



Version 1
August 2025

Data Protection Policy

We, **MT INNOVATIVE SOLUTIONS S.A.**, are dedicated to ensuring the security and privacy of your personal data and to complying with the applicable national and European legal and regulatory framework governing their protection.

Within this context, and in particular in accordance with the principle of transparency as provided under the General Data Protection Regulation (GDPR) and Law 4624/2019, as in force from time to time, this Data Protection Policy, together with any other document referred to herein, sets out the basis on which we collect and process your personal data when you use our website or our services as well as your rights regarding their protection.

1. Data Controller

The société anonyme under the name “**MT INNOVATIVE SOLUTIONS S.A.**”, with the distinctive title “**MT INNOVATIVE SOLUTIONS S.A.**” (hereinafter the “**Company**” or “**MTIS**”), acts as the Data Controller with respect to the personal data collected and generally processed in the context of its activities. The Company’s registered office is located at 41 Agiou Dimitriou Street, 185 46 Piraeus, Greece.

MTIS acts as the Data Controller with regard to the personal data it collects directly (e.g., through its website or within the context of its collaborations with clients and suppliers). However, in certain cases, MTIS may process personal data on behalf of its clients, through the services it provides. In such cases, MTIS acts as the Data Processor within the meaning of Article 28 of the General Data Protection Regulation (EU) 2016/679 (GDPR), processing the data strictly on the basis of the instructions of the respective client–Data Controller.

2. Data We Collect

Within the scope of our services and activities, our Company collects and processes various categories of personal data, such as indicatively:

- **Identification and Contact Details:** Full name, position/title, contact information (such as email address, telephone number), and any corporate affiliation (e.g., company/organisation and role), when you contact us through the available forms or enter into cooperation with us.
- **Website Data and Cookies:** Information collected during visits to our website, such as IP addresses, browser type, operating system, cookies and similar technologies. When submitting requests, we collect the data you provide (e.g., name, email, message content), as well as



Version 1
August 2025

technical information such as the IP address and browser user agent for security purposes (e.g., spam detection).

- **Account and Client Data:** If you are our client or a user of our platforms/services (e.g., the i-Platform©, the SeaSmart™ system, or i-Vessel solution), we collect the necessary data for the creation and management of user accounts. Such data may include username, password (encrypted), contact details of authorized users, as well as activity log files during the use of our systems, for operational and security purposes. We also maintain contract and invoicing information (e.g., details of legal representatives, necessary tax data) concerning our clients/partners.
- **Image and Video Data:** The security and image analysis solutions we provide (e.g., CCTV surveillance systems, the i-Platform© “smart” monitoring platforms) may collect and/or process images and video recordings depicting natural persons. It should be noted that MTIS does not collect such data directly for its own purposes, but any processing of images/video is carried out exclusively on behalf of our clients who use our services, and only where there is a valid legal basis.
- **Special Categories of Data:** As a rule, MTIS does not collect special categories of data (such as health data, religious/political beliefs, etc.). However, in exceptional cases, certain systems we provide (e.g., facial recognition access control solutions, where used by our clients) may process biometric data. In such cases, processing is carried out solely on the basis of a legal ground and with enhanced safeguards, strictly on behalf of our clients.

We only collect the data necessary for the purposes specified in this Policy and we ensure that they are always up to date and accurate, based on the information you provide.

3. Purposes of Processing

We process personal data solely for specified and lawful purposes. The purposes of processing are the following:

- **Provision of Our Services and Solutions:** We process only the strictly necessary personal data in order to provide our technological solutions to clients (e.g., installation and maintenance of the i-Platform©, SeaSmart™, or i-Vessel systems), to create and manage user accounts on our platforms, and to provide technical support. Furthermore, our surveillance systems may process image/video data for the purpose of safeguarding vessels or facilities (e.g., preventing unauthorized access or monitoring premises for the protection of persons and property).



Version 1
August 2025

- **Management of Client and Partner Relationships:** We process identification, contact and other contractual data in order to enter into and perform contracts, issue invoices, manage payments, as well as to maintain communication with clients, suppliers, or partners regarding ongoing projects, equipment deliveries, etc.
- **Communication with Interested Parties and Support:** When you send us a message (through the website contact form, by email or telephone), we use the data you provide in order to communicate with you, respond to your enquiries, provide you with information about our products/services, or take action at your request.
- **Promotion of Products/Services and Information:** On a limited basis, we may process the contact details of clients or interested parties (e.g., email) in order to send them updates regarding our products/services, company news, or event invitations. You have the right, at any time, to object to the further receipt of such communications (opt-out) by submitting a relevant request to our Company.
- **Compliance with Legal Obligations:** For example, we maintain financial records and invoices that may include names/addresses for tax and accounting purposes (compliance with tax legislation).
- **Support of Legal Claims:** The processing of personal data may also be deemed necessary for the establishment, exercise or defense of legal claims and/or for the protection of our rights.
- **System Security and Fraud Prevention:** We process log data from our networks, platforms and website to ensure the integrity, availability and confidentiality of information.

