PRIVACY ORGANIZATIONAL MODEL FOR THE PROTECTION OF PERSONAL DATA

HUMAN TECHNOPOLE FOUNDATION

SUMMARY

-GENERAL PART-

SECTION ONE

1. REGULATION (EU) 2016/679 (GDPR)

1.1. ADAPTATION OF NATIONAL LEGISLATION

The EU Regulation no. 2016/679, the General Data Protection Regulation (hereinafter also "Regulation" or "GDPR") is a legal act of European Union law whereby the European Commission intends to strengthen and unify the protection of personal data within the borders of the European Union (EU).

The new European Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data, which entered into force on 24 May 2016 and applies directly within the member States as of 25 May 2018, introduces a series of obligations aimed at ensuring the proper and lawful processing of personal data by organizations, in their capacity as Data Controllers and/or Data Processors.

In Italy the process of adaptation to the GDPR was conducted through the adoption of Legislative Decree no. 101 of 10 August 2018, in force as of 19 September 2018, which intervened on the existing Legislative Decree no. 196/2003 - the so-called Privacy Code - with joint supplementary, amending and repealing interventions.

Data subject to the GDPR are personal data, that is “identifying data” such as personal information, contact details and sensitive/particular data, such as health or political opinions and trade union membership. In general, personal data may be defined as any information relating to an identified or identifiable natural person, i.e. that can be identified directly or indirectly, a natural persons and/or individual firms (so-called “data subject”). Personal data may be processed by the data controller, i.e. the natural or legal person, the public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The controller may, in turn, appoint external and internal processors, who shall process the personal data on behalf of the controller and persons tasked with the processing who are authorised to process data, i.e. anyone acting under the authority of the controller or the processor, instructed by the latter and having access to the personal data subject to the processing.

The Regulation applies to the data of residents of the European Union and also to enterprises and bodies, organizations in general, with registered offices outside the EU that process personal data of residents of the European Union. It is therefore specified that all companies, organizations and Public Administrations present in the member States of the European Union (irrespective of whether the treatment is carried out in the EU), must comply with the legislation, including non-EU enterprises which offer services or products to natural persons in the EU territory or which simply monitor the behavior of individuals within the Union.
The adjustment to the requirements of the GDPR includes, among other privacy compliance activities, the adoption and effective and effective implementation of an “Organizational Model for the Protection of Personal Data” (hereinafter also “Privacy Organizational Model or “POM”) that allows companies, enterprises, institutions and organizations, to which the Regulation applies, to:

(i) establish a control system capable of preventing risks linked to the privacy of personal data, as identified above, and subsequently of evaluating existing controls in terms of adequacy to the requirements of the GDPR and effective operation;
(ii) promptly manage possible criticalities;

(iii) give evidence of the control system implemented in order to be exempt from liability and penalties envisaged.

1.2. GENERAL PRINCIPLES AND NEW RULES FOR THE PROCESSING OF PERSONAL DATA

The processing of personal data must be carried out in accordance with the following general principles:

- **the right to the protection of personal data**, according to which every individual has the right by which processing of his or her personal information must be carried out in a manner that ensures a high level of protection, respecting his or her fundamental rights, freedoms and dignity, with particular reference to confidentiality and personal identity;

- **the principle of lawfulness and fairness**, by which the person acting on the personal data must comply with the law on processing and ensure transparency on the part of subjects collecting data and carrying out other operations, prohibiting shams and ploys. The personal data processed in breach of the legislation on protection of personal data cannot be used;

- **the principle of purpose limitation,** whereby the collection of data must be relevant to the purpose pursued, which must be lawful, determined and not incompatible with the use of the data;

- **the principle of necessity of processing and of data use minimisation**, according to which collection and processing of data must be limited to the information required by the activity, in order to minimize the use of personal and identifying data. In fact, in the event the same purposes can be pursued without the use of personal data, processing must be carried out only for anonymous data or adopting appropriate methods which allow to identify the data subject concerned only in case of necessity;

- **the principle of proportionality,** which also provides for the verification, at every stage of processing, of whether the individual transactions are relevant and not exceeding the objectives pursued;

- **the principle of safeguarding data Integrity,** according to which personal data subject to processing must be kept and checked, also in light of the knowledge acquired on the basis of technical progress, of the nature of the information and the specific characteristics of the processing, so as to minimise the risks of destruction or loss, also accidental, of the data itself, unauthorized access or processing that is unapproved or not in accordance with the purpose of the collection, using appropriate technical and organizational measures;

- **The principle of accountability,** on the basis of which all data must be processed by the data controller in a responsible manner. The data controller must therefore demonstrate, for each processing, that he/she acted in accordance with the provisions of the GDPR. The methodological approach to be applied in order to guarantee accountability is a “risk-based” approach, i.e. an approach based on the assessment of the processing risk, which must be adopted and demonstrated by enterprises, institutions, or organizations and is of a proactive type, no longer reactive, with a focus on obligations and behaviours aimed at effectively preventing the possible event of damage. The risk inherent in processing is to be understood as a risk to data security and as a risk of negative impacts on the freedoms and rights of data subjects. These impacts must be analyzed through a specific evaluation process (e.g. Risk and Privacy Impact Assessment) taking into account the known or evident risks and the technical and organizational measures (including safety measures) to be adopted to mitigate these risks. The risk-based methodological approach must therefore follow a risk assessment

and risk management logic, in order to assess and reduce the risk posed to rights and freedoms of data subjects and identify the technical and organizational measures able to guarantee an adequate level of security;

- **Privacy by design,** which implies the need to envisage, already at the design stage of data processing, IT and application systems, the implementation of data minimization and of design logics in line with the principles being considered from the outset. Each controller must therefore ensure that the computer systems, products and/or services offered that involve the processing of personal data as well as any project initiated are, by default, protected by adequate security measures and guarantee the widest respect for rights and freedoms of data subjects, in compliance with the legislation on the protection of personal data, without any further intervention being required of them;

- **Privacy by default,** which implies the implementation by the organization of a process that foresees and regulates the methods of acquisition, processing and protection, and methods of dissemination of personal data, limiting the collection of data exclusively to the personal data truly necessary for the achievement of the aims pursued, in compliance with the principle of data minimization, and determining from the beginning the period for which the personal data collected must be kept;

- **Consent**, which must be explicitly provided for each processing carried out, where the exemptions by law do not apply. In this regard, if the request to obtain consent from the data subjects is included among other declarations, it must be distinguished and formulated in simple and clear language. A condition of validity of the consent is that the purposes for which it is requested are explicit, legitimate, adequate and relevant. In the event that consent to the processing of personal data for one or more specific purposes concerns minors, the GDPR requires the data controller to verify the documented age of the child and, where necessary, depending on the age of the minor, it requires the consent to processing by a parent or by those exercising parental responsibility. Data controllers must be able to demonstrate that the data subject has given his/her consent (i.e. opt-in principle) and consent can be withdrawn or modified;

- **Data Breach**, defined as any activity that involves the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed. In the event of data breaches, unauthorised access or, in any case, loss of data, data controllers will be obliged, within 72 hours, to notify the supervisory authority and, in cases of particular gravity, also those directly involved, informing about possible consequences, measures adopted to remedy or reduce the impact of the damage and providing the contact data of the bodies and company figures that oversee the management and protection of processing of personal data in accordance with the law;

- **Rights of data subject**, which include, inter alia: **(i) The Right to Access**, which provides for the right to access and/or know what personal data are being processed and, for example, the expected retention period or the criteria for defining this period, as well as the guarantees applied in case of transfer of data to third countries; **(ii) The Right to Data Erasure (the right to be forgotten)**, which provides for the right of the interested party to the erasure of their personal data where there are no legal obligations or prevailing interests of the controller; as well as the obligation for the data controller or data processor to inform other data controllers that process the personal data to be cancelled of the request for erasure, by notifying the data subject, at the request of the same, of the recipients to whom the request for erasure has been transmitted; **(iii) The Right to Restrict Processing**, which provides for the possibility, in case of violation of the conditions of lawfulness of the processing, to request the restricting of processing, pending the evaluation of the controller, or to request the correction of the data presented by the data subject; **(iv) The Right to Data**

