# PERSONAL DATA PROTECTION POLICY

*Data Protection Policy adopted in transposition of Regulation (EU) 2016/679, to guarantee and safeguard the fundamental rights and freedoms of natural persons.*

| | |
|---|---|
| **TITLE** | Data Protection Policy |
| **DATE OF APPLICATION** | 10/06/2026 |
| **Author** | Data Protection Officer |
| **Reviewed by** | Technacy HR Department |
| **Approved by** | Technacy Chief Executive Officer |

## REVISION HISTORY

| Version | Date | Revised by | Nature of changes |
|---|---|---|---|
| 1.0 | 21 May 2021 | DPO – Studio Paci & C. | First issue |
| 2.0 | June 2026 | DPO – Avv. Elisa Rosso | Integration with the high-level Data Protection procedure; extension of roles, responsibilities, definitions and detailed provisions; overall harmonisation of the document. |

## CONTENTS

# 1. INTRODUCTION

**Technacy S.r.l.** (hereinafter also “Technacy”, “the Company” or “the Organisation”) pays the utmost attention to the protection of personal data processed in the course of its activities. This commitment extends to employees, customers, prospective customers, suppliers, business partners and any other party that comes into contact with the Company.

This Personal Data Protection Policy (hereinafter also the “Policy”) is intended to provide a common, coherent and harmonised framework for the protection of personal data, adopting consistent security and compliance standards in line with Regulation (EU) 2016/679 (the “GDPR”), as well as the principles, guidelines and best practices on personal data protection applicable to the Company’s operational contexts.

In particular, this document sets out the requirements, obligations and conduct to be adopted by the Data Controller, as well as by the internal privacy roles – such as the Data Protection Officer (DPO), the internal (privacy) Data Processing Managers, the Authorised Persons/Processing Operators and the System Administrators – to ensure lawful, fair and secure processing of personal data and to prevent unauthorised disclosure and/or dissemination of such data.

The Policy applies both to processing carried out by the Company as “Data Controller” and to processing carried out as “Data Processor” on behalf of its clients, and aims to guarantee adequate protection to all data subjects through the adoption of a Personal Data Management System, in compliance with the fundamental rights and freedoms of individuals.

# 2. PURPOSE AND SCOPE

The purpose of this document is to describe the Organisation’s policy, methods and general procedures for processing, as well as for the security and confidentiality of data and information.

This document applies to all processing of personal data carried out by Technacy S.r.l., whether directly or through external service providers, as well as to activities managed on behalf of third parties. The Policy applies to all internal staff and is shared with third parties that collaborate in the management of information, as well as with all processes and resources involved in the design, development, launch and ongoing delivery of services.

The following fall within the scope of application:

- all processing carried out as Data Controller or Data Processor;
- processing activities carried out in the context of services provided to public and private clients;
- processing carried out using digital, paper or mixed media.

The following are excluded from the scope of this Policy:

- processing of data relating to legal entities (e.g. companies with legal personality), including their name, legal form and corporate contact details;
- processing of data that has been irreversibly anonymised, such that it no longer allows (even indirectly) the identification of a data subject.

## 2.1. Activities of the Company

The Policy applies to the Data Controller’s principal and ancillary activities, as described in the Record of Processing Activities. The Company is engaged in the development of software, applications and integrations, in particular in the field of services ancillary to telecommunications.

Management, software development and testing activities are carried out, where technically possible, in a dedicated environment separate from the IT system used for the processing of personal data; fictitious rather than real data are normally used in testing activities. Where this is not possible, specific procedures are in place to protect the personal data used in testing and software development.

# 3. REGULATORY REFERENCES AND INTERNAL PROCEDURES

This Policy is based on the following regulatory references and internal documents.

## 3.1. Regulatory references

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (hereinafter also the “GDPR”);
- Italian Legislative Decree No. 196 of 30 June 2003 – Personal Data Protection Code, as subsequently amended;
- Italian Legislative Decree No. 101 of 10 August 2018 – Provisions adapting national legislation to the GDPR;
- Measure of the Italian Data Protection Authority of 27 November 2008 – “Measures and arrangements prescribed to data controllers of processing carried out using electronic instruments in relation to the assignment of system administrator functions”;
- Measures and Guidelines of the Italian Data Protection Authority on direct marketing and anti-spam measures, video surveillance, processing of employees’ data, and the use of e-mail and the internet;
- Guidelines of the Article 29 Working Party and of the European Data Protection Board (EDPB) on consent, data portability, the DPO, the lead supervisory authority, DPIAs, automated decision-making and profiling, and personal data breach notification;
- Italian Law No. 48 of 18 March 2008 – Ratification and implementation of the Council of Europe Convention on Cybercrime (Budapest, 23 November 2001).

