ISTITUTO ITALIANO
DI TECNOLOGIA

PRIVACY ORGANIZATIONAL MODEL FOR THE PROTECTION OF PERSONAL DATA

INDEX

- GENERAL PART -

SECTION ONE

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

1.1. REGULATION (EU) 2016/679 (GDPR) AND THE ADJUSTMENT OF NATIONAL LEGISLATION

The EU Regulation 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 to ensure lawful and correct processing of personal data on the part of organizations acting as data controllers and/or as processors.

In Italy the process of adaptation to the GDPR was conducted through the adoption of the Legislative Decree no. 101 of 10 August 2018, in force as of 19 September 2018, which intervened on the existing Legislative Decree 196/2003 – 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 data regarding health or data related to 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 data of residents in the European Union and also to enterprises and bodies, organisations in general, with registered office outside the EU that process personal data of residents of the European Union. It is therefore specified that all enterprises, organisations and Public Administrations present in the Member States of the European Union (irrespective of whether processing 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 behaviour of individuals within the Union.

The adjustment to the requirements of the GDPR includes, among other privacy compliance activities, the adoption and effective implementation of an **Organizational Model for the Protection of Personal Data** that allows 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 TO BE OBSERVED FOR THE PROCESSING OF PERSONAL DATA

The processing of personal data shall be carried out in respect of 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 organisational 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, unauthorized 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 the processing of personal data in accordance with the law;
- **Rights of Data Subjects**, 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 a 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, according to which anyone, whether a natural person or a legal person, who causes damage to others as 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 c.c. 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 anonymised 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 for the Protection of Personal Data ("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 Model in compliance with the provisions of the Regulation.

In order to guarantee the effectiveness of the Model, the GDPR requires the implementation of a risk-based approach, i.e. the 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 Model;
- introduce an appropriate disciplinary system to sanction non-compliance with the measures indicated in the Model.

In order to ensure the effective implementation of the Model, the following must be envisaged:

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

1.6. GUIDELINES ON RISK ASSESSMENT AND IMPACT ON DATA PROTECTION ("RISK AND PRIVACY IMPACT ASSESSMENT")

The risk assessment and data protection impact assessment, foreseen by the Regulation, requires controllers to carry out an impact assessment before starting the processing, which can also require the consultation with the supervisory authority in the event that the technical measures and organizational measures identified to mitigate the impact of processing are considered to be insufficient, or when the residual risk posed to rights and freedoms of data subjects remains high.

In this regard, it should be noted that the WP29 guidelines[1] have been issued, which define when an impact assessment is mandatory, who should carry it out and how (the controller, assisted by the data protection manager, if designated), what it consists of, and specify the need to consider it as a process subject to continuous review and not a one-off fulfilment.

These guidelines on the data protection impact assessment provide the data controller with useful information for the performance of assessments aimed at preventing privacy risks and for the concrete implementation of a fundamental pillar established by the Regulation, i.e. data protection from the design phase (**Privacy by Design**) of all processing.

[1] ART. 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.

The guidelines also aim to promote the drafting of:

- a common European Union list of the types of processing for which it is mandatory to proceed with a data protection impact assessment;
- a common European Union list of the types of processing for which a data protection impact assessment is not required;
- common criteria on the methodology for carrying out a data protection impact assessment;
- common criteria that specify when the supervisory authority shall be consulted;
- recommendations, where possible building on the experience gained in EU Member States.

- SPECIAL PART –

SECTION TWO

2. THE ORGANIZATIONAL MODEL FOR PROTECTION OF PERSONAL DATA OF ISTITUTO ITALIANO DI TECNOLOGIA FOUNDATION

2.1. PURPOSE OF THE MODEL

This document is the Privacy Organizational Model for the Protection of Personal Data (hereinafter also "Organizational Model") of the Istituto Italiano di Tecnologia Foundation (hereinafter IIT), which processes personal data in its capacity of controller and/or processor.

This document describes the activities carried out by IIT 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 and authorities, with regard to protection of personal data (governance);

ii. risk management methods for the protection of personal data (risk management);

iii. a structured system of procedures to monitor 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).

IIT is aware of the importance of adopting and effectively implementing an Organizational Model for the Protection of Personal Data and has approved this document, which is a valid instrument for raising awareness among recipients (as defined in paragraph 2.2), to adopt behaviours that comply with the requirements of the GDPR .

