DATA RETENTION POLICY

"INNOVATION IS THE ABILITY TO SEE CHANGE AS AN OPPORTUNITY, NOT A THREAT."

TABLE OF CONTENTS

Purpose and Definitions

Changes introduced compared to the previous release

Version / Release No.	3.2
Version / Release Date	17/03/2025
Modified by	Luca Scuriatti

Purpose and Main Objectives

This document provides a summary of the measures implemented by **Openapi S.p.A.** in compliance with the **GDPR** and has been prepared to provide customers with comprehensive information regarding the **use, retention, and deletion of their data**.

Certain information has been limited for **corporate protection and security reasons**. Upon request, and where possible, additional details may be provided to interested parties.

Key Points

This document provides a summary of all the measures implemented by **Openapi S.p.A.** to ensure the proper management of data.

By its very nature, **IT systems management and data protection are continuously evolving and improving**. Customers will therefore be notified of any significant changes and will receive an annual copy of this document to keep them updated on the current status of the technologies and measures in place.

This document does not cover data that, by law, must be retained within **Openapi S.p.A. systems** (e.g. accounting records, tax data, contract signatures, etc.). Its purpose is purely informational and is intended to facilitate and simplify collaboration with customers.

GDPR – Measures Implemented

In compliance with **Art. 31 – Security Obligations**, personal data undergoing processing is stored and controlled, also taking into account the knowledge acquired through technological progress, the nature of the data, and the specific characteristics of the processing. Appropriate preventive security measures are adopted to minimise the risks of destruction or loss, including accidental loss, unauthorised access, or processing that is unlawful or inconsistent with the purposes for which the data was collected.

This section describes the database access rules and the security policies adopted.

Access to resources is divided into two functional groups:

- gcp-grp-operators
- gcp-grp-developers

ACCESS TO THE MAIN DATABASE

Access to production data is permitted only to authorised technical personnel belonging to the gcp-grp-developers group.

Access is allowed only after the individual user has been authorised through the provider's dedicated platform (**MongoDB**).

Users must first request authorisation through **two-factor authentication (2FA)** using their corporate account (**Google Workspace**). They must then authorise the IP address associated with their workstation. This authorisation remains valid for **6 hours**.

ACCESS TO FILE-BASED DATA

Access to file-based data is permitted to authorised technical personnel and after-sales support staff belonging to the gcp-grp-operators and gcp-grp-developers groups.

Only members of the gcp-grp-developers group are authorised to modify data for technical purposes.

DOCUMENT ENCRYPTION RULES

For the most sensitive documents, Openapi uses the following encryption model, currently considered the most effective method for protecting and obfuscating document content:

Encryption type: Hybrid
Asymmetric component: RSA key with 3072 bits
Symmetric component: AES-256-GCM (Rijndael)

DATABASE / SERVER LOCATION

The main database is hosted as a managed **MongoDB Atlas** service by MongoDB, Inc. within the **Google Cloud** platform in the europe-west1-b zone (**Saint-Ghislain, Belgium, Europe**), as a cluster of three servers interconnected via VPN with the main private network hosting the applications.

File-based data is stored using **Google Cloud Storage** in the same europe-west1-b zone, in compliance with **EU Regulation 2016/679**.

DATA ENCRYPTION

Only encrypted connections using SSL certificates provided and managed by **Google Trust Services LLC** are enabled on Openapi servers.

ENCRYPTION AT REST

Cloud Storage: All data stored in Cloud Storage is encrypted at rest using the **AES-256** algorithm.

Cloud SQL: Cloud SQL databases are encrypted at rest using the **AES-256** algorithm.

MongoDB Atlas: MongoDB databases are encrypted at rest using the **AES-256** algorithm.

Secret Manager: Uses **AES-256 encryption** to protect stored credentials.

ENCRYPTION IN TRANSIT

Traffic between clients and the load balancer: HTTPS with Google TLS/SSL certificates issued and managed by **Google Trust Services LLC**.

Traffic between the load balancer and internal infrastructure components:

- **Cloud Run:** Communications between Cloud Run and clients are encrypted using **TLS 1.2**.
- **Cloud Functions:** Communications between Cloud Functions and clients are encrypted using **TLS 1.2**.

Traffic between internal infrastructure components:

- **Cloud SQL:** Communications between application instances and the Cloud SQL database are encrypted using **TLS 1.2**.
- **Memcached:** Communications between application instances and Memcached are encrypted using **TLS**.
- **MongoDB Atlas:** Communications between application instances and MongoDB Atlas are encrypted using **TLS 1.2**.

DISASTER RECOVERY

Please refer to the internal document: **Privacy – Disaster Recovery Plan**.

FIREWALL AND ANTIVIRUS

Implementation of the following rules at load balancer level (**Google Cloud Armor**) and DNS level through a proxy tunnel (**Cloudflare**):

- Rate limiting
- Web Application Firewall (WAF) based on OWASP
- Adaptive Layer 7 DDoS protection
- Bot detection

INTRUSION DETECTION – PENETRATION TESTING

Google Cloud IDS (Cloud Intrusion Detection System) has been implemented to detect malware, spyware, command-and-control attacks, and other network-based threats.

An agreement is in place with a leading cybersecurity company to conduct **automated quarterly security tests and annual penetration tests**, according to varying schedules.

