P1.1-3
Customer information for the use of Cloud services

(UNI EN ISO 9001:2015 - UNI CEI EN ISO/IEC 27001:2024 – UNI CEI EN ISO/IEC 27017:2021)

Ver.4	05/11/2026	FG	Management Team	CEO	PUBLIC
REVISION	DATE	DRAFTED	VERIFIED	APPROVED	CONFIDENTIALITY

Summary

1 INTRODUCTION....4

2 SCOPE....4

3 COMPLIANCE PRINCIPLES....4

4 ROLE-BASED AND ACCOUNTABILITY-BASED SERVICE SECURITY FRAMEWORK....5

4.1 Shared responsibility model.... 5

4.1.1 CLOUD MAT (SAAS) Responsibilities Table.... 6

4.1.2 Mat Control Center (MCC) Responsibility Table.... 7

4.1.3 WILSON Cloud (SaaS) Responsibilities Table.... 8

4.2 Roles and responsibilities.... 9

5 TECHNICAL AND ORGANISATIONAL SAFETY MEASURES....9

5.1 Employee training.... 10

5.2 Company regulations and code of ethics.... 10

5.3 User Minimum privilege policy.... 10

5.4 Rules for access management.... 10

5.5 Utility lifecycle management.... 11

5.5.1 MAT.... 11

5.5.2 MCC.... 11

5.5.3 Wilson.... 12

5.6 Capacity monitoring.... 12

5.7 Logging of administrative activities.... 12

5.8 Back-up & Redundancy.... 13

5.9 Encryption by default.... 13

5.10 Segregation and isolation.... 14

5.11 Managing virtual networks.... 14

5.12 Secure Development Management.... 14

5.13 Protecting customer data.... 15

5.14 Customer data labeling.... 16

5.15 Deletion of customer data.... 16

5.16 Synchronizing Clocks.... 16

5.17 Utility programs.... 16

6 SUPPLIER SELECTION AND MONITORING....17

6.1 Evaluation and monitoring criteria.... 17

6.2 Cloud provider platforms currently used.... 17

6.3 Data geolocation.... 18

7 RESPONSIBLE USE OF AI....18

7.1 Functionality and Reliability.... 18

7.2 Confidentiality and Data Protection.... 18

7.3 Alignment with the Organization's Code of Ethics.... 18

7.4 Human Supervision and Control.... 19

7.5 Continuous Monitoring and Audit.... 19

7.6 References for AI cloud services used.... 19

8 CHANGE MANAGEMENT....19

8.1 Categories of changes.... 19

8.2 Methods of communication to customers....19
8.3 Termination of License....20
8.4 Critical Operations Management and Documentation....20
9 VULNERABILITY MANAGEMENT....20
9.1 Scope and application....20
9.2 Identifying vulnerabilities....21
9.3 Assessment and mitigation....21
9.4 Verification and Monitoring....21
9.5 Communication and Notification....21
10 INCIDENT MANAGEMENT....21
10.1 Incident reporting and digital evidence request....21
10.2 Incident handling methods....22
10.3 Disaster recovery....22
11 USE OF CUSTOMER DATA....23
12 COMPLIANCE WITH LEGAL REQUIREMENTS....23
12.1 Certifications....23
12.2 Additional legal requirements....23
13 OBJECTIVES LEVEL OF SERVICE OFFERED....24
14 COMMUNICATION TO AND FROM CUSTOMERS....24
15 THIRD-PARTY IP INFRINGEMENT REPORTS....24
16 SECOND-PARTY AUDIT POLICY....24
17 CONCLUSION....25

1 Introduction

This policy aims to make transparent the management of the cloud services offered by 40Factory to its customers.

Starting from 2024, in its evolution from start-up to scale-up, the company has faced an activity of consolidation and organizational improvement through the implementation of an Integrated Management System (IMS) for the quality and security of information, documented in its Integrated Management System Manual (IMSM). Among the objectives for the improvement of the IMS, the management has defined **an information security policy, transparent for its customers,** with the aim of:

- Describe how personal and non-personal data is processed and protected.
- Present the security measures adopted in 40Factory's integrated management system in accordance with the standards adopted by the organization such as ISO/IEC 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 27017:2021
- Ensure transparency of data processing in compliance with EU Regulation 2016/679 (GDPR)
- Meet the requirements of the NIS2 regulation for the support of customers who fall within the scope of NIS2, even though 40Factory has been recognized by the European reference authority for Italy ACN as a subject "not in the scope of NIS2" following the notification activity by the organization.

2 Scope

The document applies to all cloud services provided by 40Factory, as a cloud *service provider for* its customers. In this context, 40Factory is also a cloud *service customer*, as it uses cloud providers for internal processes and for the provision of the services offered.