The above processing purposes are specific, lawful and compatible with the context in which the personal data are collected, in accordance with the purpose limitation principle, as provided in Article 5(1)(b) GDPR. We do not perform any further processing of your data for purposes incompatible with those initially specified, without prior notice to you and, where required under the applicable legal framework, without obtaining your explicit consent.

4. Legal Basis for Processing

At MTIS, the processing of personal data is based, as the case may be, on one or more of the following legal bases:

- **Performance of a Contract (Article 6(1)(b) GDPR):** When the processing is necessary for the provision of our services to you or in order to take steps at your request prior to entering into a contract. For example, we use the personal data of clients and their users in order to create



Version 1
August 2025

accounts and provide the agreed solutions/services. Without such data, we would not be able to fulfil the terms of the contract or serve you.

- **Consent (Article 6(1)(a) GDPR):** In cases where you choose to do so, we will process your data on the basis of your consent. For example, if you opt to receive newsletters, we will use your email address solely on the basis of your explicit consent, which you may withdraw at any time. Similarly, for the use of non-essential cookies, we will first seek your consent. The data subject has the right to withdraw consent at any time, without negative consequences and without affecting the lawfulness of processing carried out prior to such withdrawal. Withdrawal only applies for the future.
- **Legitimate Interest (Article 6(1)(f) GDPR):** In certain cases, processing is necessary for purposes connected with the legitimate interests pursued by MTIS or a third party, provided that the rights and freedoms of the data subject do not override such interests. For example, we rely on our legitimate interest: (a) to ensure the security of our information systems and to prevent unlawful or malicious actions, serving both the Company's and the users' interests, and (b) for our legal protection, such as maintaining relevant records (e.g., communications and transactions), in order to be in a position to address potential claims or legal disputes.
- **Legal Obligation (Article 6(1)(c) GDPR):** In certain cases, MTIS processes personal data in order to comply with obligations arising from applicable legislation. Indicative examples of such processing include: (a) maintaining accounting and tax records which contain personal data, such as the name and contact details of a client appearing on documents (e.g., invoices, receipts), and (b) disclosing data to competent administrative or judicial authorities, upon lawful request or in the context of investigations, court proceedings or other statutory requirements.

5. Data Recipients and Disclosure

In the context of our activities, it may be necessary to disclose certain personal data to third-party recipients:

- **Authorized MTIS Personnel:** Access to personal data is strictly limited to MTIS employees and, where necessary, to external associates acting as consultants, who hold specific responsibility related to the fulfilment of the purposes of processing.
- **Processors (Subcontractors):** We cooperate with reliable third-party service providers who act on our instructions and on our behalf, in order to support the provision of our services. Such providers may include: data hosting companies and cloud infrastructure providers (data centers/cloud providers where our servers and databases are hosted), system maintenance or



Version 1
August 2025

software development providers, email or other communication tool providers, website analytics services, etc.

- **Business Partners / Affiliates:** In certain cases, we may need to share data with our business partners, such as equipment suppliers or local representatives, where this is necessary for the provision of a comprehensive solution to you.
- **Public Authorities and Legal Compliance:** Where required by law or by legal proceedings, we may disclose personal data to competent authorities. We may also share information with our advisors (e.g., lawyers, accountants) when this is necessary for compliance with obligations or for the protection of our legitimate interests.
- **Transfers to Third Countries:** Processing of your data is carried out within the European Economic Area (EEA). However, in some cases, it may be necessary to transfer or store data in countries outside the EEA, particularly where we use providers of technological infrastructure or IT services (e.g., cloud services) that are based or operate data centers in third countries. In any case of international transfer, full compliance with the requirements of Chapter V of the General Data Protection Regulation (GDPR) is ensured.

In all cases of personal data disclosure, we strictly apply the principle of minimisation and purpose limitation. We transfer only the data that are strictly necessary, depending on the specific processing purpose, and we ensure that each recipient is contractually bound to maintain confidentiality, data security, and comply with the applicable data protection laws and regulations.

6. Data Security Measures

MTIS attaches particular importance to information security and implements appropriate technical and organizational measures to protect personal data against unauthorized access, loss, alteration or disclosure. Indicatively, our measures include:

- **Access Control:** We restrict access to personal data solely to the strictly necessary personnel and, where required, to external partners, solely on a need-to-know basis.
- **Encryption:** We use secure transmission protocols (SSL/TLS) to safeguard data during transfer.
- **Application Security Safeguards:** Our platforms and software are designed and developed in accordance with secure coding best practices. In addition, vulnerability assessments and penetration tests are carried out on a regular basis.
- **Network Protection Systems & Infrastructure:** We implement modern cybersecurity solutions. Our services are hosted in data centers that meet high security standards, hold the necessary certifications, and maintain physical access safeguards.



