ADVANCED ANALYTICS AND IOT SOLUTIONS

Whitepaper MangroviaIoT MangroviaAI

Advanced solutions for Asset Management and Operational Intelligence

WHP-IOT-AI-001-1.1

SORINT.tek s.r.l.
Via Zanica, 17 | 24050 Grassobbio (BG) | Italy | Tel +39 0356975211 | Fax +39 0356975290
COD. FISC., N. REG. IMPR. BG 04153090164 | PART. IVA 04153090164 – REA BG 439855 | CAPITALE SOCIALE € 10.000,00i.v.
Società Soggetta a Direzione e Coordinamento di SORINT.lab S.p.A. con sede in Via Zanica, 17 - 24050 Grassobbio (BG) | Italy con COD. FISC., N. REG. IMPR. BG 95164770166.

DOCUMENT INFORMATION

COPYRIGHT

CONTACTS

COMPANY	NAME	EMAIL ADDRESS
Sorint.tek	Roldano Malvesititi	mangroviaiot@sorint.com

DOCUMENT REVIEW

VERSION	DATE	AUTHOR	APPROVED BY	ISSUED BY
1.0	24/11/2025	Roldano Malvesititi	Emilio Tresoldi	Marco Pozzi
1.0	24/06/2026	Roldano Malvesititi	Emilio Tresoldi	Marco Pozzi

CHANGE HISTORY RECORD

VERSION	DATE	LAST MODIFIED
1.0	24/11/2025	First Issue
1.1	24/06/2026	AI and delivery models review

REFERRAL DOCUMENTS

VERSION	DATE	DOCUMENT
NA	NA	NA

SUMMARY

Introduction

This document is a White Paper on the delivery methods of the MangroviaIoT-MangroviaAI service, focusing on architectural, security, and compliance aspects managed by SORINT.tek S.R.L.

1. Glossary

1. **LATEK:** SORINT.tek S.R.L. Via Zanica, 17 – 24050 Grassobbio (BG) – Italy
2. **CSC**: the customer
3. **SaaS – Software as a Service**: a delivery model for application software where a software provider develops, operates, and manages an application made available to its customers via the Internet.
4. **On-Premise:** an **IT architecture and delivery model** where software, hardware infrastructure, and data storage systems are installed, configured, and physically resident within the logistical facilities (local data centers) of the organization that uses them.
5. **Software/Application Modules**: the MangroviaIoT platform, the MangroviaAI platform
6. **Access Credentials:** the identification code and access keys provided by LATEK necessary for using the application modules and software associated with the Customer, and required by the same for creating dedicated accounts for authorized users.
7. **License Code:** the identification code and access keys provided by LATEK to the Customer necessary for the installation of the application modules and software by the customer on its own hardware.
8. **Devices:** the devices and tools (e.g., sensors, control units, etc.) defined in the contract for which the customer must independently provide, proceed with their installation on physical and material supports, from which the devices must collect informational data to be transmitted to the application modules and software, and ensure their configuration and connection to the application modules and software.
9. **Connectivity:** the connection of devices to the application modules and software through link to a telecommunications network or the internet, which the customer must independently provide and ensure constant monitoring and adjustment.
10. **CSP**: Cloud Service Provider
11. **GCP**: Google Cloud Platform
12. **SSRM**: Modello di Responsabilità Condivisa (Shared Responsibility Model)

2. Application Modules

MangroviaIoT is a **modular and multi-level** technological platform developed and exclusively owned by SORINT.tek S.R.L. (LATEK) aimed at asset management and operational intelligence, as it allows the acquisition, processing, and analysis of IoT data intended to support predictive and prescriptive analytics. In particular, the main objectives of the application are:

1. Manage and monitor the status of a device infrastructure through the administrative and operational management of assets distributed across the territory, with control over the communication status of sensors, representation, and reporting of any anomalies.
2. Acquire, collect, monitor, and visualize sensor data through full governance of the lifecycle of data generated by sensors, from acquisition to representation, with a metrological verification system and notification of exceedance of configurable thresholds.
3. Advanced Analytics through statistical tools and machine learning algorithms aimed at predictive and prescriptive analytics included in the solution.

