TIS PRIVACY POLICY

JANUARY 2025

VERSION HISTORY

Version	Data	Description of changes
Version 4.0	November 2020	Consolidation of the text, review of the cookie policy
Version 4.1	February 2021	Review of minor errors and verification of national legislation
Version 5.0	February 2021	Inclusion of ANNEX I - DATA MANAGEMENT PLAN
Version 6.0	March 2022	Changes to images and logos
Version 7.0	January 2025	Comprehensive review and update of content. Change of Information System to PHC

1. TIS PRIVACY POLICY

1.1. TIS commitment

At TIS, we recognise the importance of trust in managing personal data. We are committed to adhering to the highest standards of privacy by using personal data solely for clearly defined purposes and in compliance with data protection rights. Ensuring the confidentiality and integrity of personal data is a core priority for us.

This Privacy Policy outlines in detail how TIS collects, uses, and protects personal data obtained through social and opinion studies, as well as the personal data of our clients.

1.2. Who is responsible for data processing?

As part of its activities and functions, TIS is responsible for collecting and processing personal data, which is handled and stored both automatically and manually.

TIS has appointed a Data Protection Officer (DPO) who can be contacted via email at dpo@tis.pt. The DPO is specifically tasked with monitoring the compliance of activities involving personal data processing with applicable legal and regulatory standards. The DPO also serves as the point of contact between TIS and the National Control Authority, as well as between TIS and its clients or users on matters concerning data processing.

1.3. What personal data is collected?

1.3.1. What is personal data?

Personal data refers to any information, regardless of format, that relates to an identified or identifiable individual. An identifiable individual is someone who can be directly or

indirectly identified, particularly by reference to an identifier such as an identification number or location data.

1.3.2. From whom do we collect personal data?

As part of its professional functions, TIS predominantly processes personal data from individuals, especially those that allow the analysis of mobility patterns and preferences for various transport modes. These data are collected through surveys or interviews conducted in person, over the phone, or online using productivity tools when necessary.

Additionally, TIS may collect and process personal data from the following individuals (non-exhaustive list):

- TIS employees;
- Current and potential TIS clients;
- Partners and their employees;
- Service providers and their employees;
- Job and internship candidates;
- Participants in TIS-organised events (e.g., seminars and training sessions).

1.3.3. What personal data do we process and how do we collect it?

TIS only collects data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. Data collection may occur verbally, in writing (e.g., through forms and surveys), or via online questionnaires. Generally, data are collected directly but may also come from public sources (e.g., websites and official public lists).

For different purposes, we may collect the following types of personal data:

- Identification data (e.g., name, age, gender, residence);
- Contact data (e.g., mobile phone, address, email);
- Education and professional status data (e.g., education level, employment status, CV);
- Location data (e.g., IP address);
- Mobility pattern data for a reference day (e.g., start and end points of journeys, times of departure and arrival, transport modes used, reasons for travel, parking arrangements, transport ticket information).

TIS does not generally collect sensitive data such as health information or data related to criminal offences.

1.3.4. Why and on what grounds do we use personal data?

TIS processes personal data based on the following lawful grounds:

- Consent: Data collection is preceded by explicit, specific, and informed consent from the data subject, obtained through written or online means. Examples include conducting surveys, subscribing to newsletters, or registering for TIS-organised events.
- Contract execution or pre-contractual steps: Data processing is necessary for the performance of a contract in which the data subject is a party or for pre-contractual arrangements.
- Legal obligations: Processing is necessary to comply with legal requirements, such as reporting data to public, fiscal, or judicial authorities.
- Legitimate interest: Processing is necessary for TIS's or third parties' legitimate interests, provided it does not override the data subject's rights and freedoms.

1.3.5. What are the purposes for collecting personal data?

TIS processes personal data for specific, explicit, and legitimate purposes. Examples include:

- Collecting data on personal characteristics and mobility patterns to meet project objectives;
- Contracting and providing services;
- Disseminating newsletters/publications;
- Organising training and promotional activities.