Version 1
August 2025

- **Certifications and Standards:** Our commitment to security and quality is also demonstrated by the certifications we have obtained. In particular, MTIS is certified under ISO 9001:2015 (Quality Management Systems), ISO 27001:2013 & ISO 27005:2022 (Information Security Management), and ISO 22301:2019 (Business Continuity Management), among others.
- **Training & Policies:** All our staff receive regular training on cybersecurity and data protection issues, with the aim of ensuring awareness of the obligations arising from the applicable legal framework. We have established and enforce internal security policies and procedures, including policies for identifying and responding to data breach incidents.

The technical and organizational security measures we apply are reviewed and updated on a regular basis, in order to adapt to new technological developments, emerging threats and changes in the operational environment. While no information system can guarantee absolute security, our Company takes all reasonable and documented measures to ensure the highest possible level of protection of the personal data it processes.

7. Data Retention Period

We retain personal data only for as long as is strictly necessary to fulfil the purposes for which they were collected or for as long as is required or permitted by the applicable legal framework. Specifically:

- **Communication/Request Data:** Personal data collected in the context of communications or requests are retained for up to six (6) months following the last communication, in order to address any subsequent actions or follow-up requests.
- **Client and Contract Data:** Personal data related to the conclusion and performance of contracts, such as client details, platform users, orders, etc., are retained throughout the duration of the active contract or cooperation. Following the termination of the cooperation, the data are retained for as long as required to comply with legal obligations, such as the retention of tax and accounting records, typically for a period of five (5) years, in accordance with the relevant provisions of tax legislation and the limitation periods set out in the Civil Code.
- **Browsing Data & Cookies:** Our server log files, which may include IP addresses and other browsing data, are retained for a limited period, namely up to six (6) months, unless it is necessary to retain them longer for security purposes (e.g., investigation of a security incident or breach). As regards cookies, their retention period varies depending on their type: session cookies are automatically deleted upon closing the browser, whereas other cookies, such as



Version 1
August 2025

those relating to preferences or analytics, may remain stored for a period ranging from a few months up to two (2) years, depending on their functionality.

- **Video Recordings/Surveillance Data:** Image/video data collected through surveillance systems (such as security cameras operating via our platform) are retained for a limited period determined by the client–Data Controller. In any case, video recordings are automatically deleted after fifteen (15) days, unless a specific extract must be retained for a longer period because it relates to an incident (e.g., a recorded security event under investigation).
- **Other Data (e.g., CVs):** In the event that you submit a CV to us for potential cooperation/employment, we retain your data for a period of up to one (1) year from receipt, unless you provide us with your explicit consent for longer retention (e.g., for future job opportunities).

Upon expiry of the above periods, or where the processing purpose ceases to exist, we delete or anonymize personal data in a secure manner.

8. Data Subjects' Rights

Pursuant to the General Data Protection Regulation (GDPR), you have the following rights in relation to the processing of your personal data:

- **Right of Access:** To be informed whether we process your personal data and to receive a copy thereof.
- **Right to Rectification:** To request the rectification or completion of your inaccurate or incomplete personal data.
- **Right to Erasure (“right to be forgotten”):** To request the deletion of your data, where they are no longer necessary or where you withdraw your consent.
- **Right to Restriction of Processing:** To request the restriction of processing, for example when you contest the accuracy of the data.
- **Right to Data Portability:** To receive the data you have provided to us in a structured, commonly used and machine-readable format, or to request their transfer to another controller.
- **Right to Object:** To object to the processing of your data for direct marketing purposes or when the processing is based on legitimate interest.
- **Withdrawal of Consent:** Where processing is based on your consent (e.g., newsletters, cookies), you may withdraw it at any time without consequences. Withdrawal of consent does not affect the lawfulness of processing carried out prior to withdrawal.



Version 1
August 2025

Following the exercise of any of the above rights, we will review and respond to the request as soon as possible and, in any case, within the timeframe prescribed by law (**within one (1) month, with the possibility of an extension of two months for complex requests, in which case we will duly inform you**). The exercise of rights is free of charge for the data subject. However, where a request is manifestly unfounded or excessive (particularly due to its repetitive nature), the Company reserves the right to impose a reasonable fee or to refuse to respond, as provided under the GDPR.

9. Contact and Complaints

For any questions, concerns, or requests relating to this Data Protection Policy or more generally regarding the way MTIS processes personal data, the data subject may contact us as follows:

MT INNOVATIVE SOLUTIONS S.A. (MTIS)

Address: 41 Agiou Dimitriou Street, 185 46 Piraeus, Greece

Telephone: +30 216 400 3001

Email: info@mtis.tech

Furthermore, if you consider that your rights regarding the protection of personal data have been infringed or that the processing we carry out is not in compliance with the GDPR, you have the right to lodge a complaint with the competent Data Protection Supervisory Authority. For Greece, this is the Hellenic Data Protection Authority (Hellenic DPA):

- Hellenic DPA Address: 1–3 Kifisias Avenue, P.C. 115 23, Athens, Greece
- Telephone: +30 210 6475600
- Email: contact@dpa.gr
- Website: www.dpa.gr

We may update this Data Protection Policy in order to reflect changes in our practices or in applicable legal requirements.

10. Version History

VERSION	DATE	AMENDMENTS
1 st	01/08/2025	Initial Edition