3 Compliance principles

40Factory applies a policy of transparency towards customers and undertakes to comply with all current regulations as well as the standards adopted through all the necessary countermeasures to comply with the applicable requirements with a continuous monitoring plan for the maintenance of the standards adopted and their improvement.

The principles underlying the controls implemented, with references to the requirements of the standards, are:

- Security structure, based on shared roles and responsibilities, with a clear definition of responsibilities between provider, partner and customer
- Training and training of staff through a 40Factory staff training plan aimed at compliance with current regulations, customer satisfaction and information security.
- Monitoring of the services offered through activity tracking, automatic reporting systems and automatic notifications for any anomalies
- Retention of information through documented data retention and deletion policies.
- Protect data transmission through secure MFA authentication, encryption between IIoT devices, APIs, and cloud services.

- Selection of cloud providers through the definition of vendor requirements, the management of contracts including SLAs (Service Level Agreements) and DPAs (Data Processing Agreements) and their monitoring.
- Privacy and protection of both personal and non-personal data managed.
- Segregation of services offered in a multi-tenant environment.
- Change management in accordance with the service levels offered
- AI project management in compliance with ethical and information security requirements.

4 Role-based and accountability-based service security framework

4.1 Shared responsibility model

The parties involved in the provision of the cloud services offered by 40Factory are:

- **40Factory**: The organization that provides the Cloud service, as a cloud provider
- **40Factory Customers**: all customers who subscribe to and use 40Factory products. 40Factory customers can use these services to resell services and access licenses to their end customers.
- **Cloud Providers of 40Factory**, a SaaS cloud service provider used by 40Factory as a cloud customer. The provider provides the cloud tools used by 40Factory for the provision of its services.

The following table of responsibility explains the shared responsibility model adopted for each software product:

4.1.1 CLOUD MAT (SAAS) Responsibilities Table

Activity	40Factory	Cloud Providers	40Factory Customers
Physical and infrastructural security of Cloud servers		X	
SaaS application security	X		
Access and identity management			X (via customer Cloud resources, 40Factory recommends MFA configuration)
Data Backup & Restore			X (via customers' cloud resources, 40Factory recommends backup plan configuration)
Backup and restore of application layer and configurations	X	X	
Infrastructure vulnerability management	X	X	
Application vulnerability management	X		
Data retention			X
Availability and business continuity	X		X
Technical support and ticket management	X		
Deletion of data at the end of the contract			X
Cancellation of end-of-contract configurations	X	X	

4.1.2 Mat Control Center (MCC) Responsibility Table

Activity	40Factory	Cloud Providers	40Factory Customers
Physical and infrastructural security of Cloud servers		X	
SaaS application security	X		
Access and identity management	X		
Data Backup & Restore	X	X	
Backup and restore of application layer and configurations	X	X	
Infrastructure vulnerability management	X	X	
Application vulnerability management	X		
Data retention	X		X
Availability and business continuity	X		
Technical support and ticket management	X		
Deletion of data at the end of the contract	X		
Cancellation of end-of-contract configurations	X	X	

4.1.3 WILSON Cloud (SaaS) Responsibilities Table

Activity	40Factory	Cloud Providers	40Factory Customers
Physical and infrastructural security of Cloud servers		X	
SaaS application security	X		
Access and identity management	X		X
Data Backup & Restore	X	X	
Backup and restore of application layer and configurations	X	X	
Infrastructure vulnerability management	X	X	
Application vulnerability management	X		
Data retention	X		X
Availability and business continuity	X		
Technical support and ticket management	X		
Deletion of data at the end of the contract	X		X
Cancellation of end-of-contract configurations	X	X	

4.2 Roles and responsibilities

To ensure the quality and continuity of the services offered, **40Factory has defined specific roles within its organization**. The roles defined by the organization, as defined in the job descriptions, are:

Roles	*Contact*	*Responsibility*
DPO – Data Protection Officer	dpo@40-factory.com	It monitors compliance with the GDPR, informs and advises the data controller and processor of personal data, acts as a point of contact with the competent authorities and towards the outside world.
SSI – Information Security Supervisor (CISO)	info@40-factory.com	The Information Security Supervisor is responsible for implementing, managing, and controlling technical and organizational measures to protect the organization's data and information systems internally.
AI Ethics & Security Lead (CTO)	info@40-factory.com	Its task is to monitor the AI features integrated into 40Factory products in order to comply with the applicable regulatory requirements and ethical requirements defined by the organization.
Azure Global Administrator (DOM)	-	It is responsible for administering the Azure resources created by the organization to support internal services and for the delivery of the services offered.
Wilson 40Factory Administrator	-	Administrators have the ability to create new instances for customers, change licensing parameters, and monitor customer usage of the solution.