MangroviaAI is a **modular and multi-level** technological platform developed and exclusively owned by SORINT.tek S.R.L. (LATEK) aimed at operational intelligence and proactive security, as it allows the real-time acquisition and processing of continuous video streams, without any storage or saving of raw images and videos, extracting exclusively structured data and metadata aimed at supporting the automation of physical and decision-making processes. In particular, the main objectives of the application are:

1. Manage and monitor the corporate operational status and physical assets, transforming existing video surveillance infrastructures into a distributed network of intelligent sensors, with continuous control of processes in the field, operational compliance verification, and automatic reporting of any structural or process anomalies.
2. Analyze in real-time and process video streams through an immediate computing model that, excluding video data persistence in compliance with privacy regulations, is solely aimed at collecting, historizing, and visualizing only useful metric data, with an advanced detection system for critical events, filtering of false alarms through specific regions of interest (ROI), and timely notification of potential threats or inefficiencies.
3. Advanced Analytics and cognitive processing through Computer Vision algorithms, *Self-Supervised Learning* techniques, and virtual assistants based on *Large Language Models (LLM)* and *RAG* architectures, applied to data extracted from visual streams and aimed at supporting predictive and prescriptive analysis, optimizing team coordination, and providing immediate and contextual access to the corporate knowledge included in the solution.

3 Delivery Models

The MangroviaIoT-MangroviaAI product can be distributed and installed through three different delivery modes:

- **SaaS (Software as a Service)**: involves making the software and its respective application modules (specifically MangroviaIoT and MangroviaAI) available to authorized users through the use of a single copy hosted in LATEK's cloud space. In this configuration, the platform is managed entirely by LATEK, without system or security requirements being imposed on the Customer, other than the availability of a modern web browser and an internet connection.

- **On-Premise**: involves the installation of the software and its respective application modules on physical or virtual machines provided by the Customer at its own facilities (Local Data Center). In this mode, the responsibility for providing and managing the infrastructure and the orchestration platform (Kubernetes) lies with the Customer, who is required to comply with the system and security requirements specified in the following chapters.
- **Customer Cloud**: involves the installation of the software and its respective application modules on a cloud provider selected by the Customer, operating within its own dedicated account. Similar to the On-Premise mode, the Customer is responsible for providing and managing the infrastructure and the Kubernetes platform, ensuring compliance with the system and security standards defined in this document.

Unless otherwise specified, the service management model described in the following paragraphs applies to all delivery modes (SaaS, On-Premise, or Customer Cloud).

4 SaaS Delivery Model

The Software as a Service (SaaS) delivery mode involves making the software and its respective application modules (specifically MangroviaIoT and MangroviaAI) available to authorized users through the use of a single copy hosted in LATEK's cloud space.

4.1 Cloud Architecture and Responsibilities (SSRM)

The MangroviaIoT architecture is designed to be **cloud-agnostic** from an application standpoint, based on a microservices architecture on Kubernetes.

4.1.1 Infrastructure and Segregation

The SaaS environment is hosted at the Cloud Service Provider (CSP) Google Cloud Platform (GCP), which guarantees the following features:

- **Data localization**: data and cloud services are located in Europe. The primary cloud environment for MangroviaIoT SaaS is situated in the europe-west8 region (Italy). The secondary Disaster Recovery (DR) environment is situated in the europe-west9 region (France). LATEK documents and monitors requirements related to the geographic location of data.
- **Logical segregation**: separation between customers is guaranteed by the use of dedicated namespaces for B2B customers and a common namespace for B2C customers. LATEK implements rigorous technical measures to ensure logical segregation.
- **Installation flexibility**: at the application level, the product is cloud-agnostic and can reside in any Kubernetes installation.
- **Multi-tenant implementation**: installation occurs in multi-tenant mode within the service managed by GKE (Google Kubernetes Engine).

LATEK is committed to communicating proactively and promptly to its customers any entry of new infrastructure providers.

4.1.2 Shared Responsibility Model (SSRM)

The cloud service delivery follows the Shared Responsibility Model (SSRM), where LATEK and the Customer (CSC) assume defined roles based on the area of responsibility.

