing data integrity.

b) AI processing layer

It is designed according to the principles of **security, isolation and information control,** and constitutes the functional core responsible for advanced analysis of unstructured data.

This layer integrates services dedicated to **text extraction** from multiple file types, **audio transcription, semantic and linguistic analysis, automated summary generation,** and the **detection of relevant patterns and insights.**

All artificial intelligence operations are executed **within the private and controlled environment of MST GROUP**, without dependence on external services or transmission of information outside the corporate perimeter.

This ensures:

- **Complete isolation** of the processed data.
- The **non-exposure** of information to third parties or public processing environments.
- **Strict compliance** with **personal data protection and information security** regulations.

The AI layer combines different types of models:

- **Generative models,** used for text generation and advanced contextual analysis.
- **Proprietary Machine Learning and Deep Learning models**, developed internally by MST GROUP and trained on anonymized and controlled data, with the aim of covering specific use cases.
- **Internally modified and validated open source models** (like *Whisper, Llama* or *Mistral),* adapted to the technical, linguistic and regulatory requirements of each client.

Each model undergoes a rigorous **evaluation, adjustment, and validation process** prior to deployment, ensuring the **robustness, traceability, and lifecycle control of the algorithms used. Furthermore, logical and network segmentation** is maintained between the training, validation, and production environments, minimizing the risk of data exposure or leakage.

This architecture provides a **secure, governed, and auditable AI infrastructure,** aligned with the principles of **security by design, data minimization,** and **regulatory compliance** applicable to intelligent information analysis environments.

c) Storage and persistence layer

eAlicia's storage and persistence layer is designed to ensure the integrity, confidentiality, and availability of the data managed by the platform.

All information is stored on dedicated volumes, with a strict logical separation between clients that prevents cross-access to data or configurations.

Each client instance has configurable retention policies, tailored to its operational and regulatory requirements.

The system performs daily backups, stored in immutable environments isolated from the operating environment, guaranteeing full recovery in the event of data loss, corruption, or attack. Backups are periodically verified through validation and controlled restoration procedures, ensuring their availability and consistency.

This storage architecture provides a **secure, auditable persistence framework that complies with the ENS and ISO 27001 security principles,** enabling compliance with the continuity and information protection policies defined by each client.

d) Application and reporting layer

eAlicia's presentation and access layer provides secure mechanisms for viewing, querying, and exploiting results, metrics, and reports generated by the platform.

Access to information is provided through a secure web interface and a REST API that allows integration with authorized external systems.

Both channels are protected by robust authentication and a role-based access control (RBAC) system, which ensures that each user or consuming system only accesses the resources and data for which they have explicit permissions.

Reports and dashboards are generated in real time, providing up-to-date indicators on processes and results.

Each visualization includes full traceability of the data origin, allowing the consistency of the information presented to be audited and verified at any time.

This layer relies on **activity logging, auditing and protection against unauthorized access mechanisms, ensuring compliance with the confidentiality, integrity and availability** policies defined by MST GROUP and by the specific requirements of each client.

e) Integration layer (external data)

eAlicia 's **integration layer** enables secure **interoperability with external** corporate systems, facilitating the controlled exchange of information between the platform and third-party environments.

This layer incorporates **SOAP** and **REST-** based **connectors and web services,** enabling integration with enterprise resource planning (**ERP)** systems, customer relationship management (**CRM)** systems, and **contact centre platforms,** among others.

This integration is designed under principles of **modularity, traceability and security by design,** guaranteeing the consistency and protection of data throughout the communication cycle.

All connection and information transfer points are **protected by TLS 1.3 and SSL encryption,** ensuring the **confidentiality and integrity of data in transit.**

The authentication process is managed through the **standard OAuth2,** which allows granular control of access and authorizations.

mutual validation of SSL certificates is applied, reinforcing **end-to-end authentication** between the systems involved in the communication.

This layer also has **registration and auditing mechanisms** that allow monitoring of integration operations and detection of possible anomalies or attempts at unauthorized access, in compliance with the security policies of **MST GROUP and the ENS** and **ISO/IEC 27001** standards.

8.2.2 Network design and perimeter security

The infrastructure is designed under a segmentation approach **by security zones,** with the aim of guaranteeing **functional isolation, perimeter protection** and **control of information flows** between the different components of the system.