These roles are defined within the *company organization chart* and the *matrix for defining the roles and permissions* of the organization's IMS.

Based on the roles, 40Factory provides initial and continuous training of internal staff, to ensure that quality and safety requirements are met.

5 Technical and organisational safety measures

The principles underlying the technical and organizational measures introduced by 40Factory to implement information security extended to cloud services are listed and detailed below:

1. **Employee training**
2. **Company regulations and code of ethics**
3. **User minimum privilege policy**
4. **Rules for access management**

5. **Utility lifecycle management**
6. **Capacity monitoring**
7. **Logging of administrative activities**
8. **Backup & Redundancy**
9. **Encryption by default**
10. **Segregation and isolation**
11. **Managing virtual networks**
12. **Secure Development Management**
13. **Protecting customer data**
14. **Customer data labeling**
15. **Deletion of customer data**
16. **Synchronizing Clocks**
17. **Utility programs**
18. **Asset Tracking**

5.1 Employee training

40Factory, within the organization's integrated management system, defines on an annual basis the budget dedicated to the **training of all the company's personnel, both in the field of quality and information security, also specific for the management of cloud services**.

For technical staff, an advanced training plan is defined structured on these main topics:

- Information Security
- Secure coding
- Secure Development Life Cycle
- Threat modelling

5.2 Company regulations and code of ethics

The company has defined the **company regulation and policy for quality** and **regulation and policy for information security**. All employees of the organization are informed and required to comply with the company regulations to ensure the quality of the services offered and compliance with the safety requirements defined by the organization.

5.3 User Minimum privilege policy

To ensure maximum security and integrity of data and systems, **the company adopts a strict minimum *privilege policy*:** each user receives only the permissions strictly necessary to carry out their functions.

The assignment of privileges is carried out on the basis of the job held and defined, responsibilities and operational needs; It is subject to periodic reviews by the company's manager to ensure that access is always adequate and limited. This practice significantly reduces the attack surface, limits exposure to internal and external risks, and helps maintain high standards of security and regulatory compliance.

5.4 Rules for access management

Specific IT access management rules apply to all cloud services with authentication systems managed to the organization~~: all permissions~~ and privileges managed on external resources on customers' cloud tenants are therefore excluded.

The company has adopted **Microsoft EntraID as a provider for managing user authentication** as it complies with the specifications defined by the organization; for specific information refer to the Microsoft Azure EntraID documentation.

The company has established **an access management policy** based on "strong" authentication that focuses on the following principles:

- Nominal users that cannot be shared even within the 40Factory organization.
- Multi-Factor-Authentication (MFA) protection as a mandatory security measure to protect access to digital assets. MFA is enabled for all cloud services provided to customers, ensuring an adequate level of protection against unauthorized access. In addition, MFA is active on all cloud platforms used internally and is binding for all employees, regardless of their role or level of access.
- Security (MFA) on customer-owned tenants: The organization recommends setting MFA on all third-party tenants, used to access the Cloud MAT platform, not under the direct control of 40Factory.

This policy strengthens access control, reduces the risks of credential compromise, and supports compliance with the highest security standards.

The services offered by 40Factory provide **for the management of customer user privileges** for:

- The assignment of privileges.
- The revocation of user accounts.
- Inviting new users.

For additional details, please refer to the technical product documentation accessible to users.

5.5 Utility lifecycle management

The organization has defined the utility lifecycle for the products and services it provides to customers:

5.5.1 MAT

The management of the life cycle of the users is the responsibility of the MAT customer, since the authentication server is owned by the customer. The organization recommends the use of strong authentication methods and proper user management.

5.5.2 MCC

MCC's utility lifecycle follows this flow:

- **Creation of user accounts**: at the request of the customer, 40Factory staff invites users to access via e-mail address. The invitation is always made using the Single Sign-On (SSO) system based on Microsoft Entra ID.
- **Credential management**: since Single Sign-On is used, the management of credentials is delegated to the user himself through his access management system.
- **Role and permission management**: Roles and permissions are assigned by 40Factory staff to ensure that the user has exclusive visibility into the data related to their **sub-tenant**.

- **Account revocation**: at the request of the Customer or in the event of termination of the contract, the invitation is revoked and the user removed from the MCC platform.

5.5.3 Wilson

Wilson's utility lifecycle follows this flow:

- **Creation of user acconts**: at the request of the customer, 40Factory staff invites users to access via e-mail address. The invitation is always made using the Single Sign-On (SSO) system based on Microsoft Entra ID. Alternatively, the admin customer user can invite users to their Wilson environment, through the appropriate interface.
- **Credential management**: since Single Sign-On is used, the management of credentials is delegated to the user himself through his access management system.
- **Role and permission management**: roles and permissions are assigned by 40Factory staff to ensure that the user has exclusive visibility into the data relating to their **sub-tenant**. The Customer's administrator also has the possibility to independently manage permissions within his sub-tenant through a dedicated interface.
- **Account revocation**: at the request of the Customer or in the event of termination of the contract, the invitation is revoked and the user removed from the Wilson platform. Alternatively, the customer administrator can remove users from the platform via a dedicated interface.

