totalview

Data Protection Policy

Purpose

This Data Protection Policy outlines how TotalView handles, protects, and secures personal data in compliance with legal and regulatory requirements, including the General Data Protection Regulation (GDPR), national data protection laws, and specific provisions related to commercial, governmental, and European projects. As a company operating in satellite imagery tasking, processing, delivery, and IT project development, we are committed to ensuring that all personal data is handled responsibly, transparently, and securely.

Scope

This policy applies to all employees, contractors, partners, and third parties that handle personal data in relation to:

- Satellite imagery tasking, processing, and delivery.
- IT project management and development.
- Commercial, governmental, and European projects involving sensitive data.

Key Definitions

- Personal Data: Any information relating to an identified or identifiable individual (e.g., names, email addresses, location data, or any combination of data that could be used to identify a person).
- Data Subject: The individual to whom the personal data relates.
- Data Controller: The entity that determines the purposes and means of processing personal data.
- Data Processor: The entity that processes personal data on behalf of the Data Controller.
- Processing: Any operation performed on personal data, whether automated or manual, such as collection, storage, alteration, use, disclosure, or destruction.
- GDPR: The General Data Protection Regulation (EU) 2016/679, the European regulation governing personal data protection and privacy.

Legal and Regulatory Framework

As a company involved in commercial, governmental, and European projects, TotalView is subject to multiple regulatory frameworks, including:

- General Data Protection Regulation (GDPR) (EU) 2016/679.

- Project-specific privacy and data protection obligations in government contracts, European research programs (e.g., Horizon Europe, European Space Agency), and defense-related projects.

Principles of Data Protection

TotalView abides by the following data protection principles:

- Lawfulness, Fairness, and Transparency: Data is processed legally, fairly, and in a transparent manner.
- Purpose Limitation: Data is collected for specified, explicit, and legitimate purposes and not processed further in ways incompatible with those purposes.
- Data Minimization: Personal data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- Accuracy: Personal data is accurate and kept up-to-date. Inaccurate data is corrected or erased without delay.
- Storage Limitation: Personal data is kept for no longer than is necessary for the purposes for which the data is processed.
- Integrity and Confidentiality: Personal data is processed in a manner ensuring appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

Responsibilities

Data Protection Officer (DPO)

TotalView appoints a Data Protection Officer (DPO) responsible for overseeing the data protection strategy and ensuring compliance with GDPR and other applicable data protection laws.

Employees and Contractors

All employees and contractors are responsible for:

- Handling personal data in compliance with the company's data protection policies.
- Reporting data breaches or potential violations immediately.
- Participating in regular data protection training.

Third-Party Processors

Third-party processors handling personal data on behalf of TotalView must ensure compliance with contractual data protection obligations and GDPR requirements. A Data Processing Agreement (DPA) is signed with all third-party processors.

Data Collection and Processing

Types of Data Collected

The types of personal data collected by TotalView depend on the project:

- Satellite imagery tasking/processing: Personal data such as user names, contact details, geolocation data, and company details.
- IT projects: Names, email addresses, IP addresses, user credentials, and system usage data.
- Commercial and governmental contracts: Any necessary data to fulfill the terms of contracts, including billing information, legal documentation, and performance monitoring data.

Data Processing Legal Basis

TotalView processes personal data only where a legal basis exists, including:

- Contractual necessity: When processing is necessary to fulfill contractual obligations.
- Consent: Where data subjects provide explicit consent.
- Legitimate interests: Where processing is necessary for legitimate business interests.
- Legal obligations: When processing is required by law, especially in governmental projects.

Special Categories of Personal Data

Where required, TotalView may handle sensitive data such as:

- Health-related data, in the context of employees or specific projects.
- Biometric data, where relevant for access control in secure projects. Special safeguards are applied to handle such data in compliance with GDPR Article 9.

Data Protection by Design and Default

TotalView integrates privacy by design into all systems and processes. This involves:

- Risk assessments for any project handling personal data.
- Data minimization by collecting only the essential data required for the project.
- Secure development processes in IT and satellite systems that embed privacy protections from the start.

Data Transfers and International Processing

Data Sharing

- Internal: Personal data is shared between departments only when necessary for the completion of a task and in line with GDPR principles.
- External: Data sharing with third parties (e.g., subcontractors, governmental authorities) occurs only under strict contractual agreements, ensuring GDPR compliance.

International Transfers

- Personal data transferred outside the European Economic Area (EEA) is done in compliance with GDPR Chapter V.
- Adequate safeguards: TotalView ensures that adequate safeguards are in place (e.g., EU Standard Contractual Clauses) when transferring personal data to third countries.

Data Retention and Deletion

Personal data is retained only for the duration necessary to fulfill its intended purpose. Specific retention periods include:

- Satellite imagery-related data: Retained for the duration of contracts or image access periods, then deleted or anonymized.
- IT project data: Retained as required by law or project terms and deleted when no longer needed.
- Governmental and EU project data: Retained according to contractual or legal obligations, often for longer periods, subject to audit and security protocols.

Regular audits are conducted to ensure compliance with the data retention policy, and automated systems may be used to delete data when no longer needed.

Data Security Measures

Physical Security

- Controlled access to data centers and ground stations using biometric systems, key cards, and security personnel.
- Video surveillance and intrusion detection systems for all secure areas.

IT Security

- Encryption: All personal data is encrypted both in transit (using TLS) and at rest.
- Access Control: Strict user role management ensuring only authorized personnel have access to personal data.

- Firewalls and Intrusion Detection Systems: Protection of IT systems from external attacks.
- Data Backup and Recovery: Secure and encrypted backups of all critical data to ensure business continuity in case of disaster.

Satellite Data Security

- RF encryption: Secure communication channels with satellites to prevent interception.
- Access control for satellite data: Satellite tasking and access to processed imagery are restricted to authorized personnel with appropriate clearance levels.

Data Subject Rights

TotalView respects the rights of individuals under the GDPR:

- Right to access: Individuals can request access to their personal data.
- Right to rectification: Individuals can request correction of inaccurate data.
- Right to erasure ("right to be forgotten"): Individuals can request the deletion of their personal data when no longer necessary.
- Right to restrict processing: Individuals can request limitations on how their data is used.
- Right to data portability: Individuals can request their data in a commonly used, machine-readable format.
- Right to object: Individuals can object to processing based on legitimate interests or direct marketing.

All requests must be handled within one month of receipt and free of charge, unless the request is manifestly unfounded or excessive.

Data Breach Response

In the event of a personal data breach, TotalView will:

- Notify the Data Protection Officer (DPO) immediately.
- Assess the breach to determine the severity and impact on individuals.
- Notify the Supervisory Authority (if required) within 72 hours of becoming aware of the breach.
- Communicate to affected individuals if the breach poses a high risk to their rights and freedoms.
- Document the breach and the measures taken to mitigate its impact.

Training and Awareness

All employees and contractors undergo mandatory data protection training to ensure understanding of their responsibilities under this policy, GDPR, and project-specific data handling requirements. Training is refreshed regularly and whenever significant changes in legislation or technology occur.

Review and Monitoring

This Data Protection Policy is reviewed annually or whenever significant changes occur in the legal or operational landscape. Internal audits are conducted to ensure ongoing compliance with data protection regulations and best practices.

Contact Information

For any queries or concerns regarding data protection at TotalView, please contact:

Data Protection Officer (DPO)

George Keradinidis

+30 2105912644

gkera@totalview.gr

This policy ensures that TotalView remains compliant with relevant data protection laws while maintaining the highest standards in satellite imagery and IT project management.