



PRIVACY

Insight

TIM Group

2026 June



INDEX

1. The privacy model	3
2. Privacy Risk Management	4
3. Privacy Practices for TIM Customers	5
4. Customer Choices and Rights Regarding Data Processing	7
5. Data Retention and Protection.....	8
6. Data Collection for Secondary Purposes	8



1. The privacy model

The TIM Group's Privacy Model, based on a clear definition of roles and responsibilities and on a system of internal rules and guidelines, is established in accordance with applicable data protection laws. In particular, the framework refers to Regulation (EU) 2016/679—the General Data Protection Regulation (GDPR)—the Code on the Protection of Personal Data (Legislative Decree 196/2003, as amended and supplemented), as well as the provisions issued by the Italian Data Protection Authority.

Company departments are actively involved in ensuring that the processing of personal data of data subjects—customers, employees, and other individuals—is carried out in full compliance with regulations throughout all operational activities. Our policy clearly defines the technical and organizational measures to be adopted for data protection, assigns specific tasks and responsibilities to each party involved (managers, employees, and data processors), and applies to all managers, employees, and external stakeholders of the TIM Group.

This system applies across the entire organization, ensuring consistent and responsible privacy management, both in activities carried out by internal staff and in dealings with anyone who has a relationship with the Group.

In particular, the “System of Rules for the Implementation of Privacy Regulations within the TIM Group” (System of Rules) defines the operational guidelines for each area of activity. All documents related to privacy and its management are available in the privacy section of the corporate website (available at [this link](#)).

Compliance with regulatory provisions and the guidelines of the Italian Data Protection Authority is ensured through the continuous updating of internal rules and Group policies.

Governance regarding the protection of personal data is overseen by the Data Protection



Officer (DPO – Data Protection Officer), who, within the Legal, Regulatory & Tax Department, relies on the Legal Media & Privacy function—which ensures the definition and proper application of privacy guidelines and regulations, providing advice, training, and information on the application of privacy regulations—as well as the Compliance Department to ensure the fulfillment of oversight obligations.

2. Privacy Risk Management

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 related to the processing of personal data.

In this context, the General Data Protection Regulation (GDPR), effective as of May 25, 2018, introduced a framework of obligations and responsibilities that has a direct impact on the management of these risks. Key elements include:

- the principle of “accountability,” which establishes specific responsibilities for data controllers and processors, including data protection impact assessments (DPIAs), detailed documentation of processing activities, the implementation of appropriate security measures, and the timely management of data breaches, as well as the appointment of a Data Protection Officer (DPO);
- the strengthening of data subjects’ rights, such as the right to erasure (right to be forgotten) and the right to data portability;
- the strengthening of the system of financial penalties, which are now more severe and proportionate to the seriousness of the violations

As a result of these provisions, compliance with the GDPR is not only a regulatory obligation but also an essential tool for reducing risks associated with the handling of personal data, such as those related to data breaches, fines, or reputational damage.



Proper privacy management therefore means protecting the company and strengthening the trust of customers and stakeholders, thereby making a tangible contribution to the organization's stability and transparency.

In this context, the internal disciplinary system also plays a significant role in preventing privacy risks. The TIM Group imposes graduated sanctions on its employees, proportionate to the severity of the conduct in question, to deter any non-compliant behavior. 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 the retail outlet's license.

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

To support privacy risk management, we constantly monitor the effective implementation of our policies through a structured, multi-level control system. We utilize periodic self-assessment procedures, spot checks conducted by the relevant central and regional departments, and second-level controls planned based on the level of risk associated with data processing.

We take 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 respond to requests from data subjects—such as requests for access, rectification, or erasure of personal data—and to the revocation of consent, as well as to requests from the Italian Data Protection Authority.

3. Privacy Practices for TIM Customers

We provide detailed information on how we handle our customers' personal data, which is



available, among other places, in the “TIM Privacy Notices Pursuant to Data Protection Laws” section of the TIM Group’s corporate website.