## 3.2. Internal procedures and documents

This Policy is supplemented and implemented by the following internal documents, to which full reference is made for operational detail:

- Company procedure for the management of data subjects’ rights;
- Company Data Retention procedure (policy);
- Company Data Breach procedure;
- Procedure for conducting DPIAs;
- Contracts/clauses appointing Data Processors pursuant to Art. 28 GDPR;
- IT Regulations.

# 4. TERMS AND DEFINITIONS

**Ordinary personal data:** any information relating to an identified or identifiable natural person (the “data subject”). Personal data may relate only to a natural person and also includes sole traders and self-employed professionals, but does not include data relating to legal entities. A company e-mail address linked to a specific individual (e.g. firstname.surname@technacy.it) is personal data, whereas a generic e-mail address (e.g. info@technacy.it) is not considered personal data. In case of doubt as to whether information qualifies as personal data, each employee must ask their internal (privacy) Data Processing

Manager.

**Special categories of data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, and data concerning health, sex life or sexual orientation. These include in particular health data, genetic data and biometric data. The GDPR imposes greater and more specific obligations when such categories are processed.

**Judicial data:** personal data capable of revealing final decisions of the judicial authority, the register of administrative sanctions arising from criminal offences and related pending proceedings, or the status of a defendant or person under investigation pursuant to Arts. 60 and 61 of the Italian Code of Criminal Procedure.

**High-risk data:** data whose processing presents specific risks to the fundamental rights and freedoms and to the dignity of the data subject; this includes, in particular, geolocation data and video surveillance data.

**Data subject:** the natural person to whom the personal data relates (e.g. employees, suppliers, customers, users, website visitors, other parties).

**Consent of the data subject:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she agrees to the processing of personal data relating to him or her. Consent must be obtained solely on the basis of templates previously approved by the internal (privacy) Data Processing Manager; in case of doubt, the competent Manager or the DPO must be consulted.

**Profiling:** any automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person (work performance, economic situation, health, preferences, interests, reliability, behaviour, location or movements). This is considered a "high-risk" activity under the GDPR.

**Pseudonymisation:** the processing of personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures.

**Data Controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**Internal (privacy) Data Processing Manager:** a formally appointed person who has control of and responsibility for the processing carried out within their area/department, ensuring compliance with the law and ensuring appropriate access to personal data and IT systems.

**Data Protection Officer (DPO):** the person appointed by the Company pursuant to Arts. 37 et seq. of the GDPR, involved in all matters relating to the processing of personal data for which the Company acts as Controller or Processor.

**Authorised Persons/Processing Operators:** natural persons (employees and/or other third parties) authorised to carry out processing operations on personal data of which the Company is the Controller.

**System Administrator:** a professional figure dedicated to managing or maintaining processing infrastructures or their components through which personal data is processed (database management systems, complex base software, e-mail and telephony systems, networks and security systems), to the extent that they allow intervention on personal data.

**Data Processor (external):** the natural or legal person, public authority, agency or other body that processes personal data on behalf of the data controller (e.g. payroll management companies, IT infrastructure providers).

**Third party:** a natural or legal person, public authority, agency or other body other than the data subject.

**Processing:** any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, comparison, restriction, erasure or destruction.

**Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Dissemination:** making personal data known to an indeterminate number of parties, in any form, including by making it available for or open to consultation.

**Communication:** making personal data known to one or more specific parties other than the data subject, the controller, the processor and the authorised persons, in any form.

**Supervisory Authority:** in Italy, the Garante per la protezione dei dati personali (Italian Data Protection Authority). More generally, the national authority responsible for verifying compliance with data protection legislation.

**Adequate security measures:** the set of technical, IT, organisational, logistical and procedural measures appropriate for protecting data in relation to the level of risk associated with the processing.

**Record of Processing Activities:** the document drawn up by the Company that maps the processing of personal data carried out by paper-based and electronic means.

**Privacy Legislation:** the Italian Privacy Code, the GDPR and any other applicable data protection legislation, whether already in force or yet to enter into force, including the measures, guidelines and opinions of the Italian Data Protection Authority, the EDPB and any other competent authority.