Portability, which applies only to automated data processed with the consent of the data subject or on the basis of a contract with the same and provided to the data controller by the data subject, in cases where the data subject has the need to transfer them to another controller, where technically possible;

- **Data Transfer outside the EU**: The GDPR prohibits the transfer to countries located outside the EU or to international organizations if it is carried out in the absence of adequate protection standards. However, transfer is permitted in the event adequate guarantees are present, such as contractual clauses between controllers authorized by the Guarantor, agreements and binding measures between public administrative and judicial authorities, standard clauses adopted by the Guarantor, adherence to codes of conduct and/or mechanisms of certification. Furthermore, transfer beyond the EU is allowed in the case of adequacy decisions of the EU Commission (e.g. “Privacy Shield EU/USA”, Switzerland, Argentina, Australia, Canada, etc.), binding company rules (BCR), and cases of derogation (informed consent of the data subject, needs arising from performance of contractual and pre-contractual obligations, public interest, right of defence, vital interests, data taken from the public register, etc.);

- **Data Protection Officer**, defined pursuant to the Regulation as the data protection officer (DPO) who must be designated to provide specialized legal and technical advice and assistance on data protection issues. With regard to the attribution of the specific tasks set out by the Regulation, the DPO must meet a series of requirements (by way of example, legal competences, technical and security competences) that allow him/her to carry out a risk assessment, i.e. assess risks and provide opinions on IT/security issues for the purpose of applying the most appropriate security solutions and IT measures. He/she plays an activator role and also has the duty to urge the controller or processor who remains inactive, thus violating the Regulations. According to the provisions of art. 39 of the GDPR, the DPO is in charge of assigning responsibilities, raising awareness and training company personnel and anyone involved in data processing management and related control activities, establishing who and to what extent, within the company, a body or organization, must respond to any behaviour that does not comply with internal data management procedures. The DPO supports the data controller in keeping the processing register and provides, if requested, an opinion on the impact assessment on data protection, supervising performance pursuant to art. 35 of the GDPR. He/she also cooperates with the supervisory authority and acts as a point of contact with the supervisory authority for issues related to data processing;

- **Adequate technical and organizational measures**, including reports, appointments, training etc. and above all **internal procedures** that formalize within the scope of the same adequate controls set out by the GDPR and the concrete implementation of a compliance system to prevent unlawful processing of personal data that also allows to prove that the company organization has proactively adopted and implemented all the safeguards provided for by the Regulation.

1.3. LIABILITY

The processing of personal data in violation of the law may give rise to civil and/or criminal and/or administrative liability, which may be also cumulative in relation to a single fact.

In civil matters, liability may legitimize a request for compensation for damages by the injured party, as set out by the Italian Civil Code and in particular by art. 2050 of the Civil Code, according to which anyone, whether a natural person or a legal person, who causes damage to others an effect of the processing of personal data and does not prove that they have taken appropriate measures to avoid this, is required to pay compensation for the damage.

The liability linked to the processing of personal data, in fact, falls within the concept of liability for the exercise of dangerous activities, according to which - pursuant to art. 2050 referred to above – "*anyone who causes damage to others in the performance of a dangerous activity, because of its nature or the nature of the means used, is liable to compensation if he/she does not prove to have taken all appropriate measures to prevent damage*".

The concept of liability defined above, already covered by the legislation on privacy, applies regardless of the negligent or intentional behaviour of the author, who, by virtue of a reversal of the burden of proof, must provide evidence of the fact that he/she took all the measures necessary to prevent the damage caused in order to be exempt from liability. It is up to the person who has suffered the damage to provide proof of the damage and demonstrate the causal relationship between the dangerous activity carried out and the damage. The compensable damages may be of a financial nature or non-financial nature, meaning in the latter case damages compensated for on the basis of a fair decision of the judge, deriving from the physical and/or moral harm of the injured party.

With regard to criminal liability, the most significant criminal cases concern the crime of unauthorized access to a computer or telecommunications system (art. 615 ter Criminal Code), the crime of retention and unauthorized disclosure of access codes of computer or electronic systems (art. 615 quater Criminal Code), as well as the crimes provided for by Legislative Decree 196/2003 Code regarding the protection of personal data – c.d. Privacy Code - as amended by Legislative Decree 101/2018, and in particular art. 167- Illicit data processing, art. 167 bis - Unlawful disclosure and dissemination of personal data subject to large-scale processing, art. 167 ter - Fraudulent acquisition of personal data subject to large-scale processing, art. 168 - Falsehood in the declarations and notifications to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor, art. 170 - Non-compliance with provisions of the Guarantor and art. 171 - Violations of the provisions on remote controls and surveys on the opinions of workers.

Finally, with regard to administrative liability, the Regulation establishes administrative penalties that must be imposed, depending on the circumstances of each individual case, taking into due account the following elements: a) the nature, gravity and duration of the violation also considering the nature, object or purpose of the processing in question as well as the number of data subjects affected by the damage and the level of damage suffered by them; b) the intentional or negligent nature of the violation; c) the measures taken by the data controller or by the data processor to mitigate the damage suffered by the data subjects; d) the degree of liability of the data controller or the data processor taking into account the technical and organizational measures implemented by them; e) any previous relevant violations committed by the data controller or the data processor; f) the degree of cooperation with the supervisory authority in order to remedy the violation and mitigate its possible negative effects; g) the categories of personal data affected by the violation; h) the manner in which the supervisory authority has taken note of the violation, in particular if and to what extent the data controller or the data processor has notified the violation; i) compliance with these provisions; j) adherence to codes of conduct or certification mechanisms; and k) any other aggravating or mitigating factors applicable to the circumstances of the case, for example the financial benefits obtained or the losses avoided, directly or indirectly, as a consequence of the infringement.

In the event of violations of the legislation in force, the data controller and the data processor are liable for compensation and therefore required to pay compensation. The controller must compensate any damage attributable to him/her that he/she caused by violating the Regulation in the processing of data.
The data processor is liable for any damage attributable to him/her if he/she has not fulfilled the obligations specifically directed to him/her or has acted in a way that is different or contrary to the instructions of the controller.

1.4. PENALTIES

Art. 82 of the GDPR regulates the right to compensation and liability by virtue of which anyone who suffers material or immaterial damage caused by a violation of the Regulation has the right to obtain compensation for the damage from the data controller or the data processor.

The system of penalties provides for the application of the following administrative pecuniary penalties in the event of violations of the Regulations, depending on the circumstances of each case:

- a fine of up to 10 million EUR or, if higher, up to 2% of the global turnover recorded in the previous year, in the cases provided for by art. 83, paragraph 4 of the Regulation (for example, in the case of: failure to adopt protections for minors, on anonymized data, privacy by design and by default measures, joint controllers, processing registers, privacy impact assessments, instructions to appointees, security measures, data protection officer);

- a fine of up to 20 million EUR or, if higher, up to 4% of the overall turnover recorded in the previous year, in the cases envisaged by art. 83, paragraphs 5 and 6 of the Regulation (by way of example, in
case of non-compliance with the basic principles of processing, with the rights of data subjects, with the rules on extra-EU data transfers, etc.);

The GDPR establishes a margin of discretion regarding the possibility of imposing a penalty and determining the amount thereof. This does not imply autonomy in the management of the penalties for the competent national authorities but provides them with some criteria on how to interpret the individual circumstances of the case. The criteria for determining administrative pecuniary penalties (such as, by way of example, the nature, gravity and duration of the violation, the intentional or negligent nature of the violation, the degree of cooperation with the supervisory authority in order to remedy the violation and to mitigate the possible negative effects) are established in art. 83 paragraph 2 of the Regulation.