1.4. How do we ensure the security of personal data?

TIS implements various security measures, including encryption and authentication tools, to safeguard the security, integrity, and availability of personal data. While data transmission over the internet cannot be entirely secure, TIS, along with its service providers and business partners, continuously strives to implement and maintain physical, electronic, and procedural safeguards in compliance with applicable data protection standards. Key measures include:

- Restricted access to personal data based on the "need-to-know" principle;
- Encrypted data transfer;
- Secure storage of confidential data (e.g., phone numbers, email addresses);
- Protection of IT systems with firewalls to prevent unauthorised access;
- Continuous monitoring of IT system access to prevent misuse.

Third-party service providers processing personal data on TIS's behalf must implement adequate technical and security measures as required by law.

1.5. How long do we retain personal data?

TIS retains personal data only for the time necessary to achieve the purposes for which it was collected, in compliance with maximum retention periods imposed by contractual, legal, or regulatory obligations.

For example:

- One month after the project's completion, defined as client approval. Data related to billing must be retained for at least 10 years for tax compliance purposes.
- Data collected through interviews, focus groups, workshops, or surveys are anonymised or securely destroyed

For customer service and marketing purposes, data are retained until explicit withdrawal of consent.

1.6. What are the data subject's rights?

Data subjects have several rights under applicable laws, including:

- Right of access: Obtain information about data processing activities and associated details.
- Right of rectification: Request correction of inaccurate or outdated data.
- Right to erasure ("right to be forgotten"): Request deletion of data if there are no valid grounds for retention.
- Right to restrict processing: Limit the processing of data for specific categories or purposes.
- Right to object: Object to data processing, including for direct marketing.

These rights can be exercised by contacting dpo@tis.pt.

1.7. Data sharing

1.7.1. Who do we share your personal data with?

Depending on the purpose, TIS may share data with third parties, including national and international public entities and private organisations, to fulfil legal, regulatory, contractual, or public interest obligations.

Data may also be accessed by TIS service providers who are necessary for the execution of the outlined purposes, particularly for data collection services. TIS ensures that it only works with service providers that guarantee the implementation of technical and organisational measures to protect personal data and explicitly agree to comply with TIS-imposed standards.

1.7.2. Transfers of personal data outside the EEA

TIS may occasionally transfer personal data to third countries (outside the European Economic Area - EEA). In such cases, TIS ensures that data transfers comply with applicable legal standards.

1.8. Cookie policy

1.8.1. What are cookies?

Cookies are small text files containing relevant information downloaded to your access device (computer, mobile phone, or tablet) via your web browser when visiting a website. These files store information about user visits.

Cookies used on tis.pt do not collect personal information that can identify the user. They are employed to gather statistical data to analyse website functionality and user navigation experience. Types of cookies include:

- Analytical cookies: Gather anonymous information about user browsing behaviour.
- Third-party cookies: Enable the website to remember preferences such as language and region and collect user information to tailor advertising to their interests.

The privacy policies of third-party cookies can be accessed at:

- Google: Google Privacy Policy

1.8.2. Disabling cookies

All web browsers allow users to accept, decline, or delete cookies through appropriate settings. Users can disable cookies on **tis.pt** at any time by changing their browser settings.

However, disabling cookies may affect the proper functioning of some web services, partially or entirely impeding navigation. Here are links to manage cookies in common browsers:

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Apple Safari

1.9. Legislation

The processing of personal data by TIS, including electronic communications for commercial purposes, complies with national and European legislation, including:

- General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons regarding personal data processing and free data movement.
- Law No. 58/2019 – Ensuring the implementation of GDPR in the national legal systems

1.9.1.1. Amendments to the privacy policy

This Privacy Policy may be reviewed in light of changes to applicable legislation at any time, without prior notice, and may take immediate effect. Changes will be publicised on our website **www.tis.pt**. Renewed consent will be sought if necessary.