# 5. ROLES AND RESPONSIBILITIES

## 5.1. Data Controller

The Data Controller is responsible for:

- appointing and revoking the internal (privacy) Data Processing Manager for the proper coordination of the Company's processing activities;
- signing non-delegable acts;
- overseeing compliance with privacy legislation and related obligations, delegating this task to the internal Data Processing Managers;
- implementing the obligations relating to the protection of personal data set out in the GDPR and in Italian Legislative Decree No. 196/2003, as amended;
- overseeing the processing operations carried out within the Company in order to ensure their compliance with statutory provisions.

## 5.2. Data Protection Officer (DPO)

The Company has appointed Avv. Elisa Rosso as Data Protection Officer, who can be contacted at dpo@technacy.it.

The appointment of a DPO, pursuant to Art. 37 of the GDPR, is mandatory in specific cases (processing carried out by a public authority or body; core activities requiring regular and systematic monitoring of data subjects on a large scale; large-scale processing of special categories of data or data relating to criminal convictions and offences). In the absence of a specific obligation, the Regulation allows for the voluntary appointment of a DPO; in such cases, the same provisions of Arts. 37–39 GDPR apply. Reference is made to the Guidelines on the DPO (WP243), as confirmed by the EDPB.

The DPO is responsible for:

- informing and advising the Controller and the employees who carry out processing about their obligations under the GDPR and other data protection legislation;
- monitoring compliance with the GDPR and with the Controller's data protection policies, including the assignment of responsibilities, awareness-raising and staff training;
- preparing, in collaboration with the internal (privacy) Data Processing Managers, amendments and corrections to this Policy and to other procedures, in order to preserve their consistency;
- monitoring training and information activities for persons authorised to process data;
- cooperating in the preparation and review of privacy notices, consent forms and data-processor appointments;
- periodically verifying the proper maintenance of the record of processing activities, the data-breach register and the list of data processors;
- cooperating in responding promptly to requests for the exercise of data subjects' rights;
- providing advice as part of DPIAs pursuant to Art. 35 GDPR and supervising their performance;
- cooperating with the Supervisory Authority and acting as a point of contact, including for the purposes of prior consultation under Art. 36 GDPR.

All communications to the competent Supervisory Authority are kept on file at the DPO's office.

## 5.3. Internal (privacy) Data Processing Manager

Internal (privacy) Data Processing Managers act in accordance with directives issued by the Data Controller and have control of and responsibility for the processing carried out within their area/department. In particular, they are responsible for:

- ensuring compliance with current legislation within their function/area, with particular regard to the existence of an appropriate legal basis for each processing operation;
- overseeing the implementation of the technical and organisational security measures required by law;
- overseeing the updating/mapping of processing operations and keeping the Record of Processing Activities up to date, flagging any transfers of data outside the European Economic Area (EEA);
- overseeing, where necessary, the impact and risk assessment processes for the processing operations within their remit;
- ensuring the participation of Authorised Persons in training plans/courses;
- identifying any external Data Processors and overseeing the proper performance of their duties, including through periodic checks and inspections;
- informing the Controller of any personal data breaches and any non-conformities identified;
- assisting with the updating of privacy notices and consent forms, including in relations with external suppliers;
- supporting the handling of requests from data subjects under Arts. 15–22 GDPR;
- keeping the data-breach register up to date;
- preparing, with the assistance of the relevant functions, the DPIAs referred to in the dedicated section below;
- collaborating with company functions to ensure compliance with the principles of privacy by design and by default;
- referring the most significant issues relating to the processing of personal data to the DPO.

### 5.4. Authorised Persons/Processing Operators

These are all employees and collaborators who, acting under the authority of the internal (privacy) Data Processing Manager for their area, process personal data. They are responsible for:

- carrying out processing activities in accordance with the instructions received;
- not modifying existing processing or introducing new processing without the express authorisation of their Manager;
- complying with security rules for data protection;
- promptly informing the internal (privacy) Data Processing Manager of any personal data breach of which they become aware or which they suspect;
- taking part in the training courses organised by the Company.

Upon hiring or signing a collaboration agreement, each employee or collaborator receives and expressly accepts, in addition to the notice on the processing of their own personal data, this Policy as well. Each user is responsible for regularly completing the privacy training made available by the Company; failure to comply with this obligation may result in disciplinary action.

### 5.5. System Administrators

System Administrators are responsible for maintaining and managing the processing infrastructures, or their components, through which personal data is processed. For details of their appointment and the verification of their work, reference is made to the dedicated “Appointments” section of Confluence at

https://technacy.atlassian.net/wiki/spaces/ADS/overview.