With a view to national adaptation of the provisions of the GDPR, Legislative Decree 196/2003, as amended by Legislative Decree 101/2018, provides with art. 166 further indications in relation to the criteria for the application of administrative pecuniary penalties and in relation to the procedure for the adoption of the corrective and sanctioning measures.

The National Authority is given the opportunity to replace the pecuniary penalty with an admonition, "*in the case of a minor violation or if the financial penalty that should be imposed constitutes a disproportionate burden for a natural person*" (see Recital 148).

According to what is established by Recital 149 and by art. 84 of the GDPR, Italy has introduced provisions relating to criminal sanctions as an instrument for implementing and protecting the new regulation. In particular, Legislative Decree 196/2003, as amended by Legislative Decree 101/2018, provides for specific criminal cases under art. 167, 167 bis, 167 ter, 168, 170 and 171.
Art. 58 of the GDPR states that the Authorities can also make use of a series of remedies such as the possibility of limiting or even prohibiting the processing of data by a company. This could lead to the interruption of a service or business on the part of a company.

1.5. EXEMPTION FROM RESPONSIBILITY

The adoption of a Privacy Organizational Model allows enterprises, bodies and organizations to be exempt from liability. However, in order to be exempt from responsibility, the company or organization must demonstrate that it has adopted, effectively implemented and applied all the measures established under the MOP in compliance with the provisions of the Regulation.
In order to guarantee the effectiveness of the MOP, the GDPR requires the implementation of a risk-based approach, i.e. the Data Controller must:

- examine (through one or more assessments) the processing operations and identify and assess the existence of possible risks for the safety and rights and freedoms of data subjects ("Risk and Privacy Impact Assessment");

- identify the remediation and implementation activities to be carried out, through a prioritized program of adjustment and effective implementation of these actions;

- in the context of the remediation phase, provide for specific procedures aimed at implementing and controlling the adjustment program, also in relation to the elaboration and implementation of decisions that allow the company, body or organization to operate in compliance with the Regulation;

- identify methods of analysis, evaluation and management of the financial resources necessary to implement the adjustment program;

- establish obligations to inform the body in charge of supervising the functioning and compliance with the Privacy Organizational Model;

- introduce an appropriate disciplinary system to sanction non-compliance with the measures indicated in the Privacy Organizational Model.

In order to ensure the effective application of the Privacy Organizational Model, the following must be envisaged:

- a periodic check, and, if significant violations of the Privacy Organizational Model are discovered or if changes occur regarding the organization or the activities, i.e. legislative changes, the Privacy Organizational Model must be modified;
- the imposition of sanctions in the event of violation of the provisions set out by the Privacy Organizational Model.

- SPECIAL PART -

SECTION ONE

1. THE PRIVACY ORGANIZATIONAL MODEL OF FONDAZIONE HUMAN TECHNOPOLE

1.1 PURPOSE OF THE PRIVACY ORGANIZATIONAL MODEL

This document is the Privacy Organizational Model of the Fondazione Human Technopole (hereinafter "HT"), which processes personal data in its capacity of controller and/or processor.

This document describes the activities carried out by HT to ensure compliance with the GDPR and the relative methodological approach used, in addition to aspects relating to governance, risk management and compliance relevant to protection of personal data with the aim of defining:

i. organizational and management mechanisms, including roles, responsibilities for the protection of personal data (governance);
ii. risk management arrangements methods for the protection of personal data (risk management);
iii. a structured system of procedures to control the risks detected, as well as constant monitoring of the correct implementation of this system in compliance with the applicable regulatory requirements on protection of personal data (compliance).

HT is aware of the importance of adopting and effectively implementing a Privacy Organizational Model for the Protection of Personal Data and has prepared this document, which is a valid instrument for raising awareness among recipients (as defined in paragraph 1.2), to adopt behaviors that comply with the requirements of the GDPR.

1.2 RECIPIENTS

The provisions of this Privacy Organizational Model are binding for HT's employees (including managers), for collaborators subject to the management or supervision of HT's employees and for all those who, although not part of HT, operate in various capacities carrying out activities that entail the processing of personal data (hereinafter, “Recipients”).

1.3 FUNDAMENTAL ELEMENTS OF THE PRIVACY ORGANIZATIONAL MODEL

The fundamental elements of the Privacy Organizational Model, developed by HT in the context of the activities aimed at adjusting to the GDPR, can be summarized as follows:

- the preparation and forthcoming adoption of a Procedure for the management of Data Breach;
- the preparation and forthcoming adoption of a Procedure for the management of Data Retention;
- the drafting of instructions for the management of HT’s documentation;
- the need assessment and the forthcoming adoption of a methodological approach to Privacy Impact Assessment document;
- the updating of relevant privacy documentation (e.g. information, consents, internal and external appointments);
- the adoption and updating of a Processing Register;

- the planning of carrying out information and training activities on the contents and changes introduced by the GDPR and aimed at disseminating this Privacy Organizational Model;

- the provision of periodic verification activities, including sampling, to monitor the adequate implementation of the GDPR, the effectiveness and actual operation of the Privacy Organizational Model, also for the purposes of its review, and the system of procedures adopted.

1.4 LEGISLATION OF REFERENCE

This document refers to and is inspired by the following standards:

- "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, and repealing Directive 95/46/EC;

- Legislative Decree no. 101 of 10 August 2018, "Provisions for the alignment of national legislation to the provisions of the 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, and repealing Directive 95/46/EC (general Regulation on data protection)";

- Standard UNI EN ISO/IEC 27001:2013 "Information technology - -Security techniques - Information security management systems – Requirements";

- Guidelines and Specific Measures of the supervisory authority for the Protection of Personal Data;

- ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

1.5 TERMS AND DEFINITIONS

Definitions and acronyms used in this document are as follows.

GDPR: General Data Protection Regulation (EU Regulation 2016/679).

Personal data: any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller: is 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Risk: Risk for data security and for the fundamental rights and freedoms of the data subject, the likelihood and severity of which is determined with regard to the nature, scope of application, context and purpose of the processing, based on an objective assessment to establish whether data processing involves a risk or a high risk. Together with the effect of uncertainty on the objectives.

Impact: consequences of the risks of processing on the rights and freedoms of the data subjects, considering the nature, the object, the context and the purposes of the processing (e.g. due to the systematic monitoring of behaviours, or due to the large number of data subjects whose sensitive data are perhaps processed, or to a combination of these and other factors), as well as the technical and organizational measures implemented to counter/mitigate risks.

Risk Analysis and Assessment: Overall process to understand the nature of the risk, determine the level of risk for the protection of personal data, risk analysis and risk weighting, both in terms of risk for data security and risk of impact on individual freedoms.

Source of risk: element that alone or jointly with others has the inherent potential to bring about risk.

Vulnerability: weakness of an asset or a control that can be exploited by one or more threats.

Threat: potential cause of an unwanted accident that may endanger a system and/or HT data and/or processing.

Consequence: outcome of an event that influences the objectives.

Level of risk: quantitative expression of risk or combination of risks, expressed in terms of combination of consequences and their likelihood.

Risk weighting: process of comparing the results of the risk analysis with risk criteria in order to determine whether the risk and its quantitative expression is acceptable or tolerable.

Risk criteria: terms of reference against which the significance of the risk is assessed.

Risk treatment: process to modify and minimize the risk.

Control: adequate technical and organizational measure modifying the risk.

Residual risk: Risk remaining after risk treatment.

1.6 METHODOLOGICAL APPROACH FOR THE DEFINITION OF THE PRIVACY ORGANIZATIONAL MODEL: ASSESSMENT OF THE CONTEXT AND RISK & PRIVACY ASSESSMENT

With regard to all the activities of adjustment to the GDPR that have been carried out, HT has adopted a methodological approach in line with the requirements of the GDPR, the standards in the field of personal data protection.