The design is structured in the following zones:

- **Public Zone (DMZ):** Manages external communications with users and integrated systems. It includes load balancers, application firewalls (WAFs), and intrusion detection and prevention systems (IDS/IPS), which filter, inspect, and mitigate potential threats before they reach internal layers.
- **Internal services zone:** houses business microservices and AI processing modules, isolated from the public network. It only accepts authenticated and encrypted connections from the DMZ or authorized internal zones, guaranteeing the confidentiality and traceability of every interaction.
- **Data zone:** dedicated to encrypted storage and databases segregated by client or environment. Access is restricted to internal services through minimal access control policies (least privilege) and strong authentication.
- **Monitoring and backup zone: This zone houses the** observability systems, metrics, audit logs, and backups. It is completely isolated from the user's operational networks, ensuring the integrity of monitoring data and incident recovery.

Each communication between zones is encrypted using **certificates** issued by an authorized certification authority.

This network design ensures **defines in depth,** minimizes the surface area of exposure and maintains compliance with the principles of **security by design, logical segmentation** and **advanced perimeter protection** defined by the **National Security Scheme (ENS)** and the **ISO 22301 and ISO/IEC 27001 and 27002 standards.**

8.2.3 Availability and resilience

- **Geographic redundancy:** all critical services are duplicated between VODAFONE and COLT data centres, maintaining backups in Barcelona and Madrid.
- **Automatic scalability:** the system can increase resources (CPU, memory or nodes) based on demand.
- **Continuous monitoring:** performance, security and availability metrics monitored 24/7.
- **Failover procedures:** automatic switchover in case of incidents and verified restoration.

8.2.4 Version and Deployment Management

The life cycle of eAlicia's services follows a **CFI/CD model (Continuous) Integration / Continuous Deployment)** that guarantees traceability, quality and safety in all phases of development.

Software versions are managed through **internal repositories** and validated in **isolated testing environments, structured in development, pre-production,** and **production** environments.

Each deployment requires:

- **Automated validation** through unit, functional, and integration testing.
- **Security review,** which includes static analysis, vulnerability scanning, and compliance checks.
- **Audit log,** ensuring full traceability of actions taken.

All changes are **documented and recorded in accordance with the MST Group's quality and safety** policies, ensuring compliance with applicable internal and regulatory standards.

8.2.5 Monitoring and alerts

The platform has **continuous monitoring systems** that allow for the detection of incidents, operational failures, and performance deviations in real time.

The **logs** are centralized and stored in a **secure analysis environment, with limited retention** policies, **restricted access,** and mechanisms that guarantee the **integrity and traceability** of the collected information.

The system also has **automated alerts** that notify the responsible teams of any abnormal event, facilitating a quick and effective response.

Relevant system events are monitored and incident management and response procedures defined according to **ISO 22301 are applied,** ensuring continuity of service and coordinated action in the event of any anomaly.

8.3 Data Processing and Artificial Intelligence

Data processing at eAlicia is governed by the principles of **minimization, *anonymization,* security and traceability,** guaranteeing the integrity of the information and compliance with European standards of data protection and ethics in AI.

The platform combines automated capture, processing and analysis processes with human supervision in critical phases to ensure reliable and auditable results.

8.3.1 Audio Capture and Tuning

Audio recordings from customer interactions (calls, voice recordings, etc.) undergo a **preliminary acoustic tuning stage** before transcription.

The techniques applied include:

- **Volume and frequency normalization.**
- **Background noise filtering.**
- **Channel separation and *dialysis*** (upon request).
- **Detection of silences and significant pauses.**

These processes improve the accuracy of speech recognition models and the final quality of the transcriptions.

8.3.2 Automatic Transcription

Speech-to-text transcription is performed using ***open source*** **automatic speech recognition models,** including Whisper, its variants, and other specific models implemented in the controlled environments of the **MST Group.**

All transcripts are processed exclusively on **MST's internal network,** ensuring that **there is no access to the transcript templates from external services** or transfer to providers.

Each transcript is **automatically validated** using metrics for quality, **semantic accuracy,** and **key entity detection,** and a monthly percentage is subsequently **reviewed by human auditors** within internal quality control and validation processes.