### 5.6 System Operators

System Operators are responsible for managing and overseeing the correct functioning of the systems and applications entrusted to them, operating on the Company's instructions. For details of their appointment and the verification of their work, reference is made to the dedicated "Appointments" section of Confluence at https://technacy.atlassian.net/wiki/spaces/ADS/overview.

### 5.7. Organisational roles and training

The roles defined within the Organisation are: administration, customer support, sales and marketing, management, system engineers, developers, system administrators and system operators.

Pursuant to Art. 29 of the GDPR and Art. 2-quaterdecies of Italian Legislative Decree 196/2003, all persons authorised to process data must be duly instructed and trained on their duties, responsibilities and processing operations, and bound to confidentiality. Training is characterised as follows:

- **Specific** – corresponding to the type of duties/role performed;
- **Appropriate** – in relation to the type of processing carried out;
- **Ongoing** – scheduled and periodically updated, in particular for new hires;
- **Documented** – its delivery and subsequent updates must be evidenced by registers, certificates or other records;
- **Effective** – understanding and adoption of the procedures must be periodically verified.

## 6. GENERAL PROVISIONS FOR THE PROCESSING OF PERSONAL DATA

### 6.1. Processing of personal data

Personal data may only be processed for the purposes set out in the Privacy Notice given to the data subject at the first useful contact and in compliance with the individual appointments of authorised persons. In general, data must be:

- processed lawfully, fairly and transparently;
- collected and recorded for specified, explicit and legitimate purposes, and used in a manner compatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected or processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which it is processed;
- processed in a manner that ensures appropriate security, by means of suitable technical and organisational measures.

Personal data may not be disclosed to third parties unless the data subject has given express consent or another legal basis exists (for example, third parties whose involvement is necessary for the performance of the contract, such as consultants or payroll providers who process the data as Processors). For transfers abroad, reference is made to the dedicated section.

### 6.2. Classification of personal data

Personal data is classified under the GDPR into the following categories:

- ordinary personal data;
- special categories of personal data (Art. 9 GDPR);
- data relating to criminal convictions and offences or related security measures (Art. 10 GDPR), which may only be processed under the control of a public authority or where authorised by EU or Member State law;
- high-risk data (relating to profiling, geolocation, video surveillance and behavioural data);
- authentication data (codes, passwords or PINs enabling physical or logical access to systems, applications or premises).

## 6.3. Principles and rules of processing

Pursuant to Arts. 5 and 24 of the GDPR, the processing of personal data must comply with the following principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality. These principles and safeguards are also applied and verified down the chain to any sub-processors.

### *Lawfulness, transparency and fairness*

Processing is lawful only if at least one of the following legal bases applies: consent of the data subject; performance of a contract or pre-contractual measures; compliance with a legal obligation; protection of vital interests; performance of a task carried out in the public interest; legitimate interest of the controller or of third parties, provided that this does not override the rights and freedoms of the data subject. Consent is therefore only one of the legal bases, not the only one. For purposes other than those of the contract to which the notice relates (e.g. marketing), express and separate consent must be obtained, documented and recorded.

### *Purpose limitation*

Data must be collected for specified, explicit and legitimate purposes and subsequently processed in a manner that is not incompatible with those purposes. The introduction of a new purpose requires the prompt sharing of updated documentation (notice and, where applicable, consent) with data subjects.

### *Data minimisation*

Data must be adequate, relevant and limited to what is necessary in relation to the purposes pursued. Where it is not possible to use anonymous or aggregated data, the use of personal data must be kept to a minimum.

### *Accuracy*

Data must be accurate and, where necessary, kept up to date; procedures must be in place for the prompt erasure or rectification of inaccurate data.

### *Storage limitation*

Data must be kept in a form which permits identification of data subjects for no longer than is necessary to achieve the purposes pursued.

### *Integrity and confidentiality*

Personal data must be processed in a manner that ensures its integrity and confidentiality, preventing unauthorised access or use.

## 6.4. Privacy Notice

Data subjects must receive an appropriate Privacy Notice. When data is collected directly from the data subject, the notice is provided under Art. 13 of the GDPR at the time of collection. When data is obtained through third parties, the notice is provided under Art. 14: within a reasonable period and in any event no later than one month; at the latest at the time of first contact, where the data is used to communicate with the data subject; no later than the first disclosure, where the data is to be disclosed to another recipient.