1.6.1 ASSESSMENT: PRINCIPLES

In this regard, HT has carried out an in-depth analysis of its activities in order to understand its context (internal, external, etc.).

As part of this analysis, HT has, first of all, carried out a series of legal/organizational and technical assessment activities.

This assessment has been articulated in the following main phases:

i. collection of information useful for the preparation of the Processing Register adopted by HT in compliance with legal obligations;

ii. collection of relevant privacy documentation;
iii. collection of information on information flows and systems to support the census the processes examined data processing and evaluation of technological security measures;
iv. examination of security systems and measures;
v. evaluation of technical and organizational measures, of the security risk and of the risks of impact of processing on the rights and individual freedoms of data subjects;
vi. overall assessment of the risk of impact on the rights and freedoms of data subjects.

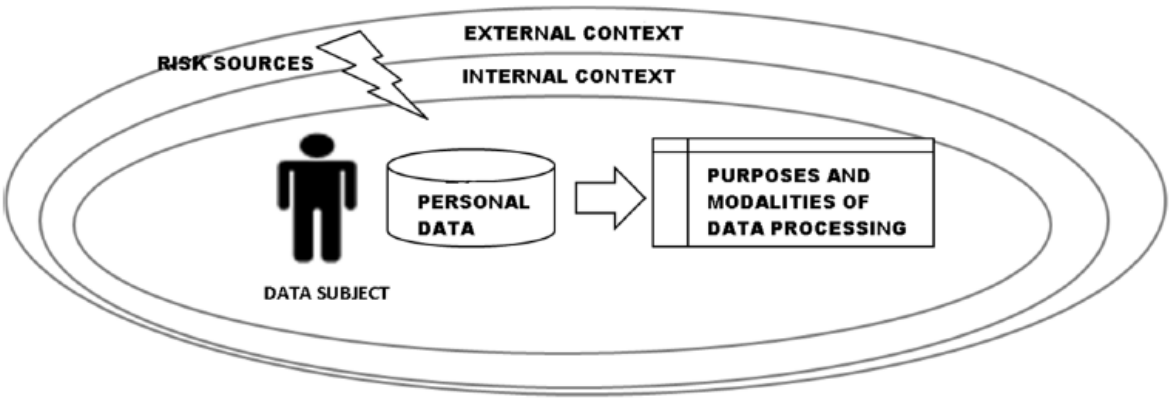
At the end of the assessment carried out in July 2019, a final report was prepared, which highlighted the privacy risk profile and the actions to be taken.

The relative documentation is available at the Legal Department, in charge of archiving it and making it available for consultation to anyone who is entitled to view it.

1.6.2 ASSESSMENT: ANALYSIS AND EVALUATION OF THE CONTEXT

The personal data processed are influenced by factors relating to the external and internal reference context. These factors also constitute the source of risks for the protection of personal data and have been evaluated in the context of the assessments described above.

Figure 1 - Assessment of the reference context

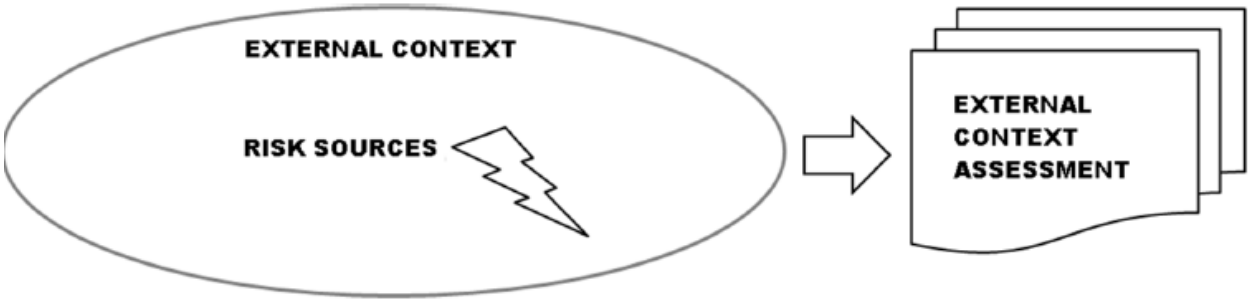


External context

The assessment of the external context must take into consideration the following factors:

- sectoral context: evaluation of aspects concerning suppliers, third parties, visitors of the sector in which HT operates;
- regulatory context: evaluation of the applicability of the GDPR and of regulations, including specific sector regulations, to HT on the protection of personal data;
- technological context: evaluation of the trend of threats and vulnerabilities inherent in the use of IT systems for the processing of personal data;
- socio-economic context: evaluation of the intrinsic value of personal data processed by HT and potential threats;
- territorial context: evaluation of the characteristics of the territorial context outside HT and of its impact on the protection of personal data.

Figure 2 - External context assessment

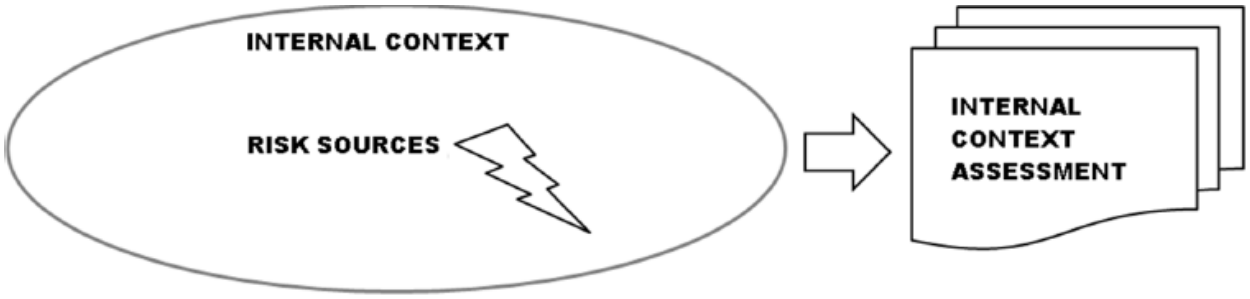


Internal context

The evaluation of the internal context must take into consideration the following factors:

- legal context: evaluation of the legal nature and liability of HT on the basis of which personal data is processed;
- organizational and human resources context: evaluation of the organizational and human resources model through which personal data is processed;
- IT context: evaluation of IT services, of the relative IT infrastructure, of the systems processing personal data and related security measures.;
- physical and environmental context: evaluation of physical sites (locations, power plantes) and environmental characteristics through which personal data is processed.

Figure 3 - Internal context assessment



The evaluation of the external and internal context of reference for the protection of personal data is reported in the deliverables of assessment carried out.

1.6.3 ASSESSMENT: ANALYSIS OF THE PARTIES INVOLVED IN THE PROTECTION OF PERSONAL DATA

The main parties involved in the protection of personal data identified by HT during the assessment are the following.

TABLE OF THE PARTIES INVOLVED IN THE PROTECTION OF PERSONAL DATA OF HT		
PARTY INVOLVED	**INVOLVEMENT**	**NEEDS AND EXPECTATIONS**
Data Controller	Ensures compliance with the requirements of the applicable legislation	Ensure compliance with applicable data protection requirements. Evaluate and address data processing risks. Define and assign roles and responsibilities with regard to the processing of personal data within the company, data controller, and to external parties that process data on its behalf.
External Data Processor	External party processing personal data on behalf of the Data Controller	To be appointed External Data Processor in accordance with GDPR requirements. Receive clear and documented instructions from the Data Controller regarding the processing to be carried out.
Internal Data Processor	Internal party processing personal data within HT	To be an instrument of accountability and control on behalf of the Data Controller. Receive clear and documented instructions on the processing of personal data by the Data Controller and provide it to the internal persons tasked with processing. Receive training for the correct application of personal data processing requirements. Receive awareness of the risks and appropriate technical and organizational measures (“operational controls”) regarding the protection of personal data.
Internal Person Tasked with Processing	Processes personal data within HT (e.g. employee, collaborator)	Receive clear and documented instructions on the processing of personal data from the Data Controller and/or the Internal Data Processor.