8.3.3 Generating summaries and extracting insights

Generative models, based on *open-source technologies* and their internal adaptations, process transcripts to **generate summaries, classifications, and service quality indicators.** These models allow for **the identification of relevant patterns and trends,** facilitating analysis and operational decision-making.

Generative AI operates exclusively according to **criteria predefined by eAlicia** and in **private network environments,** without exposure to external services and under continuous supervision. This operating model, along with its limited and controlled use, places the solution within the **regulatory boundaries of the AI Act,** classifying it as a **limited-risk system** and thus complying with applicable transparency and security requirements.

8.3.4 Quality meters and configurable variables

eAlicia incorporates a **dynamic performance measurement system,** based on configurable variables defined by each client and adapted to their operational needs. These variables may include, among others:

- Regulatory compliance.
- Accuracy of information.
- Communicative efficiency.

- Courtesy, tone, and empathy.
- Resolution of the query.
- Compliance with the internal protocol.

eAlicia's assessment system is based on principles of objectivity, non-discrimination, impartiality, and transparency, ensuring that results are not influenced by factors such as gender, age, origin, language, or other personal characteristics. These principles comply with the AI Act 's obligations for limited-risk systems, guaranteeing fair and auditable assessments.

The analytical models calculate the results in a weighted and standardized way, generating a **Global Quality Index (IQS)** and complementary metrics by agent, team and campaign, providing an accurate and fair view of service quality.

8.3.5 Human supervision and explainability

All AI processes at eAlicia are subject to **mandatory human oversight**. Automated results do not replace professional assessment, but rather complement it. Furthermore, the platform implements **Explainable AI (XAI)** principles that allow auditors to visualize:

- What elements of the conversation motivated the rating?
- What criteria or variables were applied?
- What factors influenced the recommendation or *insight* generated?

This transparency is fundamental to complying with the **AI Act** and with the ethical policies of MST GROUP.

8.4 Legal and Regulatory Compliance

eAlicia has been developed under a **Compliance strategy by Design,** ensuring that the platform and its processes are designed from the ground up to comply with European and national regulations on **security, privacy and data protection.**

The main applicable regulations and frameworks are:

- **AI Act** (European Artificial Intelligence Act).
- **GDPR** (General Data Protection Regulation) and LOPSDTGDD (Organic Law 3/2018).
- **ISO 27001, ENS** (National Security Scheme), SOC 2 Type II and NIST SP 800-53.

eAlicia, the platform, and its processes are **aligned with its requirements and best practices,** adopting technical and organizational controls directly inspired by these frameworks. This approach ensures a high level of security, governance, and risk management throughout the system's lifecycle.

8.4.1 Compliance with the AI Act

The **AI Act 's regulatory framework** establishes a classification of artificial intelligence systems according to their level of risk.

eAlicia is considered a **limited-risk system,** given that:

- Its function is **to support** the auditing, measurement and analysis of interactions.
- **It does not make autonomous decisions** that affect fundamental rights.
- It operates in **private network environments,** without connection to external services or transfer to third parties.
- Their results are **always subject to human supervision.**

Measures taken to comply with the AI Act:

1. Comprehensive technical documentation
2. Full recording and traceability of results
3. Mandatory human supervision
4. Periodic assessments of bias, performance, and fairness
    - Continuous adjustment of models to mitigate deviations.
5. AI governance and controlled lifecycle
    - Active monitoring of model behaviour.
    - Pre-deployment validation in pre-production environments.
6. Secure and private execution environments
    - Processing on the **MST internal network**
    - Isolation of personal data and strict access controls.
7. Transparency and compliance reporting for clients
8. Internal policies for the responsible use of AI
    - Aligned with ethics, non-discrimination and proportionality.
    - Procedures for detecting misuse or deviations.
    - Ongoing training of technical and analytical staff.

8.4.2 Compliance with GDPR and LOPSDTGDD

The data processed by eAlicia is processed in accordance with the principles of the **GDPR** and complementary Spanish legislation (LOPSDTGDD**)**:

- **Purpose limitation:** the data is used exclusively for quality audits.
- **Minimization:** only the strictly necessary data is captured.
- **Anonymization and pseudonymization:** identities are replaced by irreversible identifiers.
- **Data subject rights:** mechanisms to exercise access, rectification, erasure and portability.
- **Impact assessment (DPIA):** mandatory for every new project or client.