Updating the notices is the responsibility of the relevant internal (privacy) Data Processing Manager, who consults with the DPO. No changes may be made to adopted notices without the prior written approval of the internal (privacy) Data Processing Manager and/or the DPO.

#### *6.4.1. Direct notice (Art. 13 GDPR)*

Where data is collected from the data subject, the notice contains, among other things: the identity and contact details of the Controller; the DPO's contact details; the purposes and legal basis of the processing; any legitimate interests pursued; any recipients; any intention to transfer data to third countries and the related safeguards; the retention period; the data subject's rights; the right to withdraw consent; the right to lodge a complaint with the Supervisory Authority; whether the provision of data is mandatory or optional; and the existence of any automated decision-making process.

#### *6.4.2. Subsequent notice (Art. 14 GDPR)*

Where data is not collected from the data subject, the notice, provided within a reasonable period not exceeding one month, contains, in addition to the information set out under Art. 13, the categories of data collected and the source of such data. The notice is not required where the data subject already has the information, where the recording of data is expressly required by law, or where providing the information proves impossible or would involve a disproportionate effort.

#### *6.4.3. Further notice (new purposes)*

When new purposes are introduced, a specific further notice is provided to the data subject before processing for the new purpose begins. The internal (privacy) Data Processing Managers concurrently update the record of processing activities.

### 6.5. Processing of the Company's personal data

Processing mainly concerns data relating to employees, customers, suppliers, persons subject to video surveillance systems and website visitors.

#### *6.5.1. Employees*

The personal data of employees, both prior to and during the employment relationship, is collected from each employee and, only where necessary, from third parties, for purposes connected with recruitment and with the establishment and management of the employment relationship. The Company processes such data, even without consent, where necessary to comply with contractual, statutory or collective-bargaining obligations, as well as to defend a right in legal proceedings and to protect the employee's health. In other cases, express consent is obtained.

#### *6.5.2. Access to data in the absence of the Authorised Person (emergency access)*

Where it is necessary to access data and/or electronic devices assigned to an absent employee (e.g. termination of employment, illness, death), the employee's direct line manager, having verified that no alternative is available, submits a written request for access to the internal (privacy) Data Processing Manager. The internal (privacy) Data Processing Manager, having verified the request, provides instructions and informs the Information Systems Manager. At the end of the operation, the requesting party provides written confirmation and, where possible, informs the absent authorised person.

#### *6.5.3. Customers*

Customers are informed, by means of specific notices, of the processing of their personal data, both for commercial and for contractual purposes.

#### *6.5.4. Suppliers appointed as Data Processors under Art. 28 GDPR*

For suppliers appointed as Data Processors, the Company uses their data exclusively for contractual purposes.

#### *6.5.5. Website visitors*

Website visitors are informed, through a specific notice and any cookie policy available on the corporate websites, of the data recorded during connection, browsing, registration and/or completion of forms.

#### *6.5.6. Video surveillance*

Where video surveillance systems are installed, data subjects are informed of the relevant processing arrangements through specific notices, provided both in extended form and by means of appropriate signage placed before the range of the cameras.

## 7. RIGHTS OF THE DATA SUBJECT

The Company makes available to data subjects a postal address and an e-mail address through which they may exercise the rights set out in Chapter III of the GDPR (Arts. 15–22): access, rectification, erasure, restriction, portability, objection, and the right not to be subject to automated decision-making, including profiling.

The Organisation has adopted a specific Procedure for the Management of Data Subjects' Rights, to which reference is made for operational detail. In summary, the procedure governs:

- the receipt of requests (by e-mail, web form, ordinary post);
- verification of the requester's identity before acting on the request;
- response times: one month from receipt, extendable by a further two months (up to a maximum total of three months) in cases of particular complexity or a high number of requests, with the data subject to be informed of the extension within the first month; a response is due even where the request is refused;
- recording of each request and its outcome in a dedicated internal register;
- arrangements for involving the DPO in cases of legal uncertainty or potential conflict between the rights of the data subject and statutory obligations.

If an employee receives a request for the exercise of rights, they must immediately notify their internal (privacy) Data Processing Manager.

## 8. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES (ART. 32 GDPR)

The Organisation adopts technical and organisational measures appropriate to the level of risk, pursuant to Art. 32 of the GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risk to the rights and freedoms of natural persons.

Depending on the risk assessment, the Company adopts, or undertakes to adopt, the following measures, by way of example and not exhaustively:

- encryption of personal data in transit and at rest, where technically applicable;
- pseudonymisation of data in development and testing contexts;
- role-based access control (RBAC) and multi-factor authentication (MFA) for critical systems;
- regular back-up procedures with periodic testing of restoration;
- Business Continuity and Disaster Recovery plans, tested periodically;
- periodic vulnerability assessment and penetration testing activities;
- monitoring and logging of access to processing systems.

