

Data Protection Policy

Document control

Item	Value
Organisation	TotalView Ltd, Ethnarchou Makariou 44, 121 32 Peristeri, Greece
Version	2.0
Effective date	28 September 2026
Next review	September 2027
Owner	Management of TotalView Ltd
Data Protection Contact	George Keradinidis
Classification	Public

Version	Date	Change
2.0	30/01/2026	Full revision: Data Protection Contact role replaces DPO reference; controller and processor roles; Greek law; RoPA and DPIA; breach handling as processor; data subject request procedure
1.0	31/01/2021	First issue

1. Purpose and scope

This policy sets out how TotalView Ltd ("TotalView") collects, uses, protects and deletes personal data in line with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and Greek data protection law.

TotalView provides satellite imagery sourcing and delivery, Earth Observation analytics, geospatial platforms and IT project development for commercial, public sector and European clients. Our core services work mainly with imagery and geospatial data, not with data about individuals. The personal data we process relates mostly to employees, clients, partners, suppliers, platform users and website visitors.

The policy applies to all employees, contractors and third parties who process personal data for or on behalf of TotalView, in any format and on any system.

2. Definitions

- **Personal data:** any information relating to an identified or identifiable natural person, such as a name, email address, IP address or location data.
- **Processing:** any operation on personal data, such as collection, storage, use, disclosure or deletion.

- **Controller:** the organisation that decides why and how personal data is processed.
- **Processor:** an organisation that processes personal data on behalf of a controller.
- **Sub-processor:** a processor engaged by TotalView to process personal data on behalf of a client.
- **Personal data breach:** a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Data Protection Contact:** the person designated by TotalView management to coordinate data protection compliance (see section 5). This role is not a Data Protection Officer within the meaning of Article 37 GDPR.

3. Legal framework

TotalView complies with:

- the General Data Protection Regulation (EU) 2016/679;
- Greek Law 4624/2019 on the protection of personal data;
- Greek Law 3471/2006 on electronic communications, including cookies;
- data protection and confidentiality terms in client contracts and in European programmes such as Horizon Europe and those of the European Space Agency.

The competent supervisory authority is the Hellenic Data Protection Authority (www.dpa.gr).

4. Data protection principles

TotalView applies the principles of Article 5 GDPR to all processing:

- **Lawfulness, fairness and transparency:** data is processed on a valid legal basis and people are told how.
- **Purpose limitation:** data is collected for specified, legitimate purposes and not reused for incompatible ones.
- **Data minimisation:** only the data needed for the purpose is collected.
- **Accuracy:** data is kept accurate and corrected or deleted when wrong.
- **Storage limitation:** data is kept no longer than necessary.
- **Integrity and confidentiality:** data is protected by appropriate technical and organisational measures.
- **Accountability:** TotalView keeps records that demonstrate compliance.

5. Roles and responsibilities

Management is accountable for data protection compliance and provides the resources it requires.

Data Protection Contact. TotalView is not required to appoint a Data Protection Officer under Article 37(1) GDPR. It is not a public authority, and its core activities do not involve large-scale systematic monitoring of individuals or large-scale processing of special categories of data. Management has instead designated a Data Protection Contact, who:

- maintains this policy and the Record of Processing Activities;
- coordinates data protection impact assessments where required;
- receives and coordinates data subject requests;
- coordinates the response to personal data breaches, including notifications to the Hellenic Data Protection Authority and to clients;
- reviews data processing agreements with clients, suppliers and sub-processors;
- advises project teams on data protection requirements for new projects and systems;
- ensures staff are aware of their data protection obligations;
- acts as the point of contact for clients, data subjects and the supervisory authority.

Employees and contractors must follow this policy, access personal data only when their work requires it, keep it confidential, and report any suspected breach to the Data Protection Contact immediately.

Processors and sub-processors acting for TotalView must sign a data processing agreement meeting Article 28 GDPR before processing any personal data.