5.6 Capacity monitoring

The company has defined the following **activities for managing the monitoring of cloud services provided to customers:**

- Cloud Services are **monitored on a daily basis** through an interface that provides information about resource usage and reachability of service endpoints
- In addition to continuous monitoring, there is **an automatic push notification system**, which immediately notifies managers of the events of: unreachable application, excessive use of service resources or saturation of infrastructure capacities.
- It also automatically detects and notifies **you of any configuration changes to managed services** to verify that they come from trusted sources and align with business processes

5.7 Logging of administrative activities

The organization has implemented:

- **Logging systems of the administrative activities** carried out by 40Factory personnel performed for the updating, configuration and management of the resources necessary for the provision of the services offered; this information is available only to 40Factory personnel.
- **Logging systems of the activities carried out by the customers' administrative users** within the cloud platforms provided to the customers; these logging systems are available to the administrators defined by the customers.

- **Logging systems of the activities performed by customer-defined users** within the cloud platforms provided to its customers, such logging systems are available to customer-defined administrators.

Access to logging logs is defined based on the roles and permissions of individual users.

5.8 Back-up & Redundancy

For the provision of cloud services, 40Factory **adopts backup & redundancy tools made available by the chosen cloud platforms (Microsoft Azure for data and configurations; the Kubernetes clusters on Scaleway hold no data and can be rebuilt from versioned configurations) to guarantee** the level objectives offered defined in the following document.

Backup policy

The organization performs automatic backups, several times a day, of all production environments of the software offered, including customers' customized configurations, the data they upload and their software repositories, as defined in its backup, disaster recovery and redundancy procedure. Backups are retained for 14 to 30 days depending on the resource, and databases support point-in-time restore over the last 7 days, to ensure an adequate time window for any recovery operations.

The organization recommends that its customers configure back-up and redundancy in tenants that synchronize data to the MAT platform, not under the direct control of 40Factory.

Disaster recovery testing

To ensure effective backup procedures and data availability when needed, **the organization conducts recovery tests at least once a year and after significant infrastructure changes; the status of backups is also checked every six months.** These simulations make it possible to verify the consistency and integrity of the saved data, as well as ensuring the operational readiness of the technical team in the execution of recovery activities.

Back-ups follow the encryption and data management policy in line with all other data managed by the organization.

5.9 Encryption by default

The organization has adopted cryptographic technologies made available for storage by the cloud service provider:

Azure Storage data is transparently encrypted and decrypted with AES 256-bit encryption, one of the strongest block ciphers available, FIPS 140-2 compliant.

Encryption configured according to the *security by default principle:*

- Azure Storage encryption is enabled for all storage accounts, including Resource Manager and classic storage accounts.
- Azure Storage encryption can't be disabled.
- Because your data is protected by default, you don't need to change your code or applications to take advantage of Azure Storage encryption. Data in a storage account is encrypted regardless of the performance tier (standard or

premium), access tier (hot or cool), or deployment model (Azure Resource Manager or classic).
- All new and existing block blobs, append blobs, and page blobs are encrypted, including blobs in the archive access tier.
- All Azure Storage redundancy options support encryption, and all data in the primary and secondary regions is encrypted when geo-replication is enabled.
- All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted.

For more information about the cryptographic modules underlying Azure Storage encryption, see Encryption API: Next Generation.

For information about encryption and key management for Azure managed disks, see Server-side encryption of Azure managed disks.

5.10 Segregation and isolation

The 40Factory infrastructure for the provision of cloud services is defined so as to ensure the segregation of the data and resources of individual customer instances. Each MAT customer environment runs in a dedicated isolated space (Kubernetes namespace), created, updated and decommissioned exclusively through pipelines and an orchestrator managed by the DevOps team, under the responsibility of the DevOps Manager. MAT customer data reside in the cloud resources of the customer's tenant (IoT Hub, storage, Entra ID and, where the CMMS module is included, SQL database) and are never copied to 40Factory resources.

5.11 Managing virtual networks

Virtual network segregation is adopted as a security measure in 40Factory solutions for the separation of individual software instances released to customers.

The configuration and management of virtual networks in our cloud environments follows security principles that align with policy guidelines.