The adequacy of these measures is reviewed at least annually and whenever significant changes are made to systems or processing operations. Measures are enhanced for processing involving special categories of data, in accordance with the principle of proportionality.

## 9. CONTRACTS: APPOINTMENT OF THIRD-PARTY SUPPLIERS AS DATA PROCESSORS (ART. 28 GDPR)

Whenever a supplier or, more generally, an external party has access to personal data processed by the Company, it must be appointed as a Data Processor pursuant to Art. 28 GDPR, following verification of its suitability to process personal data in compliance with applicable Privacy Legislation, by means of any checks required by the internal (privacy) Data Processing Manager in conjunction with the DPO.

Where the checks show that the supplier is unable to provide sufficient technical and/or organisational guarantees, the contract may not be signed. Where the outcome is positive, the manager of the relevant company function obtains the approval of the internal (privacy) Data Processing Manager to sign the Art. 28 GDPR appointment letter. Once the verification has been completed and the appointment signed, the internal (privacy) Data Processing Manager updates the list of data processors and notifies the DPO of the appointment; a copy of the appointment is retained by the Company.

These principles and safeguards are verified for every supplier whose service involves the processing of personal data, including through periodic audits and systematic monitoring of the state of implementation of the safeguards. The safeguards are applied and verified down the chain to any sub-processors as well.

It should be noted that, where Technacy processes personal data on behalf of a Client, it is the Company itself that must receive the appointment as Data Processor under Art. 28 GDPR.

## 10. PRIVACY BY DESIGN AND PRIVACY BY DEFAULT (ART. 25 GDPR)

The internal (privacy) Data Processing Manager monitors the correct processing of personal data, and its accuracy, reliability and currency, both at the point of acquisition and during processing. Each new type of processing is reported to the internal (privacy) Data Processing Manager, who assesses whether the DPO should be involved and whether the record of processing activities should be updated.

Where a new activity is to be carried out, or a product or service involving the processing of personal data is to be developed or updated, the following principles must be observed:

- **Privacy by design**: every project or product must be developed taking data protection issues into account from the design stage, determining appropriate technical and organisational measures on the basis of a risk assessment;
- **Privacy by default**: every project or product must ensure that, by default, only the personal data necessary for each specific processing purpose is processed (in terms of data quality, scope of processing, retention period and accessibility), preventing data from being made accessible to an indefinite number of people without the involvement of the individual concerned.

To this end, the user coordinates with their internal (privacy) Data Processing Manager, who in turn coordinates with the DPO to assess whether a DPIA should be carried out and whether other departments should be involved in the risk analysis and in defining the action plan. At the end of the project, the internal (privacy) Data Processing Manager, together with the DPO, carries out a general assessment of the new product or service's compliance with GDPR principles. No new products, services, tools or features involving the processing of personal data may be developed without following these guidelines.

## 11. PROCESSING OF SPECIAL CATEGORIES OF DATA (ART. 9 GDPR)

The Organisation, in its capacity as Data Controller, may process special categories of data; in such cases, it identifies in advance an appropriate legal basis from among those set out in Art. 9(2) of the GDPR (including the explicit consent of the data subject; obligations under employment and social security law; occupational medicine or health-care purposes; reasons of substantial public interest in the area of public health).

On occasion, in its capacity as Data Processor on behalf of clients, the Company may also find itself – albeit sporadically – processing special categories of personal data under Art. 9 of the GDPR (e.g. health data, biometric data, data relating to ethnic origin) depending on the nature of the services provided. In such cases:

- the Record of Processing Activities expressly indicates the type of special data processed for each client/processing operation;
- the Art. 28 GDPR contracts with client controllers specify the applicable instructions and the enhanced security measures required;
- the technical and organisational measures adopted for such processing are enhanced compared to the standard, in accordance with the principle of proportionality;
- the need to carry out a DPIA is systematically assessed before the start, or before any modification, of processing involving special categories of data.

## 12. MANAGEMENT OF PERSONAL DATA BREACHES (ARTS. 33–34 GDPR)

Articles 33 and 34 of the GDPR set out the requirements of the privacy-incident management process. Such an incident is defined as a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed, or to its unavailability.

