



GDPR, DATA RETENTION POLICY & DPA

"Innovation is the ability to see change as an opportunity, not a threat."

Version / Release No.: 4.0

Version / Release Date: 30-09-2026

Modified by: Legal & Privacy Department

TABLE OF CONTENTS

1. Purpose and Definitions	2
2. Security Obligations (Art. 32 GDPR)	2
3. Obligations of the Data Processor (Art. 28 GDPR)	3
4. Data Retention Policy and Termination of Processing	4
5. GDPR – Affiliates and Sub-Processors (Art. 28, para. 2)	4



Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.

Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

1. Purpose and Definitions

Purpose and Key Objectives

This document summarizes the measures implemented by Openapi S.p.A. in compliance with the GDPR (EU Regulation 2016/679) and serves as a **Data Processing Agreement (DPA)** pursuant to **Article 28 of the GDPR**.

It has been prepared to provide customers with all relevant information regarding the use, retention, protection, and deletion of data.

Certain strictly technical information has been minimized for corporate security and protection purposes. However, further details may be provided upon request to interested parties.

1.1 Privacy Roles (Art. 28 GDPR)

For the purpose of providing the services, the parties assume the following roles:

- Customer (Data Controller): Determines the purposes and means of processing the personal data entered and processed through Openapi platforms.
- Openapi S.p.A. (Data Processor): Processes personal data exclusively on behalf of the Customer and in accordance with the Customer's documented instructions, solely for purposes strictly related to the provision of the requested services. *(Note: For certain services, Openapi acts as an independent Data Controller pursuant to its TULPS licence and the related legal requirements.)*

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

2. Security Obligations (Art. 32 GDPR)

In compliance with applicable security obligations, personal data is stored and controlled in a manner designed to minimize the risks of destruction, loss, unauthorized access, or unlawful processing.

Database Access Rules and Confidentiality

Access to resources is divided into two functional groups: **gcp-grp-operators** and **gcp-grp-developers**.

Access to production data is permitted only to authorized technical personnel. Access must be requested in advance through the MongoDB platform and requires **Google Workspace two-factor authentication (2FA)** and **IP whitelisting**, with access granted for a maximum period of **6 hours**.

All personnel authorized by Openapi to process data are legally bound by confidentiality obligations and receive ongoing training on personal data protection.

Data Encryption

- Hybrid encryption model for sensitive documents: RSA asymmetric key (3072 bits) and AES-256-GCM (Rijndael) symmetric encryption.
- Encryption at rest: Data stored in Cloud Storage, Cloud SQL, MongoDB Atlas, and Secret Manager is encrypted using the AES-256 algorithm.

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

GDPR - AFFILIATE AND DPA

- **Encryption in transit:** HTTPS with TLS/SSL certificates (Google Trust Services LLC) and TLS 1.2 for internal traffic between instances (Cloud Run, Cloud SQL, Memcached, etc.).

Database / Server Location

The primary infrastructure (MongoDB Atlas and Google Cloud Storage) is hosted within the Google Cloud platform in the “**europa-west1-b**” zone (Belgium, Europe), ensuring that data remains within the **European Economic Area (EEA)**.

Firewall, Antivirus and Intrusion Detection

- Implementation of **Google Cloud Armor** (rate limiting, WAF with OWASP rules, Layer 7 DDoS protection, and bot detection).
- Implementation of **Google Cloud IDS** for malware and network threat detection.
- Annual penetration testing and quarterly automated security testing carried out by leading cybersecurity companies.

3. Obligations of the Data Processor (Art. 28 GDPR)

In its capacity as Data Processor, Openapi S.p.A. ensures compliance with the following regulatory obligations:

3.1 Assistance to the Data Controller (Data Subject Rights and DPIA)

Openapi assists the Customer, through appropriate technical and organizational measures, in fulfilling requests from data subjects to

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

exercise their rights, including **access, rectification, erasure, and data portability**.

Openapi also provides support to the Customer where the latter is required to carry out a **Data Protection Impact Assessment (DPIA)**

3.2 Data Breach (Personal Data Breach)

In the event of a personal data breach involving data processed on behalf of the Customer, Openapi undertakes to notify the Customer (Data Controller) promptly and without undue delay after becoming aware of the breach, and in any event within **48 hours**. This enables the Customer to comply with its obligation to notify the competent Supervisory Authority within the **72-hour period** required by the GDPR.