		Receive training for the correct application of personal data processing requirements. Receive awareness of the risks and appropriate technical and organizational measures ("operational controls") for the protection of personal data.
External Person Tasked with the Processing	Processes personal data of IIT and is appointed by the External Data Processor	Receive clear and documented instructions regarding the processing of personal data from the External Data Processor. Receive training for the correct application of personal data processing requirements. Receive awareness of the risks and appropriate technical and organizational measures ("operational controls") for the protection of personal data.
System Administrator	Processes personal data of HT and is appointed by the external Data Processor	Receive clear and documented instructions on the processing of personal data from the Data Controller. Receive training for the correct application of personal data processing requirements. Receive awareness of the risks and appropriate technical and organizational measures ("operational controls") for the protection of personal data.
Data Subjects	Subject whose personal data are processed	Obtain from HT, the Data Controller, that the processing of personal data is carried out in compliance with the applicable requirements, with particular regard to the principles. Be informed about the treatments carried out by HT. To be able to express their consent to individual processing operations, where necessary. Have an easily accessible point of contact to exercise your rights.
Data Protection Authority (or "supervisory authority")	Supervise the correct application of the legislative requirements	Receive timely reports from HT, the Data Controller, in the event of incidents or breaches of information protection.

		Receive cooperation from HT, in the context of requests regarding the application of regulatory requirements.

1.6.4 ASSESSMENT: RISK ANALYSIS

With the introduction of the GDPR, privacy has become risk-based.

In the context of the activities to adjust to the GDPR, HT has examined and managed risk with the following activity cycle:

i. Identification of the architecture, of the parties involved, of roles and responsibilities for risk management;
ii. implementation of risk management, through risk evaluation and assessment and of risk treatment - i.e. identification, implementation of organizational and technical measures to mitigate risks, as well as prioritization of the same (remediation and implementation);
iii. monitoring and review of the model (monitoring for continuous improvement) aimed at achieving continuous improvement of the data protection risk management system.

Figure 4 - Data protection risk management

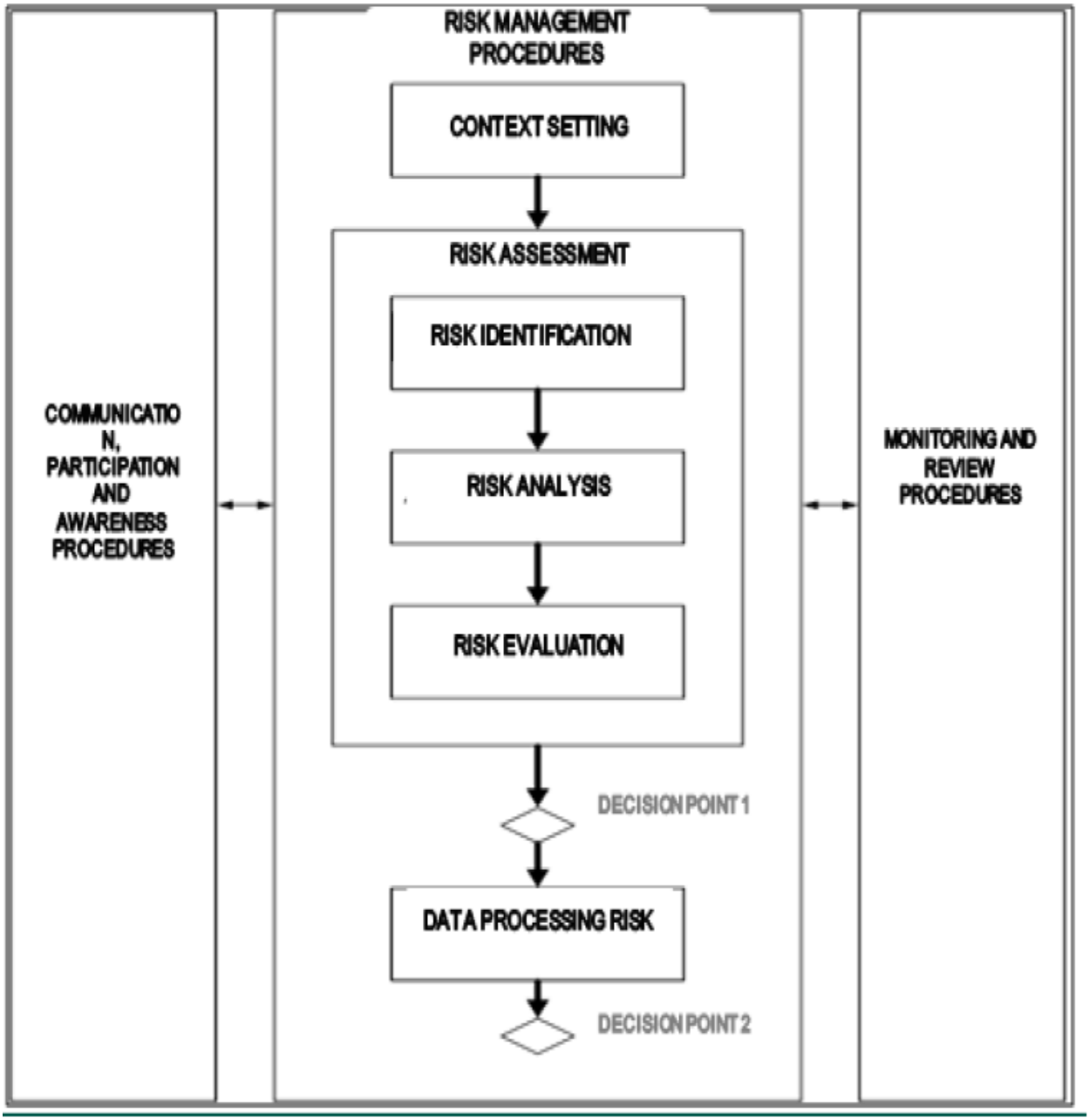
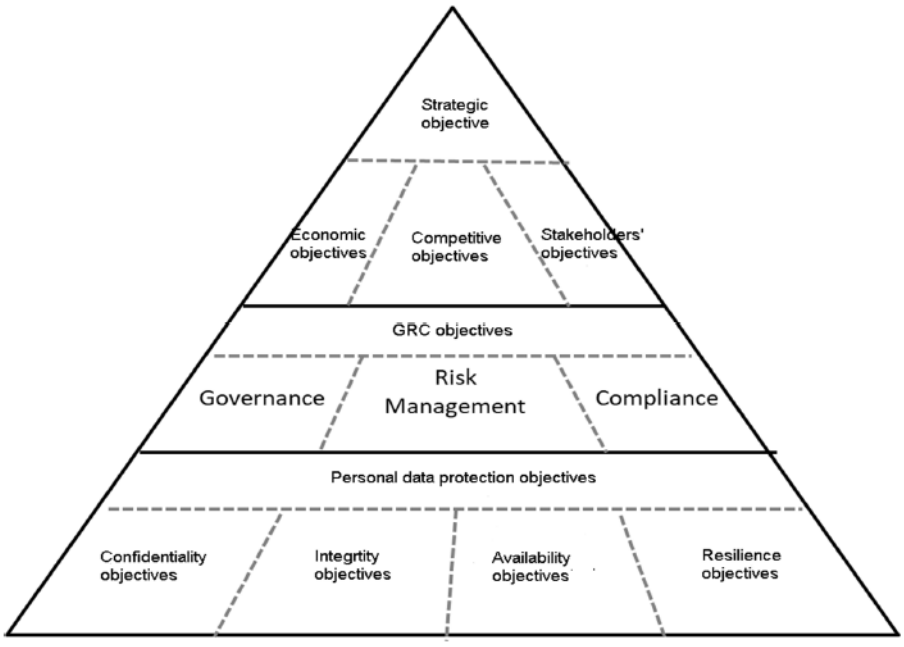


Figure 5 - Risk assessment and impact assessment

The protection of personal data is carried out by HT in the pursuit of the following strategic objectives:

1. confidentiality of personal data processed;
2. availability of the personal data processed, also following incidents that could lead to the loss of operational continuity in the processing of such data and the related resilience objectives;
3. integrity of personal data processed.