2. DATA MANAGEMENT PLAN (DMP)

According to the European Commission, "Personal Data" refers to any information about an individual, related to their personal, professional, or public life, allowing for direct or indirect identification.

The Data Management Plan (DMP) outlines the aspects of data creation, storage, backups, documentation, preservation, and access. It is a living document that describes how data are treated, identifying creation and documentation processes, access permissions, reuse, and storage locations.

Information collected varies depending on its purpose, with TIS collecting information from its employees, clients, and partners.

2.1. Employee information management

Within this DMP, the management of employee information is structured across three mediums: the Information System, Digital Archive, and Physical Archive.

Management (both at the Department and Human Resources levels), members of the Board of Directors, and staff assigned to the Accounting and IT Support Services have access to all employee data.

Each employee has access to their Individual Employee Record in the Information System (PHC).

2.1.1. Objective

Collected data aim to manage Human Resources.

2.1.2. Information system

Employee data are registered in the Information System (PHC), stored internally on the server, and collected during the hiring process.

The employee record includes the following information:

Mandatory:

- Short Name
- Full Name
- Initials
- Date of Birth
- Address
- Postal Code
- Tax Identification Number
- Social Security Number
- Bank Account Number (IBAN)
- Number of Dependents
- Emergency Contact
- ID Type
- ID Document Number
- Job Title
- Academic Qualifications
- Nationality
- Marital Status
- Gender (options: female, male, other, prefer not to say)
- TIS Email Address
- Admission Date
- Contract Type (Permanent, Fixed-term, Intern, Freelancer, Indefinite)
- Contract Duration (in months)
- Current Salary
- Contract End Date
- Termination Date
- Disability Status
- Administrator Status
- Membership of Governance Bodies

Optional:

- Personal Phone Number
- Personal Email Address
- Additional Qualifications

- Spouse's Name, Tax Identification Number, and Social Security Number
- Disability Status of Spouse or Dependents
- Children's Names, Tax Identification Numbers, and Social Security Numbers

2.1.2.1. Internal data management

Collected data are managed and updated by Human Resources (HR) and the Accounting Service. HR leadership is responsible for ensuring data integrity. Employees can access their records in the Information System and must notify HR or Accounting for updates. Data access is restricted to authorised personnel, including HR, Accounting, IT Support, and Administration.

All non-essential data must be deleted within two months after an employee's departure.

2.1.3. Digital archive

For each TIS employee, the following are stored digitally:

- Curriculum Vitae
- Employment Contract
- Copy of ID Card
- Criminal Record
- Academic Certificates

These are collected at hiring and updated as necessary. Data are stored in a secure network folder managed by HR.

2.1.3.1.1. Internal data management

HR is responsible for maintaining the records. When updates occur, previous versions are deleted by HR. All employees have access to CVs and academic certificates for project submissions and management. Upon departure, unnecessary data are deleted within two months.

2.1.4. Physical archive

The following are stored physically for each TIS employee:

- Curriculum Vitae
- Employment Contract

- Copy of ID Card
- Criminal Record
- Academic Certificates

These are collected at hiring and updated as necessary. Data are stored in a locked cabinet managed by HR and IT Support Services (SAI).

2.1.4.1. Internal data management

HR is responsible for maintaining and updating records. Outdated versions are destroyed by HR. Access is restricted to HR and Administration. Upon employee departure, unnecessary data are destroyed within two months.

2.1.5. Data shared with third parties

2.1.5.1. Website

Employee identification data are publicly shared via the TIS website:

- Shared Information: Name, photo, and brief CV.
- Purpose: Team presentation.
- Transfer: Data are manually entered on the website, hosted within the EEA.

2.1.5.2. Accounting services

Data from the Employee Record are shared with external accountants:

- Shared Information: Complete Employee Record and Employment Contract.
- Purpose: Payroll processing and Social Security registration.
- Transfer: Records are scanned and emailed manually.