3.3 Right to Audit and Inspection

Openapi provides Customers with the information necessary to demonstrate compliance with the obligations set out in **Article 28 of the GDPR**. For security reasons related to the shared cloud infrastructure, the right to audit is normally deemed satisfied through the provision of security reports, penetration test summaries, and company certifications (e.g. **ISO 9001, adherence to the CISPE Code of Conduct**).

4. Data Retention Policy and Termination of Processing

The Data Controller intends to retain data in accordance with the

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy

REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007

Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

GDPR – AFFILIATE AND DPA

principles of **data minimization and storage limitation**, ensuring that retention periods are proportionate to the purposes for which the data was collected. Where the same data is processed for different purposes, the specific retention periods required for each purpose will apply.

Termination of Processing (Art. 28(3)(g))

In the event of termination of the service agreement, or upon the Customer's written request, Openapi will delete or return the personal data within **30 days**, except for data that must be retained in accordance with applicable legal obligations.

The data will be deleted from the application. The only information retained will be data subject to statutory retention requirements for tax and accounting purposes, or statistical data that has been previously anonymized and irreversibly dissociated from the user profile.

5. GDPR – Affiliates and Sub-Processors (Art. 28(2))

To ensure the proper provision of the services, the Customer authorizes Openapi S.p.A. to engage the sub-processors listed in the table below.

Right to Object: In the event that a sub-processor is added or replaced, Openapi will inform the Customer at least **15 days in advance**. If the Customer wishes to object to such change on valid

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

GDPR - AFFILIATE AND DPA

data protection grounds, it may notify Openapi accordingly. Where no alternative technical solution is available, the Customer shall have the right to terminate the agreement.

List of Authorized Sub-Processors:

SUPPLIER NAME – VAT NO.	TAX IDENTIFICATION NUMBER
Innolva S.p.A	01836920304
Younique Business S.r.l.	01739090460
1-Reputo S.r.l.	03808010981
Smart Business Solution S.r.l	01402410771
Sevendata S.p.A	10107290966
Infocert S.p.A.	07945211006
Namirial S.p.A.	02046570426
Aruba S.p.A.	01573850516
Yousign S.r.l.	12318380966
Mcloud Ltd	GB226312538
Google Ltd	IE6388047V

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

GDPR - AFFILIATE AND DPA

SUPPLIER NAME - VAT NO.	TAX IDENTIFICATION NUMBER
MongoDB Ltd	IE9793087U
Infocamere S.p.A.	02313821007
Agenzia delle Entrate	06363391001
Trust S.r.l.	03470460928
SD S.r.l. (non solo patronato)	03153930809
Caf e patronato online	04502430657
Geometra De Marinis Gianluca	01403900556
Studio Borghese BBM EUROMAX	09161331005
Stipel S.r.l.	02725720276
CRIF S.p.A.	01691720468
Abbrevia S.p.A.	01978010229
ATUB Associazione Consumatori	97786780011
Svanera Giovanna	02542840984
Obiettivo Impresa S.r.l.	01761590569

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

GDPR - AFFILIATE AND DPA

SUPPLIER NAME - VAT NO.	TAX IDENTIFICATION NUMBER
Global Fev S.a.s.	02697600035
Studio Lo Conte Enrico	12201941007
Servizi Informativi S.r.l.s.	03728230834
Injenia S.r.l.	03008670360
iospedisco S.r.l.	05501000870
A-Cube S.r.l.	10442360961
Toc Toc S.r.l.	12925931003
Poste Italiane S.p.A.	01114601006
Postel S.r.l.	05692591000
Infobip S.r.l.	07579600961
Infinite Loop Development Ltd	IE6409820U
Eurocredit Business Information S.r.l.	07693660966
Borsino Service S.r.l.	14476731006
Sanguinetti Editore S.p.A.	04156070155

Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.



Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015

GDPR - AFFILIATE AND DPA

SUPPLIER NAME - VAT NO.	TAX IDENTIFICATION NUMBER
Checkout	FR69838307775
SGR Compliance SA	CHE112.339.606



Openapi S.p.A. Company subject to the direction and coordination of Open Holding S.p.A.

Viale Filippo Tommaso Marinetti 221 - 00143 Rome, Italy
REA No. 1378273 - Share Capital €50,000.00 fully paid-up - VAT No. IT12485671007
Company with a quality management system certified by Istituto Giordano - UNI EN ISO 9001:2015