PRIVACY

Insight

TIM Group

June 2025

INDEX

1. Privacy policy

The TIM Group's privacy model, consisting of a clear identification of roles and responsibilities as well as a system of internal rules and guidelines, is fully compliant with European personal data protection regulations. In particular, it refers to the General Data Protection Regulation (GDPR), the Privacy Code (Legislative Decree 196/2003, as amended), as well as the measures issued by the Italian Data Protection Authority.

The company functions are actively involved in ensuring that the processing of personal data concerning data subjects — customers, employees, and other individuals — is carried out in full compliance with applicable laws during all operational activities. Our policy clearly defines the technical and administrative measures to be implemented to safeguard data, assigning specific tasks and responsibilities to each party involved (managers, employees, designated personnel) and applies to all managers, employees, and external stakeholders of the TIM Group.

This system is applied across the entire organization, ensuring a consistent and responsible approach to privacy management for both internal staff and anyone having dealings with the Group.

Furthermore, the "System of Rules for the Implementation of Privacy Regulations in the TIM Group" (System of Rules) sets out the operational guidelines for each area of action. All documents relating to privacy and its management are available in the Privacy section of the corporate website (accessible at this link TIM Group | Privacy).

1.1 Responsibilities and Obligations

Within the TIM Group, we clearly define the areas of authority and responsibility of our employees and stakeholders with regard to the protection of customer data. From an organizational perspective, this matter is overseen by the Data Protection Officer (DPO), who, within the Legal, Regulatory & Tax Department, is supported by the Legal Media &

Privacy function. This function ensures the definition and proper implementation of privacy guidelines and regulations, while also providing advice, training, and information on the application of privacy laws. In addition, the Compliance Department is responsible for ensuring the fulfillment of supervisory obligations.

2. Risk Management in Privacy Matters

Privacy risk management is integrated into the broader Enterprise Risk Management (ERM) system adopted by the TIM Group, which enables the structured identification, assessment, and monitoring of risks associated with the processing of personal data.

In this context, the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, introduced significant regulatory changes that have had a direct impact on how these risks are managed. Among the main changes are:

- the introduction of the obligation of 'accountability', which establishes more stringent requirements for data controllers and processors, including the data protection impact assessment (DPIA), thorough documentation of processing activities, the adoption of adequate security measures, and the timely management of data breaches, in addition to the appointment of the Data Protection Officer (DPO);
- the strengthening of data subject rights, such as the right to data erasure (right to be forgotten) and the right to data portability;
- the increase of financial penalties, which are now significantly higher and proportionate to the severity of violations.

As a result of these provisions, GDPR compliance is not merely a legal obligation but also an essential tool for mitigating risks related to personal data management, such as those associated with breaches, sanctions, or reputational harm. Proper privacy management therefore means protecting the company while strengthening customer and stakeholder trust, thereby contributing tangibly to the organization's resilience and transparency.

From this perspective, the internal disciplinary system also plays an important role in preventing privacy risks. The TIM Group applies graduated sanctions to its employees, proportionate to the severity of any non-compliant behavior, to deter improper conduct. Depending on the type of incident and the level of responsibility, measures may include suspension, termination of employment, or, in the most serious cases, immediate revocation of a retail outlet's license.

These measures help reinforce compliance with company policies and promote an organizational culture based on responsibility and the protection of personal data.

To support privacy risk management, we constantly monitor the actual application of our policies through a structured, multilayered control system. This includes periodic self-assessments, random audits conducted by central and regional functions, and second-level checks planned according to the risk level associated with specific processing activities.

Each year, we adopt all necessary measures to ensure that internal provisions are effectively integrated into our operational processes. This enables us to promptly manage any personal data breaches and to respond both to data subjects' requests—such as access, rectification, or erasure of their personal data, and withdrawal of consent—and to requests from the Italian Data Protection Authority.

3. Privacy Practices for TIM Customers

We provide detailed information on how we manage our customers' personal data within the "TIM Privacy Notices pursuant to personal data protection regulations" TIM Group | Privacy section of the TIM Group Corporate website.