- **International transfers:** no transfers are made outside the EEA.

8.4.3 Certifications and/or compliance with standards

eAlicia adopts the main international standards:

- **ISO 27001:** Information Security Management System.
- **ISO 22301:** Business Continuity Management System.
- **ENS:** compliance with the Spanish National Security Scheme.
- **SOC 2 Type II:** Internal controls for security, availability, and confidentiality.
- **NIST SP 800-53:** Framework for risk management in information systems.

Internal audits are conducted annually and customers can request compliance verification.

8.4.4 Ethical audits and responsibility

MST Group maintains a **systematic program of ethical audits** aimed at verifying the **fair, transparent, and non-discriminatory behaviour** of the AI models used by eAlicia. These audits evaluate both transcription models and analytical and generative models, ensuring that their operation aligns with the principles of **fairness, proportionality, and respect for fundamental rights.**

The program includes:

- **Periodic review of biases** related to gender, age, origin, accent or any other personal factor that could affect the objectivity of the results.
- **Ethical impact assessments,** focused on the interpretability of the results and the absence of automated decisions that affect rights or freedoms.
- **Validation of the weighted behaviour** of the Global Quality Index (IQS) and other metrics, ensuring that the evaluation criteria are **consistent, impartial and auditable.**
- **Transparency analysis,** ensuring that customers and human auditors can understand how metrics, summaries, and rankings are generated.
- **Review of regulatory compliance,** ensuring alignment with the **AI Act** for limited-risk systems and with the MST Group's responsible use of AI policies.

The results of these audits are **formally documented,** communicated to those responsible for safety and quality, and integrated into the **continuous improvement cycle,** allowing adjustments to models, rules, parameters, or procedures if deviations or areas for improvement are detected.

This approach reinforces MST GROUP's commitment to **responsible, supervised, and safe AI,** maintaining high standards of quality and trust.

8.5 Information Security

Security in eAlicia is structured around three pillars:

1. **Secure and isolated infrastructure.**
2. **End-to-end encryption of data in transit.**
3. **Rigorous management of access, identities and vulnerabilities.**

8.5.1 Encryption and communications

- **Data in transit:** protected by **TLS 1.3** and **SSL.**
- **Credential encryption:** encrypted with **AES-256**
- **Internal channels:** exclusive use of corporate VPNs (IPsec VPN between PSDTs)
- **Integrity: digital signatures and** *checksum* verification on all critical files.

8.5.2 Access control

- **Authentication** and strong password policy.
- **Role-based authorization (RBAC).**
- **Principle of least privilege.**
- **Auditable access logs and periodic reviews.**

8.5.3 Incident Monitoring and Response

MST's internal SOC monitors the infrastructure 24/7, with intrusion detection tools (IDS**/IPS)** and event correlation systems.

Any incident generates an automatic alert and a standardized response procedure with defined severity levels.

8.5.4 Continuity and recovery

The VODAFONE and COLT centres operate in **active-active mode,** guaranteeing continuity of service in the event of incidents.

- **RTO (Recovery Time Objective):**
  - Mild incidence: less than 30 minutes.
  - Serious incident: 3 hours
  - Very serious incident: up to 36 hours
- **RPO (Recovery Point Objective):**
  - Incidence mild: less than 30 minutes

    - Serious/very serious incident: Daily backup

Contingency and backup plans are described in our **ISO 22301 certification.**

8.6 Privacy and Data Protection

The processing of information at eAlicia is governed by the fundamental principles of the **GDPR** and the **LOPSDTGDD,** applied from the initial design of the platform: *Privacy by Design* and *Security by Default.* Every module and process is built considering privacy as a structural requirement and not as an additional feature.

8.6.1 Anonymization and pseudonymization

Before any model training, all personal data is replaced with irreversible identifiers.

- **Text:** Names, phone numbers, emails, and any personal identifiers are removed upon express request by the service.
- **Metadata:** limited to essential technical information.
- Anonymization algorithms are reviewed periodically to ensure their effectiveness.

8.6.2 Retention and elimination

The data lifecycle is clearly defined:

- The data is retained only for the period necessary to fulfil the audit purpose.
- Once completed, they are securely and verifiably destroyed upon express request.
- Customers can request certified disposal reports.
- Audio recordings are kept for a maximum of 3 months, although this period may be modified upon express request.