A breach, if not addressed adequately and promptly, may cause physical, material or non-material damage to individuals (loss of control over their data, discrimination, identity theft or fraud, financial loss, reputational damage, etc.).

The GDPR requires the Controller to notify the Supervisory Authority of a breach within 72 hours (or otherwise without undue delay). Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, they too must be informed without delay. To this end, the Organisation maintains an incident register (data-breach register).

Anyone who becomes aware of a case, even merely suspected, of a personal data breach must report it as soon as possible to their internal (privacy) Data Processing Manager and follow the steps set out in the dedicated Data Breach Procedure, to which full reference is made.

## 13. DATA PROTECTION IMPACT ASSESSMENT (DPIA) (ART. 35 GDPR)

Pursuant to Art. 35 of the GDPR, the Controller is required to carry out a Data Protection Impact Assessment (DPIA) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. The obligation to carry out a DPIA arises, in particular, where at least two of the high-risk factors identified by the EDPB (Guidelines WP248 rev. 01) are present:

- systematic evaluation or scoring, including profiling;
- automated decisions producing legal effects or significantly affecting the data subject;
- systematic monitoring, including of publicly accessible areas;
- large-scale processing of special categories of data (Art. 9) or of data relating to criminal convictions and offences (Art. 10);
- large-scale processing of data;
- matching or combining datasets;
- data concerning vulnerable subjects (in particular minors);
- innovative use or application of new technologies;
- processing that prevents data subjects from exercising a right or making use of a service or contract.

Reference is also made to the list of processing operations requiring a DPIA published by the Italian Data Protection Authority pursuant to Art. 35(4) of the GDPR. The Organisation has adopted a Procedure for Conducting DPIAs, to which reference is made. The DPIA is carried out before the processing begins and, where necessary, with consultation of the DPO; the results are documented and kept on file.

Where the DPO assesses that the processing presents a high risk in the absence of mitigating measures, the Supervisory Authority is consulted in advance pursuant to Art. 36 of the GDPR.

## 14. RECORD OF PROCESSING ACTIVITIES (ART. 30 GDPR)

The Organisation draws up and maintains an up-to-date Record of Processing Activities, both in its capacity as Controller and as Processor. Although Art. 30(5) of the GDPR provides a formal exemption for organisations with fewer than 250 employees, this exemption is in practice inapplicable to Technacy S.r.l., since the Company:

- carries out processing that is not occasional, within the context of services provided continuously to its clients;
- processes data on behalf of third parties as a data processor, including processing that may involve special categories of data under Art. 9 GDPR;
- operates in the telecommunications and software development sector, with processing that, by its nature and scale, makes the record mandatory.

The Record contains, among other things: the name and contact details of the Controller (and any joint controller, representative and internal Manager); the purposes of the processing; a description of the categories of data subjects and personal data; the categories of recipients; any transfers to third countries and the related safeguards; the erasure timeframes for the various categories of data; and a general description of the security measures adopted.

The Record is kept under the responsibility of the internal (privacy) Data Processing Manager, who is responsible for keeping it up to date for their area. Any change is reported to the DPO. The Record constitutes a permanent accountability tool and is made available to the Supervisory Authority upon request.

## 15. RETENTION PERIODS (ARTS. 5 AND 17 GDPR)

Personal data is processed for the time strictly necessary to fulfil the purpose set out in the Privacy Notice. The specific retention periods for each category of processing, as well as the methods of erasure or anonymisation at the end of the retention period, are set out in the Data Retention Procedure, to which full reference is made.

The procedure also sets out the internal managers responsible for carrying out erasure activities and the methods for verifying and documenting them. All users are required not to use data after the expiry of the relevant retention period and to report to their internal (privacy) Data Processing Manager any expiry not followed by erasure/anonymisation.

## 16. TRANSFERS OF DATA TO THIRD COUNTRIES (ARTS. 44–49 GDPR)

In the course of its activities, the Controller tends not to transfer personal data to countries outside the EU. Should the need arise, data subjects are informed in advance and appropriate safeguards are adopted, which, depending on the circumstances, may include:

- verification of the existence of an adequacy decision of the European Commission for the destination country (Art. 45 GDPR); these include the EU–US Data Privacy Framework, adopted by Commission Implementing Decision (EU) 2023/1795 of 10 July 2023, with verification of the recipient's certification in the official DPF register prior to transfer;
- execution of standard contractual clauses adopted by the European Commission (Art. 46(2)(c) GDPR);
- adoption of supplementary measures where necessary, in accordance with EDPB Recommendation 01/2020 and subsequent updates;
- by way of derogation from the above safeguards, for specific types of processing (Art. 49 GDPR), verification of the existence of a contract or pre-contractual measures in the interest of the data subject, or the acquisition of explicit consent to the transfer.

