

**SELECT SERVICE PARTNER RESTAURANTS HELLAS SINGLE-MEMBER S.A.
PERSONAL DATA RECORDING POLICY VIA VIDEO SURVEILLANCE SYSTEM ("CCTV")**

1. General

This "PERSONAL DATA RECORDING POLICY VIA VIDEO SURVEILLANCE SYSTEM" (hereinafter the "Policy") describes the terms and conditions under which a video surveillance system (hereinafter the "CCTV System") has been installed and operates at the business premises of the company under the name "SELECT SERVICE PARTNER RESTAURANTS HELLAS SINGLE-MEMBER S.A.", trading as "SSP", headquartered at Athens International Airport, Building 11 – Office 2/I132, 19004, Tax ID No. 099351845 and GEMI No. 006681301000 (hereinafter "SSP"), by SSP itself.

The purpose of this Policy is to inform visitors/users/customers/contracting parties/employees at SSP's premises (hereinafter the "Users") about the processing of their personal data through the CCTV System. It also describes Users' rights regarding the protection of their personal data and explains what kind of personal information SSP collects in this context and how such data is managed.

2. Scope – Purpose of Processing

The CCTV System records the movements of Users entering/moving within/remaining in SSP's premises, as follows:

- The CCTV System is installed solely for the protection of persons and property.
- Specifically, it consists of permanently installed cameras recording areas where SSP operates, aiming to prevent criminal acts against the company's assets and property rights (e.g. theft, embezzlement), as well as to safeguard the life, physical integrity, health, and property of Users present in the monitored areas.
- The CCTV System is not used to monitor SSP employees at their workplace for evaluation, supervision, or training purposes, nor to track Users' behavior or habits.
- The CCTV System does not record sound.
- SSP processes only strictly necessary data (data minimization), meaning only image data is collected and recording is limited to areas where there is an increased likelihood of unlawful acts (e.g. theft).

- Under no circumstances are cameras focused in a way that excessively interferes with Users' private life or personal data.
- SSP does not further process the collected data for purposes other than those described above.

3. Data Controller

SSP is the Data Controller of your personal data collected through the CCTV System, in accordance with Regulation (EU) 2016/679 (GDPR), Greek Law 4624/2019, relevant guidelines of the Hellenic Data Protection Authority (HDPa), and the European Data Protection Board guidelines.

SSP has placed appropriate signage in monitored areas informing Users about CCTV recording and providing contact details for submitting requests regarding personal data processing (see section 9).

4. Legal Basis for Processing

The legal basis for processing personal data via CCTV is Article 6(1)(f) GDPR (legitimate interests). Processing is necessary to protect SSP's and Users' assets, as well as their life, physical integrity, and health.

Following a balancing test between Users' rights and SSP's legitimate interests, the latter prevail, particularly regarding security and protection against unlawful acts.

5. Data Processing – Authorized Personnel

Access to recorded material is restricted to specifically authorized SSP employees. Live monitoring is also limited to designated authorized personnel.

These employees are bound by confidentiality obligations and are aware of the purpose and lawful use of the data.

Personal data is not disclosed to third parties without Users' consent, except where required by law or by competent authorities (e.g. judicial, prosecutorial, or police authorities).

6. Recording Method – Retention Period

The CCTV System uses dome-type cameras (DAHUA models, etc.) operating since May 1, 2026.

- Data consists of visual recordings stored in a secured SSP-controlled area.
- Access is restricted to authorized personnel.

- Data is transmitted in real time and stored digitally using compression algorithms.

Retention periods:

- 15 working days (standard retention)
- 30 days in case of incidents involving SSP
- 3 months in case of incidents involving third parties

After these periods, data is deleted.

7. Data Security Measures

SSP applies the following security measures:

- Antivirus protection on systems
- Physical security of equipment
- Access control via passwords
- Periodic review of access rights
- Regular system maintenance
- Cybersecurity policies implementation

These measures are regularly updated to ensure maximum data protection.

8. Data Transfers

Personal data may be shared with third parties (e.g. legal advisors) only when necessary and under confidentiality obligations.

Data may also be disclosed to authorities or involved parties when required by law or for legal claims.

9. Data Subjects' Rights

Users have the following rights (under conditions):

- Right of access
- Right to data portability
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to object (subject to limitations)

Requests can be submitted via email to: **gdpr.gr@sspeeme.com**

- Access/erasure requests: response within 15 working days
- Other rights: response within 30 working days (extendable)

Users may also file a complaint with the Hellenic Data Protection Authority.

10. Policy Updates

SSP reserves the right to amend this Policy at any time. Updates will be posted on:

<https://www.foodtravelexperts.com/our-markets/europe/greece/>

Users are encouraged to review the Policy regularly.

Last updated: 27/04/2026