Area of Responsibility	**LATEK Responsibility (CSP)**	**Customer Responsibility (CSC)**
Physical Infrastructure and Data Center	Periodically monitors the Cloud Service Provider (GCP) for compliance with security, incident management, and availability commitments.	No Responsibility
Network, virtualization and HW	Ensures system hardening, network monitoring, and segregation of virtual environments and tenants.	No Responsibility
Platform	Manages base infrastructure configurations (GKE, Load Balancer, storage), ensuring security, regular updates, and high service availability.	No Responsibility
SaaS Application Module	Develops and maintains the software by adopting a secure development approach. Grants the license for use of the Software.	Management of Software use for defined Purposes. Solely responsible for the completeness, accuracy, updating, and truthfulness of data entered into the Application Modules and, in any case, the Software.
Encryption and Key Management	Guarantees data encryption “at-rest” and “in-transit” and correct management of cryptographic keys (managed by GCP or provided by the customer), ensuring confidentiality, integrity, and data protection.	Has the right to provide its own encryption keys, simultaneously ensuring their correct management and protection.
Access and Users	Provision of Access Credentials for the customer administrator (application access). LATEK provides the initial credentials through a secure channel,	Creation and management of Dedicated Accounts for Authorized Users. Custody and protection of Credentials, being the sole party responsible for use by third parties. Periodic review of application accounts and

	including an obligation to change the password at first login by the Customer administrator. Implementation of MFA/OTP for administrators (for infrastructure access). Implementation of MFA/OTP for administrators (for infrastructure access).	respective authorizations, ensuring assigned privileges respect the principle of "least privilege".
Intellectual Property	Maintains full and exclusive ownership of the Software and Application Modules.	No responsibility
Human Resources	Ensures that personnel have adequate training, competence, and experience. Personnel are trained and made aware of security issues, cybercrime in general, and best practices to be implemented in the CLOUD.	Ensures that personnel using the service are adequately trained in terms of information security and capability.
Subcontractors	LATEK is entitled to delegate the performance of certain Contract services to its affiliated companies. LATEK will, however, remain jointly and severally liable to the Customer for the services performed by the subjects listed above.	No responsibility

5 On-Premise and Customer Cloud Delivery Models

Unlike delivery models in SaaS (Software as a Service) mode, where the management of the entire infrastructure is the responsibility of the provider, **On-Premise** and **Customer Cloud** installations provide for a **shared responsibility model**. In these scenarios, operational continuity, physical security, updating, and resilience of the underlying infrastructure and platform are joint responsibilities that require the active collaboration of the Customer.

To this end, the operational and infrastructural *best practices* expected to guarantee the highest standards of security and efficiency of the Mangrovia system are reported below:

5.1 Installation Planning

- **Cloud:** Plan for distribution across different availability zones (*Availability Zones*) to prevent service interruptions caused by localized failures.
- **On-Premise:** Evaluate machine separation across different buildings and use of redundant power sources or backup generators.

5.2 Access Control (Principle of Least Privilege)

- **Direct Access:** Limit direct access to Mangrovia via VPN and only to a small number of selected users.
- **Standard Access:** Shield the system via firewall, allowing traffic only on specific ports (HTTPS and MQTT) and from known sources.
- **Physical Security (On-Premise):** Monitor and limit physical access to machines, networks, power systems, and utilities to authorized personnel only.

5.3 Disk Management and Redundancy

- **Cloud:** Choose disks redundant across multiple availability zones.
- **On-Premise:** Use redundant disk systems (e.g., RAID, Longhorn or equivalent) and apply encryption at rest.

5.4 System Updates

- Always keep libraries and software updated based on security requirements.
- **Cloud:** Manage Kubernetes node updates.
- **On-Premise:** Regularly update the operating system, drivers, Kubernetes versions, firewall, and every other infrastructure component.
- **Mangrovia Updates:** Be ready to receive periodic platform security releases. Timelines, downtime, and maintenance will be agreed upon.

5.5 Backup and Security Audits

- **Backup:** Plan and perform regular system backups using provided tools, archiving them in safe and protected storage systems.
- **Audit:** Periodically schedule security audits, both technical (e.g., firewall verification) and behavioral (e.g., phishing tests), defining action plans based on the results obtained .

5.6 Staff Training

- Ensure that personnel are adequately trained on system operational procedures and on general cybersecurity risks related to the business.

6. Development, Testing and Code Security

LATEK adopts rigorous secure software development practices, compliant with the principles of **Security by Design** and based on **OWASP** guidelines.

6.1 Secure Development Lifecycle (SDLC)

The **Secure Code Development Procedure** adopted by Sorint.TEK focuses particularly on **web based** applications as in the case of MangroviaIoT.