2.2. RECIPIENTS

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

2.3. FUNDAMENTAL ELEMENTS OF THE MODEL

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

- the adoption of a procedure for the pseudonymisation of personal data;
- the adoption of a procedure for the management of data breach;
- the adoption of a procedure for the preliminary assessment of the impact on data protection (PIA - Privacy Impact Assessment);
- the drafting of document on the methodological approach to Privacy Impact Assessment;
- the provision of specific procedures to regulate activities deemed to be at risk with regard to privacy: e.g. CV management, management of Tenure Track CVs, data retention;
- updating relevant privacy documentation (e.g. reports, consents, internal and external appointments);

- adoption and updating of a processing register;
- the designation of a person responsible for the protection of personal data or data protection officer (DPO), with the assignment of specific tasks for the effective implementation and effective application of compliance pursuant to the GDPR (for example, providing day-by-day advice on the issues concerning data protection, performing risk assessments, providing opinions on IT/security issues for the purpose of applying the most appropriate security solutions and IT measures);
- carrying out information and training activities on the contents and changes introduced by the GDPR and by this Model;
- the provision of periodic verification activities, including sampling, to monitor the adequate implementation of the GDPR, the effectiveness and actual operation of the Organizational Model, also for the purposes of reviewing it, and the system of procedures adopted.

2.4. 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";.
- ART. 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.

2.5. TERMS AND DEFINITIONS

Definitions of the acronyms used in this document are as follows:

TERM	DEFINITION
GDPR	General Data Protection Regulation (European Regulation UE 2016/679).
Personal Data	Personal data means 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	Processing means 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	Controller means 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	Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Pseudonymisation	Pseudonymisation means the processing of personal data in such a manner that the personal data 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 technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
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 established 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.
Defining the Context	Definition of internal and external parameters to be taken into consideration when managing risk, definition of the field of application and risk criteria for risk management policy.
External Context	External environment in which IIT tries to pursue its goals. [The external context may include: the cultural, social, political, cogent, financial, technological, economic, natural and competitive environment, whether international, national, regional or local. Key drivers and trends having an impact on IIT objectives; relationships, perceptions and values of external stakeholders].
Internal Context	Internal environment in which IIT tries to pursue its goals. [The internal context may include: governance, organizational structure, roles and responsibilities; policies, objectives and strategies put in place to pursue them; skills, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); information systems, information flows and decision-making processes, relations and perceptions and values of internal stakeholders who share the culture of IIT; standards, guidelines and models adopted by IIT; forms and extensions of contractual relations].
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.
Identification of Risk	Risk analysis, identification and description process.
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 IIT 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 comparison of 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 risk.

Control	Adequate technical and organizational measure modifying the risk.
Residual Risk	Risk remaining after risk treatment.

2.6. METHODOLOGICAL APPROACH FOR THE DEFINITION OF THE 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, IIT has adopted a methodological approach in line with the requirements of the GDPR, the standards and best practices in the field of personal data protection.

2.6.1. ASSESSMENT: PRINCIPLES

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

As part of this analysis, IIT 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 updating and enriching the census and the processing register adopted by IIT in compliance with legal obligations;

ii. collection of relevant privacy documentation;

iii. collection of information on information flows and systems to support the processes examined and assessment 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, a final report was drafted, which highlighted the privacy risk profile and the actions to be taken. This activity was completed at the end of January 2008 with the presentation of the aforementioned report to the IIT Executive Committee.

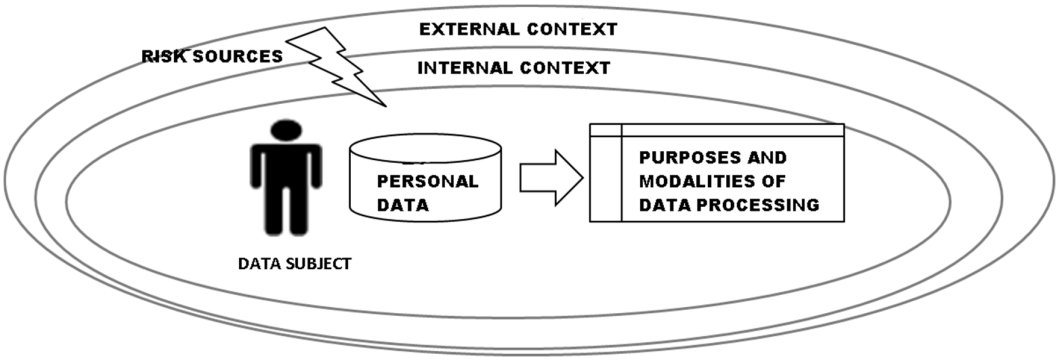
The methodology adopted is described below.

The relative documentation is available at the Legal Affairs Directorate, in charge of archiving it and making it available for consultation to anyone authorized to view it.