Figure 6 - Data protection objectives



The analysis of the maturity level at the GDPR, the gap analysis and the related reference action plan, currently implemented by HT, is included in the final assessment report mentioned in point 1.5.1.

The mapping of the treatments, together with the analysis of the measures implemented and in progress, as well as the assessment of the risks associated with each treatment, are documented in the Processing Register, which also illustrates the methodology adopted.

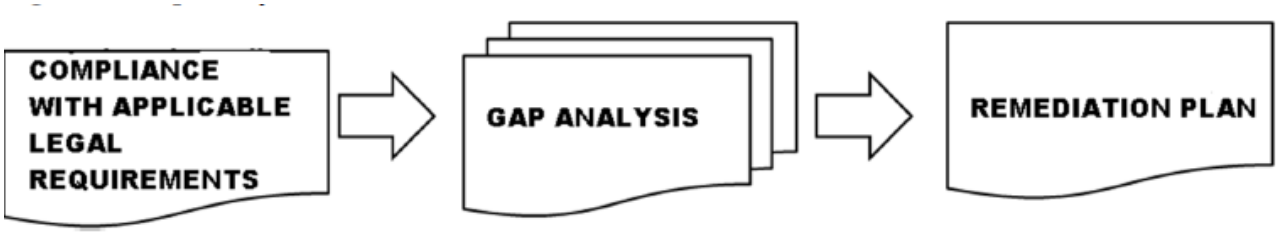
1.6.5 ASSESSMENT: GAP ANALYSIS

Following the assessment, the related gap analysis was performed to identify:

1. any deviation from the requirements ("gap analysis");

2. any realignment plans (remediation plan).

Figure 7 - gap analysis and remediation plan



1.6.6 REMEDIATION: THE PRINCIPLES

Following the assessment carried out, HT deemed it necessary to take the following appropriate measures:

- Privacy Information and consents: updating and drafting of privacy Information (e.g. for employees, collaborators, candidates, suppliers, suppliers, visitors, customers, internal organs and bodies of HT) and related consents;

- Procedures: planning of the adoption of procedures specifically in the field of privacy, such as the procedure relating to the management of Data Breach, Data Retention, etc.;
- Appointments of internal subjects: adoption of the appointments as Data Processor, Internal Data Processor and System Administrator in order to define the scope of processing allowed to internal subjects processing personal data. In this context, profiles are envisaged with authorization to access data which are diversified according to processing carried out by people tasked with processing, so as to limit access to data to authorised parties only;

- Appointments of external subjects: appointments of third-party companies that access the data as External Data Processor and System Administrator. In this context, it is planned to keep the list of external suppliers - and in particular those that process personal data - updated periodically;

- System administrators: updating of appointments;

- Privacy Organizational Model: adoption of this POM;

- Security measures: adoption and/or formalization of appropriate processes with regard to the security of personal data and adoption or reinforcement of security measures on systems;

- Training: provide for periodic training of employees and collaborators in the field of personal data protection;

- Register of data processing: obligation to adopt a register to track all processing carried out;

- Maintenance: adoption of periodic GDPR compliance verification processes.

1.6.7 REMEDIATION: POLICIES

- ***Data protection policies***

HT has deemed it necessary to undertake to ensure that all processing of personal data is performed in compliance with the applicable mandatory requirements, with particular reference to the principles and rules to be observed.

HT, in the context of this Privacy Organizational Model and of the procedures adopted and disclosed internally at HT, formalizes the guidelines regarding behavioural principles and new rules, pillars of compliance regarding protection of personal data, raising awareness all the staff, including those who collaborate with HT, through adequate information and training activities, of the systematic and punctual observance of the same principles and rules.

In particular, the following procedures have been adopted and/or are in the process of being adopted:

- Data Retention which describes which data are processed by HT, what are the necessary data retention timeframe and therefore the storage timeframe;

- Data Breach, which describes the process of notifying the Data Protection Authority and the Data Subject, where deemed necessary, of personal data breaches;

For more details, please refer to the procedures published on HT's intranet.

1.6.8 REMEDIATION: THE INFORMATION, THE CONSENTS

HT considered it necessary to make a commitment to ensure that all persons whose personal data are processed are adequately informed.
For this reason, HT has planned the updating of all the information to the Data Subjects and the related consensus and is planning awareness-raising activities for employees and collaborators.

1.6.9 REMEDIATION: APPOINTMENTS AND INSTRUCTIONS

HT deemed it necessary to commit to ensuring that all persons processing personal data are properly informed and trained. For this reason, HT has planned the appointment of Internal and External Data Processors and Internal Person Tasked with Processing.

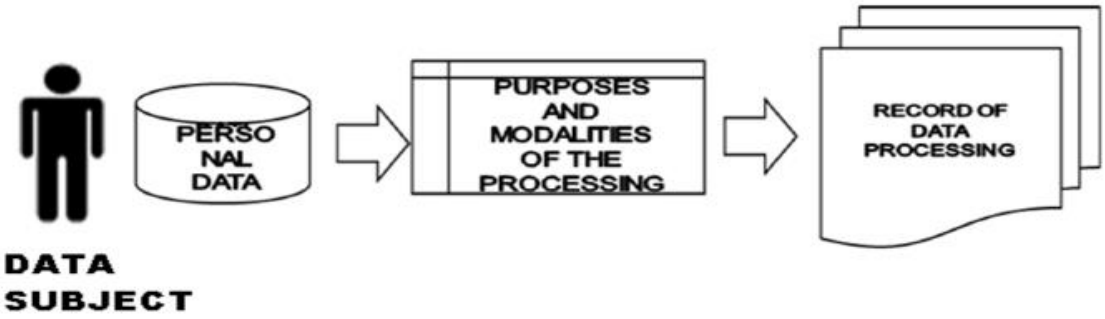
1.6.10 REMEDIATION: TRAINING - AWARENESS

HT deemed it necessary to commit to ensuring that all persons processing personal data are properly trained.
For this reason, HT is planning adequate training for both the Internal Person Tasked with Processing and the Internal Data Processors, regarding the contents of the GDPR and the procedures adopted by HT.

1.6.11 REMEDIATION: THE PROCESSING REGISTER

Following the assessment activities carried out, it has emerged that HT processes data that can be classified as personal data pursuant to the GDPR.
HT has deemed it necessary to prepare the descriptive list of such processing operations contained in the Processing Register.
The Processing Register includes the processing activities carried out under the responsibility of the Data Controller.
The structure of the document includes: in Chapter I, general information such as the relevant legislation, the main definitions relevant to GDPR purposes; in Chapter II, all the information required by art. 30, paragraph 1 of the Regulation for the drafting of the Processing Register by the Data Controller; in Chapter III, all the changes made to the Register as part of the future updating of the same; in Annex 1, an Excel file called "Treatment mapping and risk assessment"; in Annex 2, a Word file called "Methodology for risk and impact assessment".

Figure 8 - Register of personal data processing



In this regard, for more details, please refer to what has been highlighted in the HT Processing Register.

1.6.12 REMEDIATION: THE RIGHTS OF THE DARA SUBJECT

HT has deemed it necessary to commit to ensuring that Data Subjects can adequately exercise their rights and that the persons tasked be aware of them. Proper Informative have been prepared.