2.1.5.3. Occupational health and safety services

Employee data are shared with the company responsible for occupational health and safety:

- Shared Information: Full name, date of birth, admission date, category, and job title.
- Purpose: Scheduling health check-ups in compliance with legal requirements.
- Transfer: Data are emailed to the service provider.

2.1.5.4. Health insurance

Employee data are shared with the health insurance provider:

- Shared Information: Information requested in the insurer's form, completed and signed by the employee.
- Purpose: Including employees (and optionally family members) in the TIS health insurance scheme.
- Transfer: Data are emailed using the insurer's form.

2.1.5.5. Banks and insurers

Employee data are shared with banks for corporate credit and meal cards:

- Shared Information: Information requested in the bank's form, signed by the administrator, plus a copy of the ID card.
- Purpose: Issuing corporate credit cards and meal cards.
- Transfer: Data are submitted manually, with ID copies sent via internal mail.

2.1.6. Access control

Upon hiring, employees are granted access to their Employee Record in the Information System through a username and password.

HR, Accounting, IT Support, and Administration staff have access to all employee data. Upon termination, access is revoked:

- Return of access card
- Network access deactivation
- Email account closure
- Removal from the PHC system

Additionally, regarding the TIS email account:

- The email account provided by TIS is intended solely for professional use.
- The content of emails sent or received, whether from personal or professional email accounts, that are of a personal or non-professional nature, is protected by privacy and confidentiality rights under the law and the Constitution.
- TIS commits to not accessing any employee emails if it is evident or ascertainable that the email is not of a professional nature.

- In the event of employment termination, TIS may access the employee's email account to recover information related to their commercial activities or ongoing project management

2.2. Client information management

Within this DMP, the management of client information is included, which is collected in the Information System (including the invoicing system).

TIS clients are associated with the projects they contract. Therefore, the Project Manager is responsible for collecting, ensuring the quality of the data, and entering it into the system. Staff assigned to the Accounting Service are responsible for the accuracy of the data entered into the invoicing system.

All employees have access to client data recorded in the Information System. Access to the Information System is controlled through a username and password.

2.2.1. Objective

The collected data aims to facilitate project management, invoicing, and commercial activities of TIS.

2.2.2. Collected data

Two levels of information are collected:

- Company Information: Company name, address, and Tax Identification Number (NIF). Optional details include phone numbers, general emails, and website URLs.
- Client Representative Information: Name and the organisation they work for. Optional fields include title, date of birth, academic qualifications, phone numbers, and email addresses.

2.2.3. Internal data management

Project managers are responsible for collecting and maintaining client-related project data, while Accounting staff manage invoicing-related data. All employees can access client records in the Information System using a username and password.

2.2.4. Data shared with third parties

The only shared data relate to project invoicing.

2.2.5. Impact of a data breach

As the collected information is of a public nature, there is no significant impact in the event of a data breach.

2.3. PARTNER INFORMATION MANAGEMENT

Within this DMP, the management of partner information is included, which is collected in the Information System (including the invoicing system).

Partners are defined as the companies selected by TIS to collaborate on projects. The Project Manager is responsible for ensuring the quality of the data and entering it into the system. Staff assigned to the Accounting Service are responsible for the accuracy of the data entered into the invoicing system.

The data collected is managed and updated by the Project Manager and staff assigned to the Accounting Service.

All employees have access to partner data recorded in the Information System. Access to the Information System is controlled through a username and password.

2.3.1. Objective

The collected data aim to manage and evaluate partnerships.

2.3.2. Collected data

Two levels of information are collected:

- Partner Company Information: Company name, address, and Tax Identification Number (NIF). Optional details include phone numbers, general emails, and website URLs.
- Partner Representative Information: Name and the organisation they work for. Optional fields include title, date of birth, academic qualifications, phone numbers, and email addresses.

2.3.3. Internal data management

Project managers are responsible for collecting and managing project-related partner data, while Accounting staff manage invoicing-related partner data. All employees can access partner records in the Information System using a username and password.