The practices include:

1. **Authentication:** application of complexity and rotation criteria for passwords. Invalid access attempts are logged, and passwords are stored through *hashing* mechanisms.
2. **Session Management:** Session tokens are managed by the server, and authenticated sessions expire after inactivity (Time Out).
3. **Access Control:** verification that the user is authorized to act on the destination data (Business Layer) and implementation of the principle of least privilege.
4. **Input Validation and Output Encoding:** input validation must occur as early as possible to prevent the entry of incorrect data. To prevent attacks like SQL Injection, it is **expressly prohibited** to use string concatenation to build SQL statements with user-controlled data, and it is **mandatory** to use parameterized queries.
5. **Logging**: Logs do not contain confidential information, including system details, credentials, or unnecessary passwords. All authentication attempts, particularly errors and all access control failures, must be recorded.

6.2 Environment Segregation

The **physical and logical separation between production and development environments** is guaranteed to prevent accidental deletions (in separate GKE clusters). **Debug mode** is only supported in development/testing environments.

6.3 Test Data Protection

LATEK implements measures for test data protection. The preference criteria are:

- Use of *data sets* that **do not contain personal data**.
- If not feasible, the data must be **anonymized or pseudonymized**.
- In cases where using real data is necessary, the activity will be tracked and justified. Data will be safely deleted at the end of use.

6.4 Vulnerability Management and Control

LATEK adopts a systematic and traceable approach to the management of technical vulnerabilities, in order to guarantee an adequate and constantly updated level of security. The planned activities include:

1. **Monthly vulnerability checks**: a vulnerability analysis related to the source code (SAST), libraries, and third-party components is performed monthly. These checks are executed via the Semgrep tool, integrated into the GitLab release pipeline, ensuring continuous and automated control.
2. **Annual independent assessments (VA/PT):** with annual periodicity, Vulnerability Assessment and Penetration Test activities are commissioned from specialized external companies.

These independent checks allow for the identification of any criticalities not detectable by automatic analysis tools and strengthen the overall security level of the environment.

7. Operational Continuity and Reversibility

LATEK has defined specific **High Availability** (HA) and **Disaster Recovery** (DR) procedures for the MangroviaIoT SaaS product.

7.1 Architecture for Continuity

The MangroviaIoT Software, based on Kubernetes, is structured to ensure high availability (HA) through:

- **Multi-AZ Support:** VMs, disks, and cloud storage *buckets* are configured for **Multi-AZ** (Zone) support within the primary region (**europe-west8, Italy**) or the secondary region (**europe-west9, France**), ensuring redundancy across different Zones.
- Use of **regional managed Kubernetes services (GKE) with multi-AZ support** and node pools configured across different AZs.
- Application data is backed up daily with a weekly retention period. Backups are stored within dual-region buckets.
- Application information (microservice versions, configurations, and *secrets*) are **versioned and persistently maintained in GitLab projects external to the cloud provider**, and are never modified directly in the cloud, but via GitLab CI/CD pipelines. This is fundamental for restorability.

7.2 Backup and Recovery Objectives (DR)

Responsibility for **Information Backup** lies with LATEK. Backup systems are configured to maintain multiple copies of data in physically/logically different locations: backups are kept on multi-AZ cloud storage with dual-region replication.

To ensure operational continuity and infrastructure resilience, several Disaster Recovery (DR) strategies are provided, calibrated to different risk scenarios and operational needs; the supported DR modes include:

- **Intra-Region DR (AZ Failure):** The goal is to guarantee an **RPO (Recovery Point Objective): 0h** (no data loss) and **RTO (Recovery Time Objective): 4h**.
- **Multi-Region DR (Total primary region unavailability):** The strategy is based on a *Backup & Restore* approach in a backup region (eu-west4), with defined objectives: **RPO: 1 day** (equal to the data backup frequency) and **RTO: 3 days**.
- **Restore:** The Multi-region DR procedure involves rebuilding the GKE cluster in the secondary region and performing a *restore* of the necessary Postgres databases using the available data backups. The Multi-region DR recovery procedure is verified annually.

Portability and Technical Migration: Since the architecture is cloud-agnostic, LATEK has a formalized procedure (**Cloud Provider Migration Procedure**) covering the switch to an alternative provider. Configurations, *secrets*, and microservice

versions are **persistently maintained in GitLab projects external to the cloud provider**, allowing the instance to be rebuilt in a different environment.