1.6.13 REMEDIATION: THE INTERNAL CONTROL SYSTEM OF HT

HT deems it necessary to commit to ensuring the adoption of adequate control, monitoring, audit and privacy review tools.
To this end, it has prepared this Privacy Organizational Model for the protection of personal data, which takes into account the internal control system, aimed at verifying the suitability or effectiveness and the actual operation of the specific controls to address the risks of compliance that have been identified.
The control system involves all activity sectors of HT in that operational tasks are distinct from control tasks, reasonably reducing any potential conflict of interest.
In particular, the HT internal control system is based not only on the rules of conduct established in this Privacy Organizational Model, but also on the following elements that are being adopting:

- the Organization, Management and Control Model adopted pursuant to Legislative Decree 231 of 2001 and the Code of Conduct and the Code of Scientific Conduct;
- the Ethics Code;
- a system of internal procedures;
- the hierarchical-functional structure (organization chart), the parties involved in the protection of personal data (including internal and external parties, Processors, and Persons Tasked with the Processing) and the organizational structures of governance and supervision of HT;
- the system of delegations of authority and powers of attorney;
- integrated information systems aimed at separating functions and protecting the information they contain;
- the traceability of operations, according to which the operations have to be as adequately documented as possible, and the processes of decision, authorization and development of the operations must be verifiable ex post, inter alia through appropriate documental support;
- the support provided by the Legal Office to the other Departments and/or Offices, in the management of those activities that imply compliance with specific laws and regulations (e.g. personal data protection management);
- periodic audits of the effectiveness of the controls performed by the Consiglio di Sorveglianza.

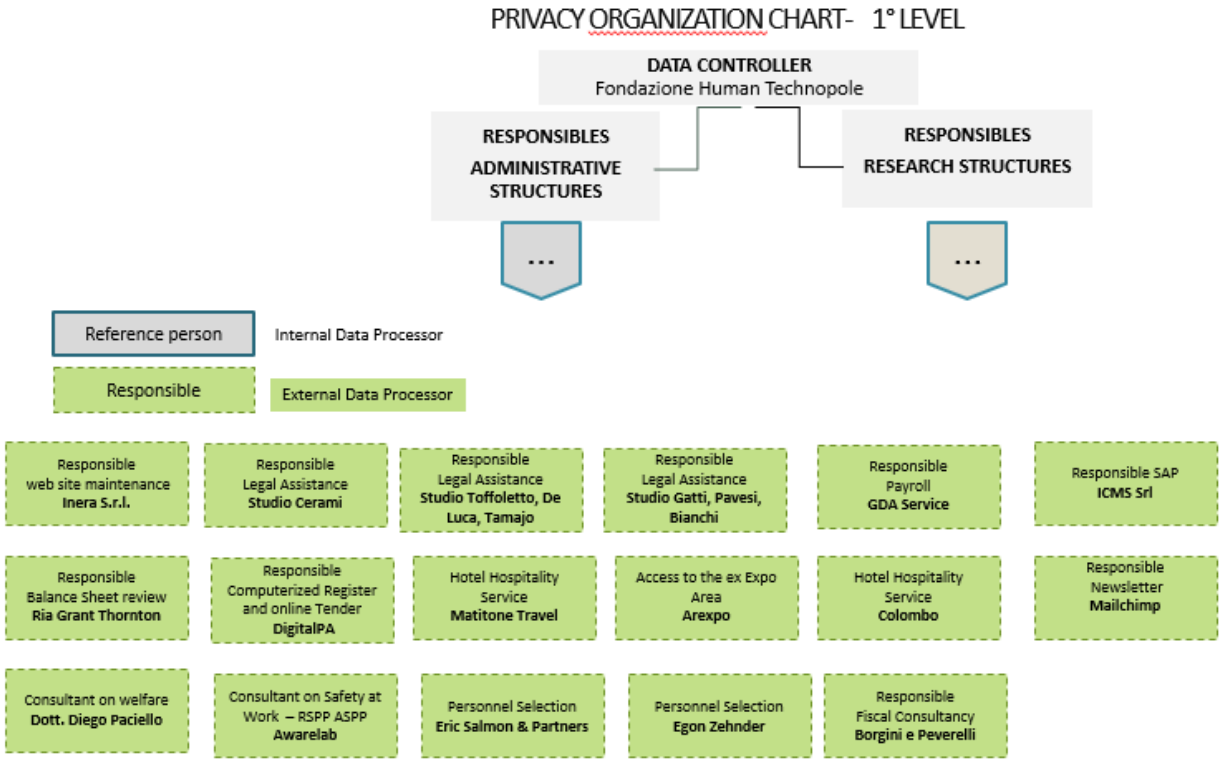
SECTION TWO

2. BODIES AND FUNCTIONS INVOLVED IN DATA PROTECTION

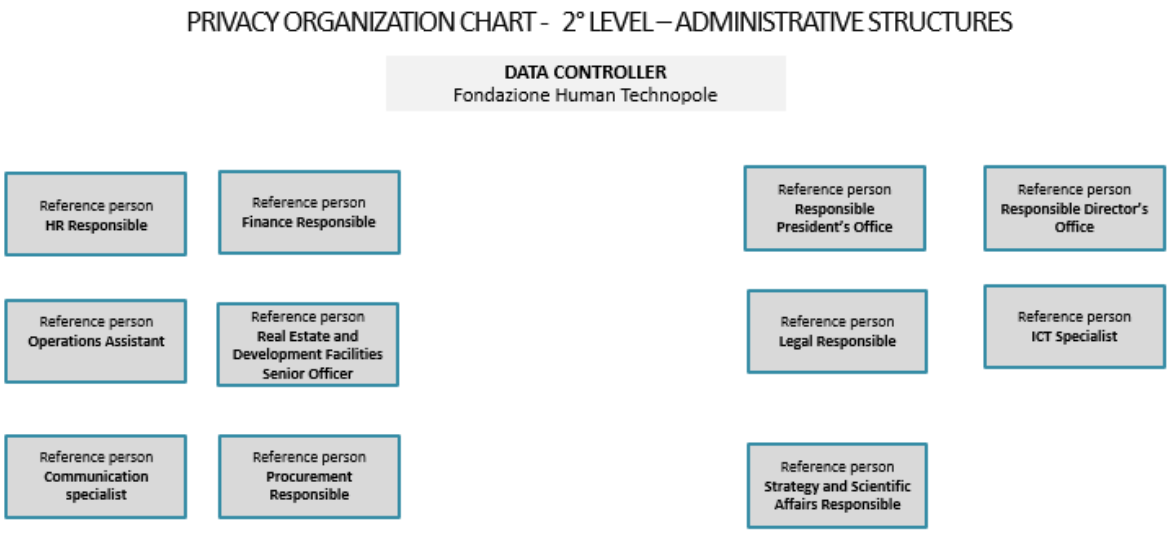
2.1 PRIVACY ORGANIZATION CHART

Fondazione Human Technopole has arranged its own organization chart as follows:

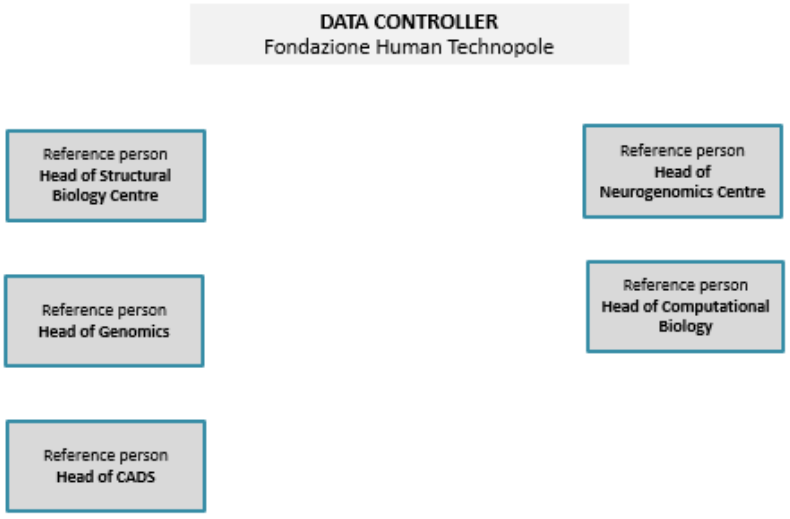
Level I privacy organization chart



Level II Privacy organization Chart: Administrative Structures



Level II Privacy Organization Chart: Research Structures



2.2 APPOINTMENT OF THE DATA PROTECTION OFFICER

As part of the program to comply with the GDPR, studies are still in the process of determining whether or not it is mandatory, in light of the legal nature of the Foundation, to designate a Data Protection Officer (DPO) pursuant to Art. 37 of the GDPR.