8.6.3 Impact Assessments (DPIA)

Before on boarding new clients or implementing new features, the organization conducts a comprehensive risk analysis to identify any potential impact on individuals' rights and freedoms. This analysis is carried out in accordance with GDPR principles—such as data minimization, proportionality, transparency, and accountability—and, where applicable, with the risk assessment and classification requirements established by the AI Act.

Based on the identified risks, appropriate technical and organizational mitigation measures are defined and implemented, ensuring secure, ethical, and compliant data processing. Where necessary, a Data Protection Impact Assessment (DPIA) or a High-Risk AI Systems Impact Assessment is carried out, ensuring the adoption of additional controls to safeguard fundamental rights.

8.6.4 Rights of the interested party

The mechanisms for exercising the rights of access, rectification, erasure, objection, limitation of processing and portability are fully enabled for all interested parties, in accordance with the provisions of the **General Data Protection Regulation (GDPR)** and the **LOPSDTGDD.**

MST GROUP acts at all times as **the data processor,** applying only the documented instructions provided by the **data controller (client) and ensuring the implementation of appropriate technical and organizational measures in accordance with GDPR standards and applicable ISO 27001** controls.

All procedures relating to the exercise of rights, as well as the obligations and guarantees associated with the processing of personal data, are described and developed in the **Privacy Policy** published by the data controller and accessible to users through the corresponding website.

8.7 Technological Integrations

eAlicia provides its clients and integrating BPOs with several secure interoperability mechanisms, including APIs RESTful, SOAP Web Services, and file transfer via **SFTP.** All these methods are designed to guarantee the confidentiality, integrity, and traceability of the information exchanged.

• Encryption of communications (HTTPS):

APIs and SOAP Web Services are exposed exclusively through encrypted channels using HTTPS (SSL/TLS), ensuring that data in transit cannot be intercepted or modified.

• File transfer using SFTP:

For file-sharing-based integrations, a secure channel is provided via SFTP, which uses robust encryption and strong authentication to protect data transmission.

• Error management and traceability:

The services implement standardized response codes (HTTP 200–500) and generate detailed traces that allow for proper diagnosis, monitoring, and technical auditing in accordance with the best practices and controls established in **ISO 27001.**

This architecture ensures that integrations with eAlicia are carried out securely, consistently, and in accordance with regulatory and information protection requirements.

8.7.1 Compatibility

The platform is compatible with the main business environments:

Salesforce, Microsoft Dynamics, Genesys, Avaya, Zendesk, SAP, Oracle and other CRM/ERP/IVR solutions.

8.7.2 Webhooks and events

eAlicia offers the ability to integrate *Webhooks* that allow real-time notifications to be sent to the client's systems, facilitating automation and immediate monitoring of relevant events. Events that can be notified include:

- Completion of audits.
- Operational metrics update.
- Generation and availability of new reports.
- Automatic issuance of alerts for detected deviations or incidents.

Note: The activation, design and deployment of these *Webhooks* is done at the client's request, adapting to their technical and operational needs.

8.8 Reporting and Analytics

The eAlicia platform features an advanced interface with configurable *dashboards* designed to provide a clear and flexible view of operational and quality results. These dashboards allow for aggregated or detailed analysis of information, whether by agent, campaign, or contact centre, adapting to the needs of supervisors, auditors, and operations managers.

Key indicators that can be viewed include:

- Global Quality Index (IQS).
- Compliance with scripts and operational protocols.
- First Call Resolution (FCR).
- Indicators of empathy, customer experience, and satisfaction levels.

These dashboards allow for continuous performance monitoring and facilitate decision-making based on objective and auditable data.

8.8.1 Customized Reports

The eAlicia platform allows for the generation of reports both automatically and on demand, guaranteeing the continuous availability of accurate and up-to-date information. These reports can be exported in multiple formats, including PSDTF, XLSX, JSON, and CSV, and their periodic delivery can be scheduled to ensure the regular distribution of information to the relevant teams.

Each client has access to customized templates and evaluation criteria tailored to their processes, ensuring that reports accurately reflect their operational needs, internal metrics, and quality standards.