Full execution of the migration process requires **5 business days**.

7.3 Contractual Reversibility (Offboarding)

- Upon termination of the Contract, LATEK will proceed with the **secure and permanent deletion of all Customer data and information** (including personal data - PII), 60 days after the date of actual termination, unless there are legal obligations for retention.
- The **Customer** has the **right and responsibility to extract and transfer its data** and Information at any time prior to deletion, using the Software's standard export functionality. This guarantees the right to data portability in consistency with what is provided for by Art. 20 of the GDPR.
- Exceptionally, the Customer may request the Provider, within the 60-day period, a **paid service for data export assistance**. This service will be subject to a quote and hourly rates to be agreed upon and must be completed within a maximum term of 30 days, after which final deletion will still be executed.

8. Access Management and Operational Security

8.1 Software Access and Credentials

Application access to the MangroviaIoT Software by the customer and authorized users occurs through **Access Credentials** (User ID and Password) initially provided by LATEK.

LATEK reserves the right to adopt, in addition to or instead of User ID and Password, other or different access methods for using the application modules and the Software such as, by way of example but not limitation, digital certificates on smart cards or MFA/OTP with the obligation of prior communication to the Customer.

- **Customer responsibility:** The customer is solely responsible for creating and managing **dedicated accounts** for authorized users. Access credentials and authorization codes are **strictly personal and non-transferable**. The customer has the obligation to safeguard them with maximum diligence.
- The customer has the right to request activation of strong access methods already natively supported by the application, such as two-factor authentication (MFA/OTP).
- Access to the infrastructure and cloud services on which MangroviaIoT resides is for the exclusive use of LATEK personnel and is subject to strong authentication and privileged access management criteria.
- **Strong Authentication (MFA):** LATEK has implemented a two-factor Strong Authentication procedure (MFA/OTP) for all accesses using nominal IDs to the SORINT.Tek infrastructure and for administrators in Cloud environments, promoting it as a *best practice*.
- **Privileged Access:** The use of privileged utility programs is defined and regulated.

8.2 Communications Security and Encryption

LATEK applies cryptographic controls to both data *at rest* and *in transit*.

- **Encryption in Transit:** For transmission over public networks (necessary for Customer **Connectivity**), the use of **TLS 1.2 or higher (preferably TLS 1.3)** cryptographic protocols is required to ensure *in transit* security and the integrity of personal or sensitive data.
- **Encryption at Rest:** The **System Hardening Procedure** mandates encryption (AES-256) *at rest* for data protection.
- **Key Management:** LATEK defines and documents Key Management procedures and, where possible, uses the cloud provider's native services for automatic key and certificate rotation. The customer is still left with the right to provide and manage its own encryption keys if it prefers to maintain direct control.

8.3 Logging and Monitoring

Event log collection and analysis represent a fundamental element of operational security. In particular:

- System Administrator logs are subject to continuous monitoring, with particular attention to critical events such as account lockouts in Keycloak. In the event of relevant occurrences, an automatic email notification system for administrators is activated.
- System Administrator logs are retained for a period **not less than 6 months** and are protected to ensure the absence of sensitive information such as credentials or passwords.
- Application logs are maintained for a period of 1 month.

LATEK constantly monitors cloud resources to ensure correct service delivery and compliance with contracted SLAs. Capacity and performance are supervised through:

- The monitoring and observability systems of the Cloud Service Provider (CSP).
- Continuous monitoring of availability and status of GKE pods with automatic alert systems and email notifications in case of unavailability, reboots, or service degradation.

This approach allows for anticipating scalability needs, preventing bottlenecks, and ensuring the operational continuity of the platform.

8.4 Change Management

Technical and process changes are managed through an approval process, by means of notification procedures to customers where necessary. The notification procedures include details related to:

- Category and reason for changes;
- Date and time of the planned intervention;
- Technical description of the changes to the infrastructure or to the hosted applications;
- Notification of start or end of intervention.

Every application change to MangroviaIoT is managed through a CI/CD pipeline, ensuring that no change is directly applied to production cloud environments. This approach ensures version control, traceability of changes, deployment automation, and reduction of operational risk.

Furthermore, LATEK is committed to notifying customers of any change executed or planned by CSPs that might impact active cloud services.