- Each virtual network is segmented to isolate the different environments (development, test, production) and minimize exposure to risks.
- In the Kubernetes clusters each customer environment is isolated in its own namespace; external traffic goes through a single entry point with TLS encryption and a web application firewall.
- Access to network resources is tightly controlled through a dedicated firewall, granular security rules, and continuous traffic monitoring.
- The principle of minimum access necessary is also applied at the network level, ensuring that data flows are only authorized if explicitly provided.
- Configurations are subject to periodic review to ensure consistency with security and privacy requirements.

5.12 Secure Development Management

The organization takes **a structured approach to software development that integrates cybersecurity principles into all phases of the lifecycle of its digital products and services.** The goal is to ensure that the solutions provided are designed and implemented to minimize information security risks.

- Development follows a **Secure Software Development Lifecycle (SSDLC)** model. Each phase – from requirements analysis to design, from development to production – includes dedicated security controls for the identification and mitigation of vulnerabilities.
- The source code is peer-reviewed and, when appropriate, dynamic testing. These activities allow errors or vulnerabilities to be detected at an early stage, intervening before production is put into production.
- The development, test, and production environments are **physically and logically separated**. Access to each environment is controlled and tracked, reducing the risk of unauthorized changes or contamination between environments.
- Each change to the software is subject to a formalized **change management** process, which includes documentation, approval and verification via pull request. Changes are tested in staging environments before final release.
- Development teams receive **ongoing training** on secure development best practices, including major known vulnerabilities (e.g., OWASP Top 10) and mitigation techniques.

5.13 Protecting customer data

The protection of customer data is a key priority, ensured through advanced technical and organisational measures throughout the entire management cycle.

- Data is processed in secure cloud environments, with segregation processes that ensure a clear separation between production, test and development environments.
- In production, each customer operates in a logically isolated environment to prevent unauthorized access and ensure the confidentiality of information. Real customer data is never used outside the production environment and for purposes other than the provision of the services offered, guaranteeing their confidentiality.
- Periodic vulnerability tests are performed on all components that handle sensitive data, with particular attention to exposure surfaces and access controls. Any vulnerabilities identified are managed according to structured remediation and traceability procedures. All activities comply with the requirements of applicable international regulations on security and data protection.

Access to customer data by support staff is granted solely for the provision of the **various services performed**. Specifically:

- **MAT Customer data**, permission managed by *the customer's system administrator.* Access is requested from the customer exclusively for 40Factory personnel involved in the development of the project. The access procedure is managed by invitation of the company account of 40Factory staff; therefore, in the event of revocation of the company user, the permits will be automatically revoked.
- **MAT Customer Configuration files**, permission managed by the *MCC Administrator*. Access is granted to personnel involved in the project management and configuration of the customer's data models. Access permissions are managed by invitation to the company account of 40Factory staff, so in case of revocation of the company user the permissions will be automatically revoked.

- **Wilson Customer data**, permission managed by *Wilson Administrator*. Access is granted to 40Factory personnel involved in project management and configuration of customer tenants.

5.14 Customer data labeling

The cloud software services offered by 40Factory provide for **the management of uploaded customer information through labeling services**. The details of these product features are defined in the released **product documentation,** which is accessible to the users themselves.

5.15 Deletion of customer data

The software services offered by 40Factory include **data deletion management.** This management provides for the deletion of data in a secure mode that does not allow the recovery of deleted data either to the customers themselves, or to 40Factory, or to the provider of the cloud services used by 40Factory.

In addition, the customer can request the **deletion of software configuration data**, **this activity is managed directly by 40Factory staff**. This deletion process involves the secure deletion of the data itself, which can therefore no longer be recovered, neither by customers, nor by 40Factory, nor by the cloud service provider used by 40Factory.

5.16 Synchronizing Clocks

All cloud resources are configured to use **centralized time synchronization systems based on standard** protocols such as NTP (Network Time Protocol). System time is consistently aligned with trusted reference sources, ensuring consistency across system logs, security events, and distributed processes. This synchronization is critical for the integrity of audit activities, incident detection, and event correlation between interdependent services. **The synchronization mechanisms are monitored and subject to periodic checks** to detect any discrepancies or malfunctions. Time accuracy is an integral part of the security posture of your cloud infrastructure.

The *time server* configured for cloud services is *time.windows.com*.

5.17 Utility programs

40Factory does not directly provide utility programs for access to the cloud services offered. However, cloud services require **customers to use APIs.** These APIs are provided in accordance with the security levels of the services offered and the operations performed through utility programs are tracked by the cloud applications themselves.

Customers are therefore responsible for the correct implementation of the utility programs they define to protect the data and services available on 40Factory applications.

6 Supplier selection and monitoring

6.1 Evaluation and monitoring criteria

The vendors used by 40Factory for cloud services must meet the security requirements defined by the organization, ensure the confidentiality of the data processed, the geolocation of the data in accordance with the defined requirements and the contractual SLAs.