8.8.2 Advanced Analytics

eAlicia's analytics modules enable advanced assessments focused on performance optimization and data-driven decision-making. Key capabilities include:

- **Comparison of performance** between different BPOs, contact centres or operating units.
- **Identifying patterns and opportunities for continuous improvement** through detailed analysis and meaningful correlations.
- **Examination of the historical evolution of key metrics,** facilitating the monitoring of trends and the early detection of deviations.

- **Integration of data with external Business Intelligence (BI) systems** through the API, allowing the consolidation of information on corporate analytical platforms.

These modules offer a comprehensive and strategic view of performance, contributing to operational efficiency and the sustained improvement of quality levels.

8.9 Governance and Continuity

Backup Policies

The platform has defined backup policies to ensure the availability, integrity, and timely recovery of critical information. These policies include:

- **Backup Frequency:**

  Daily backups are performed, ensuring the regular and up-to-date capture of essential data.

- **Information Retention:**

  Backups are kept for a period of **90 days,** in compliance with internal continuity policies and requirements agreed with clients.

- **Geographic Replication:**

  The backed-up data is securely replicated between **VODAFONE** and **COLT data centres,** ensuring resilience to local failures and availability in contingency scenarios.

- **Verification and Restoration Testing:**

  are carried out **annually** to validate the integrity of backups and ensure the effectiveness of disaster recovery procedures.

These measures contribute to a robust framework for operational continuity in accordance with international best practices and the controls established in **ISO 27001.**

8.9.1 Monitoring and support

Security Operations Centre (SOC) and Network Operations Centre (NOC) ensure continuous (24/7) monitoring of the status of critical services, covering availability, performance and security parameters.

This continuous monitoring allows for the early detection of incidents, proactive analysis of anomalies, and the application of corrective or preventive measures in real time.

In addition, SLA indicators and metrics are applied (Service Level Agreement) aimed at guaranteeing demanding service levels, with availability targets exceeding 99.9%, in line with industry best practices and technological governance controls established in frameworks such as **ISO 27001.**

8.9.2 Life cycle management

Each component of the platform follows a **documented life cycle** that covers the phases of **development, testing, deployment,** and **review,** ensuring the quality, stability, and traceability of the changes introduced.

Changes are managed through a **formal version control system** and require **peer review before** approval, ensuring code integrity, early detection of errors, and compliance with internal secure development standards.

All records associated with the process —including evidence of testing, approvals, versions, incidents and technical documentation— are **kept for a period of five years** to allow consultation in **internal or external audit processes,** complying with the requirements established by the controls of **ISO 27001 and** DevSecOps good practices.

8.9.3 Continuity and Contingency Plan

MST Group has **documented and consolidated Disaster Recovery Plans (DRPs)** designed to ensure operational continuity and rapid service restoration in contingency scenarios. These procedures are structured according to international best practices and are **certified under the ISO 22301 Business Continuity standard.**

The implemented capabilities include:

- **Automatic Switching (Failover):**

  Automatic switching mechanisms that allow services to be restored immediately in the event of critical failures or unavailability of a system component.

- **Customer Notification Protocols:**

  Formal communication procedures that ensure **timely notification to customers** in the event of a serious incident, following the channels established in the Business Continuity Plan.

- **Annual drills and simulations:**

  The organization conducts **annual recovery drills,** validating the effectiveness of the procedures, the response capacity, and the coordination of the teams involved.

- **Multi-Zone Redundant Storage:**

  The infrastructure features **redundant storage** distributed across **multiple geographical areas,** reducing the risk of data loss and improving operational resilience.

These mechanisms ensure the availability of services in the face of disruptive events and comply with the requirements of **ISO 22301** and **ISO 27001 standards,** strengthening continuity and information security.

8.10 Ethical Audits and Bias Management

MST GROUP promotes the **responsible, safe and ethical use of artificial intelligence,** ensuring that all AI-based solutions implemented in eAlicia comply with the principles of **fairness, transparency, traceability, accountability and reliability.**

All AI functionalities deployed on the platform undergo **internal ethical audits,** which evaluate key aspects such as:

- **Fairness and absence of discriminatory biases.**
- **Transparency in models and traceability of decisions.**

- **Reliability, technical robustness and predictable behaviour.**
- **Compliance with the principle of data minimization and privacy by default (GDPR).**

Where applicable, implementations are aligned with the requirements of **the European Union AI Regulation (AI Act),** including:

- System risk classification.
- Mandatory technical documentation.
- Effective human supervision.
- Continuous management of the model lifecycle.
- Risk assessments and operational records.