9. Personal Data Protection (PII) and Lifecycle

LATEK (Sorint.Tek S.R.L.) is committed to treating personal data (PII) in compliance with the **European Regulation 679/2016 (GDPR)** and the **ISO/IEC 27018:2019** guidelines.

9.1 Roles and Obligations

The **customer** is the **Data Controller** of personal data. The Parties undertake to sign a special **Data Processing Addendum (DPA)** to govern responsibilities, with the responsibility for providing the DPA to LATEK resting with the Controller.

- **Purpose Limitation:** PII is processed by LATEK only for the purposes strictly necessary for the provision of the service, as indicated in the Cloud Policy, and not for marketing or advertising purposes. Access to PII in cloud services is strictly controlled and limited to authorized personnel who actually need it to perform their duties.
- **Data Subjects' Rights:** LATEK provides the Customer with the means and cooperation to facilitate the exercise of the data subjects' rights (access, rectification, erasure).

9.2 Subcontractor Management

LATEK is entitled to delegate the execution of services to affiliated companies or subcontractors. However, LATEK remains **jointly and severally liable** to the Customer for the services performed by such entities. The use of subcontractors for the processing of PII is communicated to the Customer before use.

9.3 Incident Management and Data Breach

LATEK has formalized procedures (Incident Response Plan, Data Breach Management Procedure) for handling security incidents.

- **Notification:** In the event of a Data Breach involving PII, LATEK informs the Customer promptly. The contractual SLA must define the maximum notification times for data breaches.
- **Contacts:** Customers can report security incidents to `incident@sorint.com` or Data Breaches to the DPO (`dpo@sorint.com`). Assistance requests for the Mangrovia product are tracked internally.

9.4 Video Data Management, Privacy by Design and Operational Continuity

The advanced **MangroviaAI** module, dedicated to **Video Analytics and Computer Vision** logic, natively integrates the principles of the European Regulation 679/2016 (GDPR), combining maximum personal data protection with high infrastructural efficiency.

The entire architecture of Mangrovia's Artificial Intelligence applications has been engineered to perform complex inference (such as *Object Detection*), relieving the Customer, as Data Controller, from the burdens and risks associated with the transmission and storage of visual data. Data management within this module is based on a purely transient processing paradigm, structured on the following technological and regulatory pillars:

- **Real-Time Inference and Zero-Data Retention:** Unlike traditional video surveillance or multimedia storage (VMS) systems, the AI applications integrated into MangroviaAI do not perform any persistent saving of video streams. Frames acquired from peripheral devices (cameras) are routed solely to the volatile memory (RAM) of the inference modules. The AI model analyzes the image in real-time to perform its task. At the exact moment the detection is completed, the original frame is discarded and the memory definitively and irreversibly overwritten. No visual data reaches or is ever written to cloud storage disks.

- **Vector Transformation and Exclusive Use of Metadata:** The system is designed to extract business information from pixels, immediately discarding the visual container. Following the inference phase, MangroviaAI extrapolates, transmits, and historizes exclusively mathematical and vector data: *bounding boxes* (spatial coordinates of the region of interest detected within the scene), classification *labels*, algorithm *confidence scores*, and respective *timestamps*. Immediately after processing, the system becomes intrinsically *blind* to the original image, retaining exclusively the derived telemetry.

- **Temporary Management for Training and Fine-Tuning:** Should it be necessary to optimize algorithmic performance through training or *fine-tuning* activities to adapt models to the specific Customer context, the system provides a dedicated operational mode. In this scenario, activatable for specific purposes, video frames necessary for training are temporarily saved in a segregated environment. The retention of raw visual data is **strictly limited** to the time period indispensable for the execution and validation of training. Upon completion of this activity, original images are safely deleted. Following the process, the platform retains and uses exclusively the new *model weights*, i.e., mathematical matrices representing the algorithm's learning, from which it is technically impossible to reconstruct or trace back to the starting visual data.

- **Privacy by Design, Anonymization and GDPR Compliance:** This setting rigorously applies the principles of *Data Protection by Design and by Default* and the *Data Minimization* required by the GDPR. Generated metadata is unstructured and anonymized at the source, resulting in no attributes that allow for the direct or indirect identification of a natural person (for example, returning only the numerical count of *people* or *vehicles*). The absence of a persistent video archive nullifies risks related to biometric data processing. In the event of a hypothetical *Data Breach* to cloud databases, the only information exposed would be numerical coordinates without visual context, with a risk to the rights of data subjects structurally equal to zero.