In the evaluation and selection of vendors and for their monitoring over time, the organization has defined and applies guidelines with a performance evaluation process and criteria, especially for cloud service providers.

The process follows a sequence of activities: RISK ASSESSMENT, SCREENING, AGREEMENT, ACCESS CONTROL, MONITORING, TERMINATION.

In the Cloud Service Provider Assessment SCREENING, the following requirements apply:

- CERTIFICATIONS
- ROLES AND RESPONSIBILITIES
- SERVICE LEVEL
- DATA ENCRYPTION
- BACKUP E RECOVERY
- AUDIT E LOGGING
- GDPR
- VULNERABILITY AND INCIDENT MANAGEMENT
- ACCESS CONTROLS
- DATA GEOLOCATION
- DATA PROTECTION AND OWNERSHIP
- AVAILABLE DOCUMENTATION AND COMMUNICATION
- SECURE DEVELOPMENT

6.2 Cloud provider platforms currently used

Currently, cloud services are provided through the use of the services of the platforms:

Microsoft Azure – below are references to the vendor's documentation regarding the requirements indicated:

- Azure customer data protection
- Azure GDPR
- Azure certifications

Atlassian – below are references to the supplier's documentation regarding the requirements indicated:

- Atlassian Certifications

Gitbooks – below are the references to the supplier's documentation regarding the requirements indicated:

- Gitbook Certifications

Scaleway – compute infrastructure (Kubernetes clusters) for the MAT environments, with data centres in the Netherlands (Amsterdam) and France (Paris): supplier references on certifications and data protection.

- Scaleway security and compliance
- Scaleway privacy policy (GDPR)

Google Cloud – generative AI services (Gemini models on Vertex AI, processed in an EU region) used by MAT AI Agents and Wilson.ai: supplier references on data governance and certifications.

- Google Cloud – Vertex AI data governance
- Google Cloud – Vertex AI data residency
- Google Cloud GDPR
- Google Cloud certifications

6.3 Data geolocation

The company has defined the geographical locations allowed for the provision of cloud services such as:

- Italy
- European Union: Microsoft Azure West Europe (Netherlands); Microsoft Azure OpenAI West Europe, Italy North and Sweden Central; Scaleway Amsterdam and Paris; Google Vertex AI in an EU region

7 Responsible use of AI

The company adopts artificial intelligence (AI) solutions with the aim of improving the efficiency of services, optimizing processes and offering advanced features to its customers, keeping transparency, security and ethics in the use of these technologies as a priority.

All AI-based systems undergo a rigorous pre-assessment to ensure compliance with the following key criteria:

7.1 Functionality and Reliability

Every AI solution must meet clear requirements in terms of performance, robustness, explainability of results, and traceability of automated decisions. Models are selected and trained according to well-defined objectives and tested on realistic scenarios to evaluate their effectiveness before putting them into production.

7.2 Confidentiality and Data Protection

The data used for training, inference or processing of AI models is handled in full confidentiality. Customer data is never used without an adequate legal basis, explicit consent, or contractual necessity. All data is processed in accordance with the applicable regulations on the protection of personal data, and pseudonymization, minimization and segregation measures are adopted when applicable.

7.3 Alignment with the Organization's Code of Ethics

Every AI system must be consistent with the organization's core values: fairness, inclusiveness, accountability, respect for human dignity, and non-discrimination. The use of algorithms is also evaluated from an ethical point of view, excluding solutions that may introduce unjustified biases, discriminatory effects or unverifiable automatisms. There is an

internal ethical approval process for all relevant AI projects, supported by a dedicated committee.

7.4 Human Supervision and Control

The AI solutions adopted never operate completely autonomously in critical contexts. Responsible human supervision is always provided, with the possibility of intervention and verification of automatic decisions. Customers have the right to know when a function or decision is assisted by AI, according to the principles of algorithmic transparency.

7.5 Continuous Monitoring and Audit

AI models and systems are subject to continuous monitoring and periodic audits to assess effectiveness, identify behavioral deviations, update datasets, and verify continued adherence to safety and ethical compliance criteria.

7.6 References for AI cloud services used

References are made to the services used by the organization for the provision of its AI services. MAT AI Agents and Wilson.ai use language models provided as cloud services by Microsoft Azure OpenAI and by Google (Gemini on Vertex AI), run in European Union regions and selected according to the task; customer data sent to the models are used only to produce the requested answer and not to train the models.

- Microsoft Enterprise AI Service of Conduct
- AI Azure privacy
- Google Cloud – Vertex AI and Gemini: data governance and privacy

8 Change Management

40Factory adopts a structured change management process for the updating, modification and disposal of its software products and services, which is integrated into the documented Product Lifecycle Management processes of the systems offered to the market.