2.3 THE GOVERNANCE FUNCTIONS OF THE PRIVACY ORGANIZATIONAL MODEL: LEGAL, ICT SUPPORT, HR AND THE OTHER SUPPORTING FUNCTIONS

Pending the evaluation on the appointment of a DPO, the aspects concerning Data Protection are handled within the Fondazione Human Technopole primarily by the Legal Office, the ICT Support Department, and the HR Department, which assume governance of the POM implemented pursuant to the GDPR, together with the additional functions that are periodically involved in the assessment and analysis of specific issues concerning data protection.

The aforementioned corporate functions are tasked with:

- informing and providing advice to the Data Controller or the Data Processor and to the employees who perform processing about the obligations pursuant to the GDPR, and other national or European Union data protection regulations;
- monitoring GDPR compliance by the Data Controller or the Data Processor in regard to personal data protection, including the assignment of responsibilities, awareness-raising, and training of the personnel involved in the processing and related control activities;
- providing opinions on the advantages of coordinating the Departments involved in the data protection impact assessment and monitoring its execution pursuant to Article 35 of the GDPR;
- managing communications and reports to the Data Protection Authority ("Autorità Garante per la protezione dei dati personali");
- supporting the Data Controller in keeping the Processing Register, in accordance with the instructions issued by it. In particular, those Departments periodically monitor the effectiveness and application of HT procedures and of the Privacy Organizational Model and provide support in the periodic updating of the Processing Register, and of the procedures and the Privacy Organizational Model as necessary.

The Legal Office and the HR Department handle the primarily organizational aspects, and for example:

- constant updates and revision of the privacy document framework (e.g. Information to the data subjects, appointments of External Processors, processing authorizations, appointments of System Administrators, etc.);
- the establishment, maintenance, and updating of the Data Processing Register, inter alia through the use of external professionals;
- the establishment of internal procedures for management of privacy compliance (e.g. data breach management procedure, data retention procedure, document management instructions);
- the planning and provision of dedicated training on privacy to the employees authorized to process personal data;
- the planning of audits for periodic reviews of proper compliance with privacy laws and compliance with procedures and instructions by the employees authorized to process personal data.

The ICT Support Department is responsible for the monitoring and possible implementation of information system measures.

Within the scope of their respective responsibilities, the Legal Office, the HR Department, and the ICT Support Department coordinate and possibly engage the Internal Data Processor and Internal

Persons Tasked with Processing in all the other Departments who can provide support in the management of Data Protection issues and management of the requests from Data Subjects.

2.4 MONITORING, ASSESSMENT AND CONTINUOUS IMPROVEMENT

HT, in its capacity as Data Controller, and the Internal Data Processors must systematically monitor the adequacy, effectiveness, and actual functioning of the Privacy Organizational Model for the protection of personal data.

In regard to its adequacy, effectiveness, and actual functioning, the Privacy Organizational Model has to be evaluated, for example but not only, in regard to:

- changes or developments in the external context of reference, including changes in the regulatory requirements regarding the protection of personal data;
- changes or developments in the internal context of reference, including developments that involve new or changed processing, processing purposes, risk scenarios, etc.;
- changes to the information systems used for the processing of personal data;
- results of internal audits that show non-compliance of processing with the applicable requirements, including the requirements defined by the Data Controller itself;
- review, on an annual or periodic basis; review on an occasional basis in the following cases:
    - serious or repeated non-compliance, including violations of the regulatory requirements or of the requirements defined by the Data Controller;
    - personal data protection incidents (“data breaches”); or significant changes in the external reference context, including changes in the regulatory framework;
    - significant changes in the internal reference framework.

Furthermore, HT is aware of the importance of adopting and effectively implementing a Privacy Organizational Model for the protection of personal data pursuant to the GDPR, suitable for preventing the risks and damage deriving from illicit processing of those data, of promoting reviews and continuous adaptation of the POM according to the opportunities for improvement identified by risk assessment, monitoring, audit and analysis of incidents and non-compliance.

2.4.1 PARTIES RESPONSIBLE FOR MONITORING, ASSESSMENTS, AND CONTINUOUS IMPROVEMENT

Monitoring is performed by the Legal Office, ICT Support, and HR, each within the limits of their own functions.

2.5 REPORTING

To promote compliance with the GDPR, HT encourages reporting of any information, action, operation and, more generally, any activity in violation of the provisions of the GDPR, as well as specific incidents relating to personal data.

HT prohibits retaliatory behavior or any other form of discrimination against or penalization of the reporting party. All information and documentation relating to the reports referred to in this paragraph are collected and kept by the Legal Office.

SECTION THREE

1. COMPLIANCE AND PENALTY PROVISIONS

In case of violation of the provisions of this Privacy Organizational Model by employees of HT or collaborators, the latter will apply, with consistency, impartiality and uniformity, disciplinary sanctions proportionate to the violations and, in any case, in compliance with the provisions of the law of the applicable National Collective Bargaining Agreement.

Compliance with the provisions of this Privacy Organizational Model must be considered an essential part of the contractual obligations of IIT employees pursuant to and for the purposes of Articles 2104 et seq. of the Italian Civil Code.

Violation of the provisions of the Privacy Organizational Model may constitute a breach of the obligations of the employment agreement and/or a disciplinary infraction, in accordance with the procedures set forth in Article 7 of the Workers' Statute, entailing all legal consequences, also with regard to the continuation of the employment agreement and possible compensation for damage. Furthermore, compliance with the principles of this Privacy Organizational Model represents an essential part of the contractual obligations undertaken by the collaborators.

Violation of the Privacy Organizational Model by third parties may constitute default on the obligations they assumed, entailing legal consequences, even in regard to the right of HT to terminate the contract and possible compensation for damages.

2. DISSEMINATION OF THE ORGANIZATIONAL MODEL

HT is aware of the importance of the role played by training and information in prevention, and in order to ensure that the processing of personal data is carried out in compliance with the applicable regulatory requirements, it will set up a communication and training program aimed at ensuring the dissemination of skills and the necessary knowledge for the proper and systematic application of company provisions governing personal data protection, including this Privacy Organizational Model.

The information and training activity must involve all employees and collaborators, and all the resources who will join the HT organization in future. In this regard, the relevant training activities must be planned and actually carried out both at the time of hiring, and on the occasion of any change of duties, and after updates and/or changes to the Privacy Organizational Model.

With regard to dissemination of the Privacy Organizational Model, HT undertakes to:

- send a communication to all personnel concerning the adoption of this Model;
- publish the Privacy Model on the intranet and/or on any other communication tool deemed appropriate;
- organize training activities aimed at spreading knowledge and developing awareness of the need to pursue the following objectives:
    - process personal data in compliance with the principles and requirements defined by applicable personal data protection laws;
    - process personal data in a way that minimizes the associated risks, being aware of the consequences of non-compliance with the regulations, procedures and operational controls defined by HT;
    - report any violations or incidents concerning the protection of personal data in a timely and systematic manner.

The documentation relating to information and training activities will be kept by the Legal Office available for consultation by anyone who is authorized to view it.