- **Infrastructural Efficiency and Disaster Recovery Optimization:** This precise architectural choice revolutionizes the operational continuity management outlined for the platform. Exclusive metadata transmission drastically reduces network bandwidth consumption. Furthermore, not having to manage, replicate, or back up massive video streams (which would involve heavy I/O bottlenecks), Disaster Recovery procedures are exceptionally

light. Backups focus solely on light relational databases and AI model configurations. This ensures rapid recovery times (*RTO*), nullifying inefficiency risks and promoting a highly scalable and sustainable cloud architecture.

9.5 Service Termination and Data Deletion

At the end of the Contract, service deactivation procedures ensure secure data management:

- **Restitution:** It is expressly understood that **LATEK shall have no obligation to return or deliver to the Customer the data and information** present on the Software at the time of termination.
- **Secure Deletion (SaaS Mode):** Within 60 days of the termination of the Contract in SaaS Mode, LATEK provides for the **secure and/or irreversible erasure and destruction** of data stored in the Cloud, in compliance with internal procedures (e.g., Information Deletion Procedure). LATEK implements measures for secure and irreversible erasure, recommending overwriting or cryptographic erasure for sensitive data.

10. Technical Support and Performance

10.1 Customer Support

Assistance requests for the Mangrovia product can be opened by customers via telephone or email (support@mangroviaiot.com). Each request is tracked via the corporate ticketing *tool*.

Contracts exclusively include second-level support assistance, provided during office hours from Monday to Friday, from 9:00 AM to 6:00 PM.

10.2 Internal Service Level Objectives (SLO)

LATEK adopts a structured set of internal Service Level Objectives (SLO), defined to ensure a constant and measurable level of service.
These objectives are monitored quarterly and represent a formal commitment to the continuous improvement of the performance and reliability of the services provided.

For Incident or urgent bugs, these are the monitored SLOs:

- **Response KPI: <** 2h (if reported during office hours) or < 11:00 AM (if reported outside office hours or on holidays).
- **Resolution KPI:** < 24h**.** Where not possible due to development needs exceeding 1 man-day or when inter-facing with other providers/partners for problem resolution is necessary, a follow-up update to the customer must be guaranteed every 4h (during working hours) until problem resolution.

For all other reports or support requests, these are the monitored SLOs:

- **Response KPI:** reporting day (< 1d) (if reported during office hours) or < 1:00 PM (if reported outside office hours or on holidays).

- **Resolution KPI:** not provided.

The customer has the right to request a detailed summary report relating to the service indicators of interest.
LATEK undertakes to provide this documentation within 15 days of the request, ensuring transparency and traceability of the monitored performance.

10.3 Service Availability SLA

LATEK ensures service availability levels aligned with the SLAs guaranteed by the Cloud Service Provider (CSP), GCP (Google Cloud Platform), on which the infrastructure is hosted.
Relevant availability values, as well as applicable conditions, are available in the official documentation of the CSP (see: **Google Cloud Service Level Agreements**).

LATEK has implemented a periodic process on the critical provider GCP to verify compliance with the commitments assumed regarding internal security management and relative certifications, security event management, and actual service availability.

10.4 Contractual Reference and Limitation

This Whitepaper describes the technical architecture, security measures adopted, and internal objectives (SLO) of the MangroviaIoT service in SaaS mode.
It is specified that all binding service commitments, license terms, economic conditions, Intellectual Property discipline, liability management, and provisions on data Reversibility (Offboarding) are entirely regulated by the Contract signed between the Customer and LATEK (Sorint.tek s.r.l.), and its MangroviaIoT General Conditions.
In the event of any conflict or divergence between the content of this Whitepaper and the contractual terms, the clauses contained in the Contract and the MangroviaIoT General Conditions shall always prevail.

10.5 Note on ISO 27017 and 27018 Controls

SORINT.tek guarantees that its operational practices and contractual requirements toward CSPs and Customers are aligned with specific controls for cloud services (ISO 27017) and for the management of PII (ISO 27018). This includes periodic verification of CSP certifications and the application of rigorous policies for privileged access management and tenant segregation.