2.3.4. Data shared with third parties

The only shared data relate to project invoicing.

2.3.5. Impact of a data breach

As the collected information is of a public nature, there is no significant impact in the event of a data breach.

2.4. Network and information security

2.4.1. Network security

TIS employs an Active Directory Windows system to authenticate users accessing computers. A firewall manages network access and blocks unwanted traffic. An SSL VPN is available for external access to TIS systems, authenticated via Active Directory and multi-factor authentication (MFA). Daily backups are performed on user computer data.

2.4.2. Equipment management

- Employee laptops are encrypted to prevent data loss in the event of theft or loss.
- Tablets are encrypted and can be remotely wiped if lost or stolen. These do not store personal data.
- Business mobile phones are encrypted and can also be remotely wiped if lost or stolen..

2.4.3. Data stored on network/cloud

TIS uses Microsoft 365 services, including SharePoint, for network/cloud storage. Dedicated SharePoint sites are created for projects requiring access by partners and clients, ensuring restricted access to other TIS data.

Data Storage and Access Control

1. File Storage
   All project files and documents are stored on a dedicated SharePoint site, which is part of Microsoft 365 services. SharePoint is configured to ensure compliance with European data protection regulations, providing secure cloud-based storage.
2. Access Control
   - Access to the SharePoint project site and its folders is restricted to authorized personnel only. Permissions are assigned based on the principle of least privilege and managed through group memberships defined in the SharePoint admin centre.
   - Membership to project-specific folders is granted exclusively to team members actively working on the corresponding tasks.
3. File-Level Security
   SharePoint enforces file-level security with robust permissions and auditing features. Each file inherits permissions from the folder unless unique permissions are explicitly set.

Network and Infrastructure Security

4. Employee and Partner Access
   Only employees of TIS and authorized project partners have access to the project SharePoint site. Access is authenticated using Microsoft Azure Active Directory credentials with Multi-Factor Authentication (MFA) enabled.
5. Network Security
   - External access to SharePoint is managed through Azure Active Directory Conditional Access policies, ensuring secure connections from approved devices and locations.
   - SharePoint operates over HTTPS, with all data transfers encrypted using SSL/TLS protocols.
   - For internal network security, Watchguard EPDR monitors and protects against threats.

Backup and Data Recovery

6. Data Backup
   SharePoint provides automatic versioning and retention policies for files:
   - Files are backed up by Microsoft with 7-day recovery from accidental deletion.

- Version history enables recovery of up to 500 versions per file, ensuring that manipulated or deleted versions can be restored, up to 30 days. Hourly versions (versions created at the top of the hour) between 30-to-60-day period. Daily versions (versions created at the beginning of each day) between 60-to-180-day period. Daily versions (versions created at the beginning of each day) between 60-to-180-day period.

7. Retention Policy
   Deleted files are stored in the SharePoint Recycle Bin for up to 93 days, after which they can still be recovered from Microsoft's second-stage backup systems for a limited time.
8. Sensitive Data Handling
   - Files containing sensitive personal data are stored in a restricted-access library within the SharePoint site. Access is limited to team members with a specific need for this data.

Technical and Procedural Support

9. Technical Resources
   Our team is supported by experienced IT personnel who ensure secure electronic communication and delivery of project outcomes in appropriate formats. SharePoint's collaborative tools also facilitate secure and efficient document sharing and editing.
10. Data Integrity
    SharePoint automatically tracks all changes to documents and maintains a version history. In case of accidental or unauthorized modifications, up to 500 previous versions are available for restoration, ensuring data integrity.

Este documento foi sujeito ao controlo da qualidade interno de acordo com o procedimento Controlo da Qualidade de Documentos (P2/05) definido no Sistema de Gestão da TIS.pt.

* Este texto foi escrito ao abrigo do novo Acordo Ortográfico *

This document was subjected to Internal Quality Control in accordance with the Quality Control Procedure for Documents (P2/05) as defined in the TIS.PT Management System.

TIS transportes inovação e sistemas