6. TotalView as controller and as processor

As controller, TotalView decides how personal data is processed for its own operations: staff and recruitment, client and supplier relationships, business development, its website, and user accounts on its own platforms.

As processor, TotalView processes personal data only on behalf of a client, for example when hosting, developing or operating a system that holds the client's users or records. In this role TotalView:

- processes the data only on the client's documented instructions, set out in a data processing agreement;
- ensures that staff with access are bound by confidentiality;
- engages sub-processors only with the client's prior authorisation and under equivalent contractual obligations;
- assists the client with data subject requests, security, breach notification and impact assessments;
- notifies the client of any personal data breach without undue delay;
- deletes or returns the data at the end of the service, as the client chooses, unless law requires retention;
- makes available the information needed to demonstrate compliance, including for audits.

7. Personal data processed and legal bases

TotalView processes the following categories of personal data as controller:

Data subjects	Typical data	Purpose	Legal basis (Art. 6 GDPR)
Employees and contractors	Identity, contact, contract, payroll, social security and tax data	Employment and legal obligations	Contract; legal obligation
Job applicants	CV, contact details, interview notes	Recruitment	Steps before a contract; legitimate interest
Client, partner and supplier contacts	Name, role, organisation, business contact details	Contracts, projects, invoicing, tenders	Contract; legitimate interest; legal obligation
Platform users	Name, email, organisation, login credentials, usage logs, IP address	Account management, service delivery, security	Contract; legitimate interest
Website visitors	Contact form details, technical data, cookies	Answering enquiries, operating the website	Legitimate interest; consent for non-essential cookies

TotalView does not use satellite imagery or geospatial data to identify or monitor individuals. It does not carry out automated decision-making with legal or similarly significant effects on individuals.

Special categories of data (Article 9 GDPR) are limited to what employment and social security law requires, such as sick-leave records, and are processed only on that basis.

8. Accountability: records, impact assessments and privacy by design

Record of Processing Activities. TotalView maintains a record under Article 30 GDPR, covering processing as controller (Art. 30(1)) and as processor for clients (Art. 30(2)). The Data Protection Contact updates it when processing changes and reviews it at least once a year. It is available to the supervisory authority on request.

Data protection impact assessments. Before starting processing likely to result in a high risk to individuals, TotalView carries out a DPIA under Article 35 GDPR. As processor, it assists clients with their DPIAs.

Privacy by design and by default. Project teams consider data protection when designing new systems, platforms and services. By default, systems collect only the personal data needed, restrict access by role, and apply the retention rules in section 11.

9. Transparency and privacy notices

TotalView informs people about the processing of their personal data at the time of collection, as required by Articles 13 and 14 GDPR, through:

- a privacy notice on its website, covering website visitors, enquiries, and client, partner and supplier contacts;
- privacy information presented to users of TotalView platforms at registration;
- a privacy notice for employees and contractors;
- privacy information for job applicants.

The notices state who the controller is and how to contact the Data Protection Contact. They also set out the purposes and legal bases, recipients, international transfers, retention periods, data subject rights, and the right to complain to the Hellenic Data Protection Authority.

Where TotalView acts as processor, informing data subjects is the responsibility of the client as controller.

10. Sharing, processors and international transfers

Internal access is limited to staff who need the data for their role.

External sharing. TotalView shares personal data with third parties only when necessary and lawful. Recipients may include:

- IT and cloud service providers;
- accountants and legal advisers;
- project partners and subcontractors;
- public authorities, where the law requires it.

Processors and sub-processors act under a data processing agreement meeting Article 28 GDPR. TotalView keeps a list of its sub-processors and provides it to clients on request.

International transfers. TotalView prefers providers that store data in the European Economic Area. Personal data is transferred outside the EEA only in compliance with Chapter V GDPR, for example:

- to a country with an EU adequacy decision, including US organisations certified under the EU-US Data Privacy Framework;
- under the European Commission's Standard Contractual Clauses, with a transfer risk assessment where needed.