APPOINTMENT OF THE DPO

Our **Data Protection Officer (DPO)** has been formally communicated to the competent Data Protection Authority in accordance with **Art. 9 of the GDPR**.

To ensure the proper provision of our services, we regularly raise awareness among and train our employees and apply a **“privacy by design”** and **“privacy by default”** approach, particularly when developing new initiatives and services for customers. The DPO also oversees relations with the relevant supervisory authorities.

TERMINATION OF DATA PROCESSING

If data processing is terminated at the customer’s request, including a request submitted simply by email, personal data is deleted from the relevant application.

Where the data relates to a commercial transaction, it may continue to be retained for **tax purposes** or, where applicable, for **statistical purposes**, after being appropriately dissociated from the user profile (**Article 16 of the Code**).

GDPR – DATA RETENTION POLICY

OPENAPI S.r.l. (hereinafter also referred to as "**OPENAPI**" or the "**Data Controller**"), in compliance with Article 5(1)(e) of European Regulation 2016/679 (hereinafter, the **GDPR**) regarding data retention (so-called "***data retention***")[1], hereby sets out the maximum retention periods and/or the criteria used to determine the retention period for the personal data of data subjects whose data is processed, including employees and equivalent personnel, customers, suppliers (including potential suppliers), etc. (hereinafter, the "**Data Subjects**").

The Data Controller intends to retain the personal data processed in compliance with the principles established by the GDPR and by Italian Legislative Decree No. 196 of 30 June 2003, as amended by Legislative Decree No. 101 of 10 August 2018 (hereinafter, the "**Privacy Code**").

Accordingly, the Data Controller ensures that the retention period is proportionate to the purposes for which such data was collected. This makes it possible to retain only information that continues to have legal relevance or has acquired historical value, while deleting documentation that is no longer considered necessary in relation to the purposes for which it was originally collected.

1. Definitions

"Data Controller": the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In this specific case, the Data Controller is **OPENAPI Italy S.r.l.**

"Data Subject": the natural person to whom the personal data relates. By way of example and without limitation, Data Subjects may include:

- an employee or equivalent personnel;
- a customer or supplier;
- users who, for various purposes, browse OPENAPI websites or websites managed by OPENAPI;
- candidates for potential job positions;
- recipients of various commercial communications.

"Personal Data": any information relating to an identified or identifiable natural person ("Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity.

“Processing”: any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, **storage**, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2. Data Retention Criteria

OPENAPI determines data retention periods in accordance with the applicable laws and regulations governing the processing of personal data. In particular, personal data is retained:

- for the period required by applicable administrative, tax, contractual, employment and other relevant laws and regulations;
- for the period strictly necessary to achieve the purposes for which the personal data was collected, in accordance with the principles of data minimisation and lawfulness of processing. Therefore, where the same data is processed for different purposes, the Data Controller establishes different retention periods according to each specific purpose;
- for the proper management of the business and, more generally, of the commercial activities set out in the company’s Articles of Association;
- with regard to certain categories of data, for the purpose of protecting OPENAPI’s interests and preserving documentary evidence in the event of legal disputes, also taking into account the applicable limitation periods for bringing legal proceedings;
- further details are available in the **Record of Processing Activities**.

[1] Article 5(1)(e): *“1. Personal data shall be […] (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’).”*

GDPR – AFFILIATES AND SUB-PROCESSORS

This document contains a list of **sub-processors** that OPENAPI may engage to support the provision of Services to its customers. Depending on the products and services provided, some or all of these sub-processors may be involved in the processing activities described.

As specified in the **General Terms and Conditions (GTC)** and in the **Data Processing Agreement (DPA)**, the customer authorises **Openapi S.p.A.** to engage the appointed sub-processors, where necessary, for the purpose of providing the requested service.

In the event of a change of supplier or sub-processor, customers will be **informed in advance** of the upcoming change.

Supplier Name	VAT Number
Innolva Spa	01836920304
younique business srl	01739090460
I-Reputo srl	03808010981
Smart Business Solution	01402410771
Sevendata Spa	10107290966
Infocert Spa	07945211006
Namiral Spa	02046570426
Aruba Spa	01573850516
Yousign srl	12318380966
Mcloud ltd	GB226312538
Google ltd	IE6388047V
Infocamere Spa	02313821007
Agenzia delle Entrate	06363391001
Trust Srl	03470460928
SD Srl (non solo patronato)	03153930809
Caf e patronato online	04502430657
Geometra De Marinis Gianluca	01403900556
Studio Borghese BBM EUROMAX	09161331005

STIPEL SRL	02725720276
Mongo db ltd	IE9793087U
CRIF SPA	01691720468
YoUnique Business Srl	01739090460
Abbrevia Spa	01978010229
ATUB Associazione Consumatori	97786780011
Svanera Giovanna	02542840984
Obiettivo Impresa Srl	01761590569
GLOBAL FEV S.A.S.	02697600035
STUDIO LO CONTE ENRICO	12201941007
Servizi Informativi Srls	03728230834
Injenia Srl	03008670360
iospedisco	05501000870
A-Cube srl	10442360961
Toc Toc srl	12925931003
Poste Italiane Spa	01114601006
Postel srl	05692591000
Infobip srl	07579600961
Infinite Loop Development Ltd.	IE6409820U
Eurocredit Business Information srl	07693660966
Borsino Service srl	14476731006
Sanguinetti Editore spa	04156070155
Checkout	
SGR Compliance SA	CHE-112.339.606