Specifically, we clearly describe the types of information we collect, which may include:

- personal and contact details, such as name, surname, address, telephone number, and email address;

- billing and contractual data, relating to active services, payment methods, subscription or top-up management;
- traffic and browsing data, such as information about calls, internet connections, or the use of apps and digital portals;
- in specific cases, special categories of data, collected in compliance with the safeguards provided by applicable law.

We also specify the purposes for which we process data[1] , such as:

- he provision of the requested service;
- the improvement of the services provided;
- the prevention of defaults and fraud, as well as the detection and counteraction of non-compliant behavior by customers or third parties (e.g., abuse or fraud);
- the fulfillment of legal obligations;
- the security and integrity of networks and systems;
- the exercise and defense of a right in legal proceedings.

For each purpose, we indicate the legal basis for processing, which may stem from contractual obligations, legal requirements, or the legitimate interests of the data controller, always ensuring respect for the rights and freedoms of data subjects.[2]

In documents addressed to both Consumer and Business[3] customers, we further explain the cases where data processing requires the customer's explicit consent. This applies, for example, to:

(1) "Purposes for which data processing is necessary and related legal basis"
(2) Information available in the following documents published on the TIM Group website: *Privacy Notice to Shareholders pursuant to personal data protection regulations; Privacy Notice to Consumer Customers pursuant to personal data protection regulations; Privacy Notice to Business and Corporate Customers pursuant to personal data protection regulations.*
(3) Paragraph 3 – Purposes for which data processing is optional and subject to consent

- promotional communications,
- personalized marketing activities,
- behavioral analysis aimed at improving user experience or offering tailored proposals.

4. Customer Choices and Rights Regarding Data Processing

We place great importance on our customers' freedom of choice regarding the use of their personal data. In line with the principles of transparency and fairness, we provide clear and accessible information on which processing activities require consent and which can be refused.

We always ensure the possibility to exercise opt-out, that is, to object to the processing of personal data in cases provided for by applicable law. At the same time, we obtain prior consent (opt-in) for all activities that are not strictly necessary for the provision of the service. These include, for example:

- promotional communications and other marketing activities, including personalized marketing;
- profiling activities aimed at offering personalized proposals;
- sharing customer data with third parties for their own promotional purposes.

Obtaining consent for these purposes is an essential condition for us and represents one of the fundamental guarantees of our commitment to responsible and respectful management of personal data (these options are described in the section "Information provided by TIM on personal data protection").

We therefore fully recognize our customers' right to maintain control over their personal data, giving them the opportunity to exercise, at any time, their fundamental rights, including:

- requesting access to personal data held by TIM;
- requesting data portability, i.e., transfer to another service provider;

- requesting the correction of inaccurate data or the deletion of processed data.

5. Data Retention and Protection

We retain our customers' personal data for a period proportionate to the purposes for which they were collected and processed, in compliance with the time limits set by applicable regulations or any contractual obligations. The information retained is managed according to the principles of relevance, non-excessiveness, and necessity, in line with the provisions of the General Data Protection Regulation (GDPR).

To protect such data, we adopt appropriate technical and organizational measures, calibrated to the level of risk. These measures are designed to ensure a level of security consistent with the state of the art, the implementation costs, the nature and purposes of the processing, as well as the likelihood and severity of potential risks to customers.[4]

6. Data Collection for Secondary Purposes

The collection of data for secondary purposes, such as promotional activities, personalized marketing initiatives, or profiling, takes place exclusively with the customer's explicit consent, as required by data protection regulations.

Currently, the percentage of data collected for non-essential purposes is 70%. This figure reflects the proportion of customers who have freely chosen to authorize processing beyond what is strictly necessary for the provision of the service.[5]

(4) Detailed information on this topic is available in the Privacy Notice to Shareholders pursuant to personal data protection regulations, paragraph 3) Data Retention; and in the Privacy Notice to Consumer Customers pursuant to personal data protection regulations, paragraph 5) Data Retention, including traffic data.
(5) For further details on these optional purposes, refer to: the Privacy Notice to Consumer Customers pursuant to personal data protection regulations, paragraph 3) Purposes for Which Data Processing Is Optional and Subject to Consent; and the Privacy Notice to Business and Corporate Customers pursuant to personal data protection regulations, the same paragraph 3.

Number of requests from government authorities in the last fiscal year:	Percentage of requests that resulted in data disclosure in the last fiscal year:
3,669,47	100