This framework ensures that the use of AI in eAlicia contributes to improving the quality and efficiency of the service without compromising people's **fundamental rights.**

8.10.1 Identification and mitigation of biases

MST GROUP applies a systematic approach to the detection and correction of biases in AI models, ensuring fair and non-discriminatory operation.

The main actions include:

- **Detection of linguistic, cultural and gender biases:**

  Periodic analyses are carried out to identify deviations that may affect specific groups or unjustifiably influence the system's results.

- **Continuous human validation and review:**

  The results generated by the models are subject to periodic human supervision, including monthly calibrations, with the aim of avoiding automation that could produce discriminatory decisions or unwanted impacts on stakeholders.

This approach aligns with the principles of fairness, transparency and proactive accountability established by the GDPR, as well as with the risk management and human oversight mechanisms required by the AI Act.

8.10.2 Continuous monitoring

The AI models deployed in eAlicia are subject to a continuous monitoring process to ensure their proper performance over time.

The main actions include:

- **Production monitoring:**

  The models are constantly monitored in order to detect deviations, anomalies, loss of reliability, or performance degradation.

- **Periodic evaluation of equity metrics:**

The indicators of fairness and equitable behaviour are periodically compared with internal and external *benchmarks,* allowing verification that the model's performance remains balanced and non-discriminatory.

This process ensures that AI systems maintain their integrity, stability, and fairness throughout their operational lifecycle.

8.10.3 Technical documentation: Models Cards

Each artificial intelligence model used in eAlicia has its corresponding ***model A card*** is a structured technical document that ensures transparency, traceability, and understanding of the system's behaviour. These *models The cards* include essential information about:

- **Objective and scope of the model:**

  The specific function of the model, the intended use scenarios, the excluded cases, and the conditions necessary for its proper functioning are specified.

- **Training dataset:**

  The origin, composition, characteristics, and preparation criteria of the dataset used to train the model are described, including curation, cleaning, and balancing practices.

- **Known limitations and risks:**

  The technical limitations, expected range of variability, possible residual biases, and risks identified during testing and audits are detailed.

- **Mitigation controls applied:**

  The measures taken to reduce bias, improve fairness, strengthen security, ensure the robustness of the system, and maintain regulatory compliance are documented.

The *model Cards* form part of the official documentation required by current regulatory frameworks, contributing to **transparency, proactive accountability** and **effective human oversight,** in line with the principles of the **AI Act** and the **GDPR.**

8.11 Technology Roadmap

eAlicia's evolution plan includes:

- **Explainable AI (XAI)** for greater transparency.
- **Multimodal models** capable of analysing text, audio, and image.
- **Emotional and tone analysis** using prosody neural networks.
- **Customer satisfaction prediction Sentiment Forecasting).**
- **Advanced automation of the audit process,** always under human supervision.

8.11.1 Continuous Improvement

MST GROUP maintains a policy of continuous improvement based on:

- Constant technological innovation.
- Periodic audits.
- Customer feedback.
- Updated regulatory compliance.

8.12 Declaration of Technical and Legal Conformity

MST GROUP, as owner and responsible for the development and maintenance of the **eAlicia platform,** declares that:

1. The infrastructure, processes, and technologies described in this document comply with applicable European and international standards regarding security, privacy, and the ethical use of artificial intelligence.
2. The data processed is kept in *private cloud environments* located exclusively in countries of the European Union and is not transferred to third countries outside the European Economic Area.
3. The processing operations comply with the **GDPR,** the **LOPSDTGDD,** the **AI Act,** the **ENS, ISO 223201, ISO 27001, SOC 2 Type II** and **NIST SP 800-53.**
4. All AI models used have been internally audited, have human oversight, and document their fairness and transparency metrics.
5. MST GROUP maintains a continuous commitment to improving safety, quality and ethics in the development of technological solutions.

9 Communications

- Systems and processes have been implemented to communicate the results of cybersecurity incident investigations, if any, and incident response.
- The CLIENT will be promptly informed of the results of the investigations into the response to cybersecurity incidents.
- Communication will be carried out by sending an email to the CLIENT's contact. This email address must be provided by the CLIENT when activating this service.