Specifically, categories of changes and methods of communication to customers are defined.

8.1 Categories of changes

The types of modifications defined on 40Factory products are:

- Application Version Update
- Security Hot Fix
- Termination of License

8.2 Methods of communication to customers.

Communications regarding updating and modification activities take place through scheduled newsletters to individual customers. During the project start-up phase, the mailboxes of the customers receiving these communications are defined.

The following types of communication are therefore defined:

- Preventive start of updating activities, modification. It contains information regarding the expected date and time of the update as well as any downtime.
- Completion of upgrade or modification tasks, contains information about the changes that have been released, and references to technical documentation.
- Notification for temporary disservice.
- Notification for the restoration of the outage.

8.3 Termination of License

40Factory adopts procedures for managing the termination of license agreements, at the request of the customer, as defined in the supply agreement. These activities are managed by the DevOps Manager and the IT manager and 40Factory staff will be responsible for:

- Remove all customer-assigned users and privileges in 40Factory cloud environments.
- Dispose of the resources allocated to the customer.
- Securely erase data logged on 40Factory services. Such data cannot be retrieved in any way as defined in the contractual conditions
- Remove any documents and project files entrusted by the customer to 40Factory.

The following data removal timelines have been defined to allow the customer to recover them:

- **After 5 days and within 10 business days**: Removal of operational data from active systems
- **After 30 days and within 60 working days**: removal of data from back-up systems

Following the deletion of the data, it will no longer be possible to recover them in any way.

8.4 Critical Operations Management and Documentation

40Factory has defined the methods of providing documentation for the management of critical operations by customers. This documentation is provided for all 40Factory products on the Gitbook platform. The available documentation is accessible on the following portals:

- MAT Documentation
- Wilson documentation
- MAT Control Center Documentation

Following the "L2 Application Engineer training", provided by 40Factory, customers will also have access to the "AE Guide" Gitbook portal. Access to this documentation is provided by 40Factory and reserved for personnel chosen by the customer: the access user is personal and non-transferable.

This approach provides customers with the tools to be aware of the management of critical operations in the software applications provided by 40Factory.

9 Vulnerability management

9.1 Scope and application

Vulnerability management applies to:

- Operating systems and server environments (on-premise and cloud)
- Software and applications developed and/or managed by 40Factory
- Corporate devices and hardware assets
- Third-party components, including libraries, plugins, middleware, and external services

9.2 Identifying vulnerabilities

Vulnerabilities are identified through:

- Monitoring of authoritative sources (ACN Portal)
- Use of automated vulnerability scanning tools on a periodic basis
- Reports from suppliers in charge of scanning and penetration testing

9.3 Assessment and mitigation

The vulnerabilities identified are treated according to an action plan that may include:

- Patching or software updates
- Implementation of temporary workarounds
- Disabling vulnerable features
- Asset isolation pending resolution

Each intervention is tracked through the internal ticketing system (based on Jira), indicating the date of detection, assigned manager, status and closure date.

9.4 Verification and Monitoring

After resolution, the following are performed:

- Technical checks to ensure that the vulnerability has been properly mitigated
- Subsequent scans to confirm the absence of the vulnerability
- Continuous monitoring to avoid regressions

9.5 Communication and Notification

In the event of critical vulnerabilities involving customer data or configurations, 40Factory provides:

- Inform the affected customer in a timely manner
- Provide technical details and guidance on corrective measures taken
- Collaborate for any containment actions by the customer

10 Incident management

The following describes the incident management policies defined and documented in the organization's integrated management system.

10.1 Incident reporting and digital evidence request

The organization defines the following channels for reporting incidents:

- Jira Service Desk Ticketing Portal

Within the relevant product sections, the category relating to Cybersecurity incidents is defined. The customer is required to fill in all the mandatory fields regarding the description of the incident, the fundamental principles impacted by the incident and the organizational impact. The 40Factory Cybersecurity team will take charge of the request to solve the problem in the shortest possible time and in line with the defined service objectives.

Through the same portal, **it is possible to request related digital evidence that can be useful for managing an incident.**

10.2 Incident handling methods

40Factory has defined the processing modality as follows:

- **Incident management**: In the event of outages that compromise the availability of cloud services, the company applies a structured incident management process. Each incident is recorded, analyzed and resolved according to standardized procedures, in order to minimize the impact on service continuity.

- **Incident classification**: Incidents are classified according to their severity, **within 24 working hours of their reporting**, impact on services and nature of the event. This classification makes it possible to correctly assign the priorities of intervention and the necessary resources.