The Organisation periodically reviews the adequacy of the safeguards adopted, including in light of regulatory and case-law developments, updating its measures whenever the relevant framework changes.

## 17. MONITORING AND CONTROL

For organisational and business reasons, and to protect company assets, the Company may need to monitor the use of its ICT systems. Such activity does not constitute monitoring of employees and is carried out in compliance with Italian law on workers' rights and data protection. As set out in more detail in the IT Regulations, to which full reference is made, the reasons for such checks include: identifying and preventing unauthorised access or communications; ensuring compliance with laws and regulations; preventing and identifying criminal activity; controlling viruses and malicious code; ensuring business continuity; investigating, where suspected, instances of inappropriate use or breaches; responding to complaints; and carrying out disciplinary or legal investigations.

Monitoring is carried out only to the extent permitted or required by law and where necessary and justifiable. Information identified (including personal data) may be used and retained for the duration of any proceedings and disclosed to third parties where necessary. Use of IT systems that does not comply with this Policy may result in disciplinary sanctions.

## 18. MANAGEMENT OF RELATIONS WITH SUPERVISORY AUTHORITIES

The DPO is the sole point of contact for relations with privacy Supervisory Authorities and coordinates the related communication process. The Company's individual functions cooperate, where necessary, in relation to communications with the Italian Supervisory Authority and, where applicable, with the authorities of other countries. Relations with the Authorities include, in particular: prior consultation where processing entails a high residual risk; notification of data breaches; and representing the Company in any audits conducted by the Authorities.

## 19. GENERAL CONDITIONS FOR IMPOSING PENALTIES

The effective operation of this Policy is ensured by an appropriate disciplinary system, which may sanction failure to comply with, and breaches of, the rules contained herein, irrespective of any criminal proceedings

that may also be brought.

Art. 83 of the GDPR sets out the criteria for imposing administrative fines, taking into account, among other things: the nature, gravity and duration of the infringement; whether it was intentional or negligent; measures taken to mitigate the damage; the degree of responsibility; any relevant previous infringements; the degree of cooperation with the Authority; the categories of data affected; the manner in which the infringement became known to the Authority; and adherence to codes of conduct or certification mechanisms.

Breaches of the obligations of the Controller and the Processor (Arts. 8, 11, 25–39, 42 and 43 GDPR) are subject to fines of up to €10,000,000 or, for undertakings, up to 2% of total worldwide annual turnover, whichever is higher. Breaches of the basic principles of processing, data subjects' rights and the rules on transfers (Arts. 5, 6, 7, 9, 12–22 and 44–49 GDPR) are subject to fines of up to €20,000,000 or, for undertakings, up to 4% of total worldwide annual turnover, whichever is higher.

## 20. RESPONSIBILITY FOR THE ADOPTION OF THE POLICY

The Organisation, both as Controller and as Processor, is responsible for its data protection policy, in line with developments in the business and market context, assessing the actions to be taken in response to events such as:

- significant developments in the business;
- new threats compared to those considered in the risk-assessment process;
- significant security incidents;
- developments in the regulatory or legislative framework on secure data processing;
- the use of new technologies.

## 21. REVIEW AND UPDATE OF THE POLICY

A review is carried out periodically, at least once a year, to verify the efficiency, effectiveness and adequacy of the technical and organisational measures applied. The instructions provided to staff assigned to processing constitute company policy on data processing and are reviewed and/or updated at least once a year.

In addition to the ordinary review, an extraordinary revision of this Policy is provided for upon the occurrence of one or more of the following events: significant regulatory changes; adoption of new processing technologies; a critical outcome of a DPIA; a particularly serious personal data breach; an internal audit or inspection by the Supervisory Authority. The outcome of the review and any amendments made are documented in the Revision History at the beginning of this document.

## 22. METHODS OF DISTRIBUTION OF THE POLICY

Technacy S.r.l. publishes and distributes this Policy to its staff and collaborators, including through internal information channels (e.g. the corporate intranet), ensuring that it is brought to the attention of all persons authorised to process data and shared, where relevant, with the third parties involved.

VAT No.: 02399920392 | E-mail: info@technacy.it | Website: www.technacy.it

**For approval – Data Controller**

_____

*(Date, Stamp and Signature)*

Cervia, 24 June 2026