# Technical and Organizational Measures Document

Version January 2025

# 1. Purpose

This Target Operating Model (TOM) outlines the technical and organizational measures (TOMs) implemented by The 297 Cloud Platform S.L. to protect personal data processed on behalf of Customers. It ensures compliance with applicable data protection legislation, such as GDPR, and safeguards personal data against unauthorized access, destruction, and modification.

# 2. Scope

### This TOM applies to:

- All personal data processing activities related to The 297 Cloud Platform S.L. services.
- Systems, employees, and approved sub-processors involved in data handling.
- Personal Data (e.g., professional contact details) processed under the service agreement.

# 3. Operating Principles

- Regulatory Compliance: Ensure all data processing complies with GDPR and other applicable regulations.
- Data Security: Implement strong technical and organizational measures to safeguard personal data.
- Transparency and Accountability: Maintain thorough documentation and audit trails for all processing activities.
- Data Integrity and Availability: Protect data against accidental loss, unauthorized access, and corruption.
- Retention and Disposal: Erase or securely destroy data when it is no longer required.

# 4. Key Functions and Responsibilities

### Data Collection and Consent Management:

- Collect only necessary data, such as professional contact information (name, email, phone number), with prior consent.
- Process no sensitive personal data as per agreement.

### Data Storage and Processing Locations:

- Data is processed and stored in private and secured Microsoft Azure cloud.
- Storage is segregated to ensure separate processing for different purposes.

### Access Management:

- Role-based access control ensures employees access only data relevant to their roles.
- All access authorizations are documented and reviewed regularly.

### Incident Management:

- Personal Data Breaches are reported to Customer within 24 hours of detection.
- Detailed incident response procedures include documentation, root cause analysis, and mitigation.

## 5. Technical and Organizational Security Measures

### Physical Access Control:

- MAP (MAP Platform & Intel EMA server) is running in the MS Azure Cloud. There is no physical IT system deployed by MAP.
- MAP (MAP Platform & Intel EMA server) is built on top of Microsoft Azure's secure foundation and takes advantage of multi-layered security across physical datacentres, infrastructure, and operations. It has state-of-art security delivered by Azure data centres globally. Azure cloud is built with customized hardware, has security controls integrated into the hardware, firmware components, and added protections against threats such as DDoS.
- MAP Premises are secured with double doors, safety doors/windows, and Securitas-managed burglar alarms.
- CCTV surveillance in all critical areas.

### System Access Control:

- MAP Platform:
  - Access control mechanisms, including Two-Factor Authentication (2FA), are implemented to restrict unauthorized access
  - Password Policies
  - Failed login attempt monitoring and automatic account lockout
  - Role-Based Access Control (RBAC) implementation
  - System logging of all access attempts

- Intel EMA Server:
  - For authentication, Intel EMA uses the OAuth 2.0 Resource Owner flow for authentication and authorization for usage with all Intel EMA REST APIs. I
  - Intel EMA also provides an internal process for managing authentication identities. For the internally managed option, Intel EMA manages authentication identities: An Intel EMA user can be simply created by providing an email address and a password for the user. The email address and a hash of the password will be stored in the Intel EMA database.
  - Access control mechanisms, including Two-Factor Authentication (2FA), are implemented to restrict unauthorized access
  - Password Policies
  - Failed login attempt monitoring and automatic account lockout
  - Role-Based Access Control (RBAC) implementation
  - System logging of user activities & system changes

## Data Access Control:

- Data, being a crucial asset, is protected through robust measures. Access control mechanisms, including Two-Factor Authentication (2FA), are implemented to restrict unauthorized access.
- Encrypted is used to safeguard its confidentiality,and a secure backup system is in place to guarantee data availability even in the face of unforeseen events.

## Transmission Access Control:

- Intel EMA acts as its own certificate authority, generating certificates for use with Intel AMT and the Intel EMA client agent.
- The root certificate for Intel EMA is created during installation along with a server settings certificate and a master encryption key.
- A TLS Server certificate will be generated during installation that will be used for communication with Intel EMA agents and endpoint client system Intel AMT. This certificate and key will be stored in the Intel EMA database, encrypted using the master encryption key Intel EMA supports multiple TLS versions, by default TLS 1.3 is used.

## Entry Control:

- Intrusion Detection System (IDS) to actively identify and mitigate potential threats. This proactive measure helps to safeguard against unauthorized access, malware, and other malicious activities, ensuring the reliability and security of our network infrastructure.
- Changes to personal data are logged. Audit logging exists in Intel EMA. Audit logs are stored in the Intel EMA database and are available for read only through a REST API.

## Availability Control:

- Secure backup system is in place to guarantee data availability even in the face of unforeseen events.

## Separation Control:

- Multi-Tenant Implementation
- Access control mechanisms, including Two-Factor Authentication (2FA), are implemented to restrict unauthorized access.
- Encrypted is used to safeguard its confidentiality

## Retention Rules:

- Personal data is erased within one month of a customer request during the agreement.
- Post-agreement, data is securely deleted.
- When all licenses are expired :
  - All data on the Intel EMA server are deleted
  - All data on the MAP Platform are archived
  - All logins of the customer on MAP Platform & Intel EMA Servers are disabled

### Security Certifications:

- Complying to OWASP best practices, incorporating their guidelines into our development and security processes. This ensures that our web applications are resilient against common security threats, providing a secure online experience for our users.

## 6. Governance and Oversight

### Policies and Procedures:

- Internal security instructions govern data handling and are reviewed periodically.
- Employees receive regular training on GDPR and confidentiality.

### Audit and Monitoring:

- Regular audits validate compliance with data protection regulations.
- Activity logs and access records are reviewed to ensure adherence to policies.

### Sub-Processor Management:

- Sub-processors require Customer's prior approval and must comply with equivalent security standards.
- Contracts include provisions for regular compliance checks.

## 7. Continuous Improvement

### Feedback Mechanisms:

- Regular updates based on audits, regulatory changes, and client feedback.

### Technology Upgrades:

- Integration of advanced security measures to strengthen defenses.

## 8. Contact Information

For any inquiries or further details about this TOM, please contact:

Data Protection Officer (DPO): Maxim Olivier, molivier@the297.com

IT Security Team: Alex Biet, abiet@the297.com

## Conclusion

These measures are part of The297Cloud Platform S.L.'s commitment to ensuring the security and confidentiality of personal data processed on behalf of the Customer. The297Cloud Platform S.L is responsible for maintaining these measures and providing documentation upon request to demonstrate compliance with the Applicable Data Protection Legislation.