- **Tracking and resolution**: All phases of incident management (reporting, analysis, response, resolution) are tracked through an internal ticketing system, indicating responsibilities, impacts and corrective actions. In the event that the incident has a serious impact on the confidentiality of the data, this will be communicated to the competent national authority (ACN) or the designated CSIRT with the following timelines:

    - Within 24 hours: Prior notification
    - Within 72 hours: detailed notification
    - Within one month: final report
    - For products with digital elements, the reporting obligations of the Cyber Resilience Act (EU Regulation 2024/2847, art. 14) also apply to actively exploited vulnerabilities and severe incidents: early warning within 24 hours, notification within 72 hours and final report to ENISA and the national CSIRT, with information to the affected users.

- **Continuous improvement**: Each resolved incident is subjected to a post-event review with the aim of learning from experience and introducing any improvement actions into the processes or controls implemented.

10.3 Disaster recovery

In the event that the incident involves the need to activate the disaster recovery plan, 40Factory applies the measures provided for within its business continuity strategy. These measures include:

- **Activation of the DR plan:** Following the assessment of the incident by the technical team and the security manager, the disaster recovery plan is activated in cases where ordinary recovery is not sufficient to ensure the timely resumption of critical activities.
- **Restore data and services**: Restore is done from periodic backups, which are regularly audited and stored as defined in the backup plan. The goal is to ensure complete data recovery and service recovery within the timeframe defined in the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) parameters. In any case, the restoration takes place within two working days, unless the cloud providers are unavailable for an extended period.
- **Communication**: During the management of the event, timely and transparent communication to customers and interested parties is guaranteed, according to the channels and methods provided for in the company crisis plan.
- **Verification and validation**: At the end of the recovery operations, a verification of the integrity of the data and the full operation of the services is carried out. A post-event report is also drawn up with an analysis of the causes, the effectiveness of the actions taken and any areas for improvement.
- **Periodic tests**: The disaster recovery plan is tested at least once a year and after significant infrastructure changes, to ensure the effectiveness and readiness of the process in the event of a real disaster.

11 Use of customer data

40Factory accesses and uses customer data for the purposes of:

- Provide the services offered to customers
- Monitor the usage of your applications for optimizing cloud services.
- Measure customer adoption rate of applications
- Improve your products or services.

The organization will in no way share the data used or its processing with parties outside the organization.

12 Compliance with legal requirements

40Factory complies with all applicable territorial legal requirements; it has also defined a management system that complies with current regulations and adopted standards by defining and verifying compliance with the following legal requirements.

12.1 Certifications

- UNI EN ISO 9001 standard
- UNI CEI EN ISO/IEC 27001 standard
- UNI CEI EN ISO/IEC 27017 standard

12.2 Additional legal requirements

- GDPR Regulation (EU 2016/679)
- NIS2 Regulation (DL 138/2024 and EU 2022/2555)
  even if 40Factory is a non-in-scope entity as a supplier of companies in the field.
- EU AI Act Regulation (EU 2024/1689)

- Cyber Resilience Act Regulation (EU 2024/2847)
- Regulation Data Act (EU 2023/2854)

The company, analyzing the legal requirements currently in place, did not highlight specific requirements on the type of encryption implemented for the provision of the services offered.

13 Objectives level of service offered

For the provision of 40Factory services, the company has defined the following objectives, considering the technological stack used by the various services:

Service	SLA
MAT Cloud	99,5%
MAT Control Center	99,5%
Wilson Academy	99,5%
Wilson Stand-alone	99,5%

SLA values are determined by means of a system of continuous monitoring of the application instances in production. Uptime is calculated as the ratio of the time each application is operational to the total observation time, on an annual basis. The monitoring tools used automatically detect any service interruptions, as well as restarts or infrastructural problems that may impact the usability of the service.

14 Communication to and from customers

40Factory communicates activities related to the provision of services offered to customers for the following cases and in the manner defined:

Typology	Channel	Recipients
Updates MAT	email	Active MAT clients
MAT Outage	email	Active MAT clients
MAT Control Center updates and outages	email, MCC Transparency page	Active MAT clients
Updates Wilson	email	Wilson Active Customers
Wilson Outage	email	Wilson Active Customers

15 Third-Party IP Infringement Reports.

The company has defined that an Intellectual Property breach is part of the Cybersecurity incident reporting flow, so the reporting method is in line with that defined for incident reporting in this document:

- Jira Service Desk Ticketing Portal

16 Second-party audit policy

40Factory allows customers to perform second-party audits only after specific agreements and after agreed planning.

An NDA is required to be signed by the customer who can request and consult the periodic audit report performed by the company.

17 Conclusion

This document establishes a clear guideline for managing licensing agreements with 40Factory, promoting transparency, accountability, and information security.