11. Retention and deletion

Personal data is kept only as long as its purpose requires, then securely deleted or anonymised.

Data	Retention
Employee and contractor records	Duration of employment, then as required by Greek labour, tax and social security law
Unsuccessful job applications	Up to 12 months after the recruitment closes, unless the applicant agrees to longer
Client, partner and supplier records	Duration of the contract, then as required by tax law and for the defence of legal claims
Records from public and EU-funded projects	As set out in the grant or contract, including audit periods
Platform user accounts	Duration of the account or contract, then deleted within 90 days unless law requires otherwise
Data processed for clients	As instructed by the client; deleted or returned at the end of the service
Website enquiries	Up to 24 months after the last contact

Paper records are shredded, and electronic records are deleted from active systems. Backups are overwritten on their normal rotation.

12. Security measures

TotalView applies technical and organisational measures appropriate to the risk, in line with Article 32 GDPR:

- role-based access control, following the least-privilege principle, with access removed promptly when staff leave;
- strong passwords and multi-factor authentication for business systems and cloud services;
- encryption of data in transit (TLS) and, where supported, at rest;
- firewalls, security updates and anti-malware protection on company systems;
- regular backups, with periodic restore tests;
- logging of access to systems holding personal data;
- security controls in software development, including separation of test and production data;
- confidentiality obligations in employment and contractor agreements;
- secure office access and locked storage for paper records.

Measures are reviewed when systems change and at least once a year.

13. Data subject rights

Individuals have the following rights under Articles 15–22 GDPR:

- access to their personal data;

- rectification of inaccurate data;
- erasure;
- restriction of processing;
- data portability;
- objection to processing based on legitimate interest, and to direct marketing at any time;
- not to be subject to decisions based solely on automated processing;
- withdrawal of consent at any time, where processing is based on consent.

How to make a request. Requests can be sent by email to the Data Protection Contact (section 16) or by post to TotalView's address.

How requests are handled:

1. The Data Protection Contact logs the request and, if needed, verifies the requester's identity.
2. TotalView responds within one month of receipt. This can be extended by two further months for complex or numerous requests, in which case the requester is informed within the first month.
3. Requests are handled free of charge, unless they are manifestly unfounded or excessive.
4. If TotalView declines a request, it explains why and informs the requester of the right to complain to the Hellenic Data Protection Authority.

Where TotalView acts as processor, it forwards any request it receives to the client without undue delay and assists the client in responding.

14. Personal data breach management

Anyone who suspects a personal data breach must report it to the Data Protection Contact immediately. The Data Protection Contact then coordinates the response:

1. **Contain** the incident and limit its effects.
2. **Assess** the data affected, the number of people concerned, and the likely risk to them.
3. **Notify the Hellenic Data Protection Authority** within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk to individuals (Article 33 GDPR).
4. **Inform affected individuals** without undue delay where the breach is likely to result in a high risk to them (Article 34 GDPR).
5. **Notify the client** without undue delay where TotalView acts as processor, with the information the client needs to meet its own obligations.
6. **Record** every breach, its effects and the remedial action taken, including breaches that were not notified.
7. **Review** the causes and update controls to prevent recurrence.

15. Awareness and review

New employees and contractors receive this policy and a data protection briefing when they join. Refresher guidance is provided when the law, this policy or TotalView's systems change significantly.

This policy is reviewed at least once a year, and whenever TotalView's processing or the applicable law changes significantly.

16. Contact

For any question about this policy or to exercise your data protection rights, contact TotalView's Data Protection Contact:

George Keradinidis, Data Protection Contact TotalView Ltd, Ethnarchou Makariou 44, 121 32 Peristeri, Greece Email: gkera@totalview.gr Phone: +30 210 5912644

You also have the right to lodge a complaint with the Hellenic Data Protection Authority (www.dpa.gr).