Specifically, we transparently describe the nature of the information we collect, which may include:

- personal and contact information, such as first name, last name, address, phone number, and email address;
- billing and contractual information related to the active service, payment methods, and the management of subscriptions or top-ups;
- traffic and web browsing data, such as information on calls, internet connections, or the use of apps and digital portals;
- in specific cases, also special categories of data (e.g., health-related data); collected in compliance with the safeguards provided by applicable law.

We also specify the purposes for which we process data¹, such as:

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

For each purpose, we also specify the legal basis for data processing, which may stem from contractual obligations, legal requirements, or the data controller’s legitimate

¹ Purposes for which data processing is necessary and the relevant legal basis



interests, always in compliance with the rights and freedoms of the data subjects².

In the privacy notices for our Consumer and Business customers³, we also provide further details on the situations in which data processing requires the customer's consent. This applies, for example, to:

- promotional communications and other marketing activities, including personalized marketing,
- profiling activities aimed at providing personalized offers;
- the disclosure of customer data to third parties for their own promotional purposes.

4. Customer Choices and Rights Regarding Data Processing

We place great importance on our customers' freedom to choose how their personal data is used. In line with the principles of transparency and fairness, we provide clear and accessible guidance on which processing activities require consent and which ones you can opt out of.

We always guarantee the option to opt out—that is, to object to the processing of personal data in the cases provided for by current legislation. At the same time, we proactively request 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 providing personalized offers;
- the disclosure of customer data to third parties for their own promotional purposes.

² Information is available in the following documents published on the TIM Group's website: Notice to Shareholders pursuant to personal data protection regulations; Notice to Consumer Customers pursuant to personal data protection regulations; Notice to Business Customers pursuant to personal data protection regulations.

³ Paragraph 3: Purposes for which data processing is optional and requires consent



Obtaining consent for the aforementioned purposes is an essential requirement for us and represents one of the fundamental guarantees of our commitment to the responsible and respectful handling of personal data (these options are described in the section “Information Provided by TIM on the Protection of Personal Data”). We also recognize our customers’ right to maintain control over their personal data by exercising, at any time, the rights provided for by law, including:

- request access to personal data held by TIM
- request data portability, that is, the transfer of data to another service provider
- request the correction of any inaccurate data or the deletion of processed data.

5. Data Retention and Protection

The TIM Group retains its customers’ personal data for a period commensurate with the purposes for which it was collected and processed, in accordance with the terms set forth in applicable law or any contractual obligations. The retained information is managed in accordance with the principles of relevance, data minimization, and necessity, consistent with the principles of the General Data Protection Regulation.

To protect this data, TIM implements appropriate technical and organizational measures, tailored to the level of risk. These measures are designed to ensure a level of security consistent with the state of the art, the costs of implementation, the nature and purposes of the processing, as well as the severity and likelihood of potential risks to customers⁴.

6. Data Collection for Secondary Purposes

Data collection for secondary purposes—such as promotional and marketing activities

⁴ Detailed information on this topic is available in the following documents: the “Notice to Shareholders Pursuant to Personal Data Protection Laws,” paragraph 3) “Retention of Personal Data”; and the “Notice to Consumer Customers Pursuant to Personal Data Protection Laws,” paragraph 5) “Retention of Personal Data, Including Traffic Data.”



(including personalized marketing) and profiling—takes place exclusively with the customer's prior consent, as required by data protection laws.

Currently, the percentage of customers who have consented to the processing of their data for secondary purposes is almost 70%. This figure reflects the proportion of customers who have freely chosen to authorize at least one additional processing activity beyond those strictly necessary for the provision of the service⁵.

Number of requests from government authorities during the last fiscal year	Percentage of requests that resulted in the disclosure of data during the last fiscal year:
4.004.188	100

⁵ For further details on these optional purposes, please refer to: the Consumer Privacy Notice pursuant to the Personal Data Protection Act, paragraph 3) "Purposes for which data processing is optional with consent"; and the Business and Corporate Customer Privacy Notice pursuant to the Personal Data Protection Act, the same paragraph 3)