2.6.2. 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 – Evaluation of the Reference Context



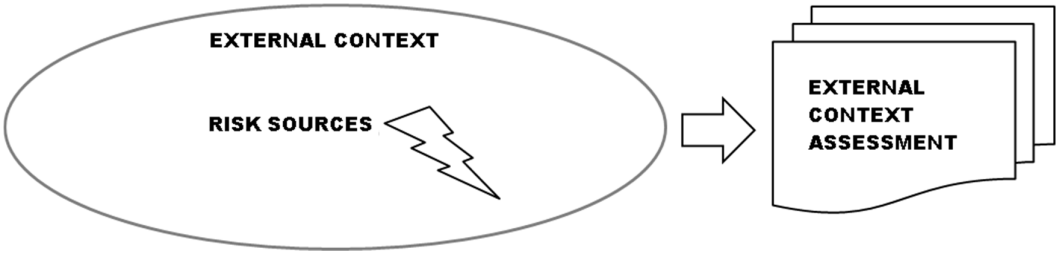
External Context

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

- sectoral context;
- regulatory context;
- technological context;
- socio-economic context;
- territorial context.

TABLE OF FACTORS FOR THE EVALUATION OF THE EXTERNAL CONTEXT	
Sectoral context	Evaluation of aspects concerning suppliers, third parties, visitors of the sector in which IIT operates.
Regulatory context	Evaluation of the applicability of the GDPR and of regulations, including specific sector regulations, applicable to IIT regarding 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 IIT and potential threats.
Territorial context	Evaluation of the characteristics of the territorial context outside IIT and of its impact on the protection of personal data.

Figure 2 – Evaluation of the External Context



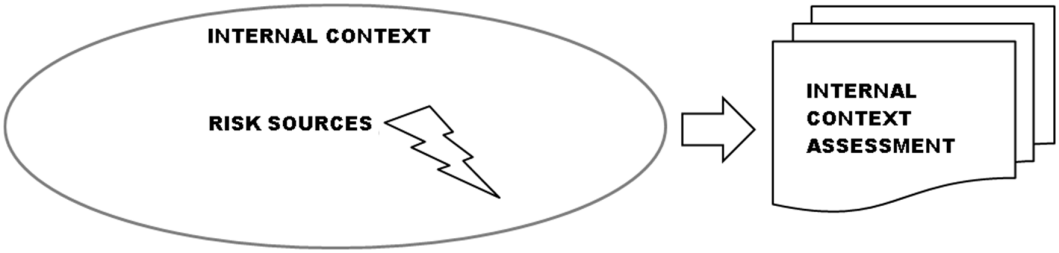
Internal Context

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

- legal context;
- organizational and human resources context;
- IT context;
- physical and environmental context.

TABLE OF FACTORS FOR THE EVALUATION OF THE INTERNAL CONTEXT	
Legal context	Assessment of the legal nature and liability of IIT on the basis of which personal data is processed.
Organizational and human resources context	Evaluation of the organizational model and human resources 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 plants) and environmental characteristics through which personal data is processed.

Figure 3 – Evaluation of the Internal Context



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.

2.6.3. ASSESSMENT: ANALYSIS OF THE PARTIES INVOLVED IN PERSONAL DATA PROTECTION

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

TABLE OF THE PARTIES INVOLVED IN THE PROTECTION OF PERSONAL DATA OF IIT		
PARTY INVOLVED	INVOLVEMENT	NEEDS AND EXPECTATIONS
Controller	Ensures compliance with the requirements of the applicable legislation	Ensure compliance with applicable requirements regarding the protection of personal data. 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 actor that processes personal data on behalf of the data controller	Be appointed external data processor in accordance with the requirements of the GDPR. To receive clear and documented instructions from the data controller regarding the processing to be performed.
Internal Data Processor	Internal actor that processes personal data within IIT	Be an instrument of accountability and control on behalf of the controller. To be appointed as internal data processor in accordance with the requirements of the GDPR.

		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 the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures (operational controls) regarding the protection of personal data.
Internal Person Tasked with Processing	Processes personal data within IIT (e.g. employee, collaborator)	Receive clear and documented instructions on the processing of personal data from the controller and/or the internal processor. Receive training for the correct application of the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures (operational controls) regarding protection of personal data.
External Person Tasked with Processing	Processes personal data of IIT and is appointed by the external Data Processor	Receive clear and documented instructions on the processing of personal data from the external processor. Receive training for the correct application of the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures (operational controls) regarding protection of personal data.
System Administrator	Processes personal data of IIT and is appointed by IIT or by the external Data Processor	Receive clear and documented instructions on the processing of personal data from the controller. Receive training for the correct application of the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures (operational controls) regarding protection of personal data.
Data Subjects	Subjects whose personal data are processed	Obtain from IIT, 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 processing carried out by IIT. Be able to express consent to individual processing, where necessary. Have an easily accessible contact point to exercise rights.
Privacy Guarantor	Oversees the correct application of the legislative requirements	Receive timely reports from IIT, the data controller, in the event of incidents or violations regarding information protection. Receive collaboration from IIT, with regard to requests concerning the application of regulatory requirements.

2.6.4. ASSESSMENT: RISK ANALYSIS

- ***Risk analysis and management***

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

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

i. identification of the architecture, of the parties involved, of the 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 - Risk Management for the Protection of Personal Data

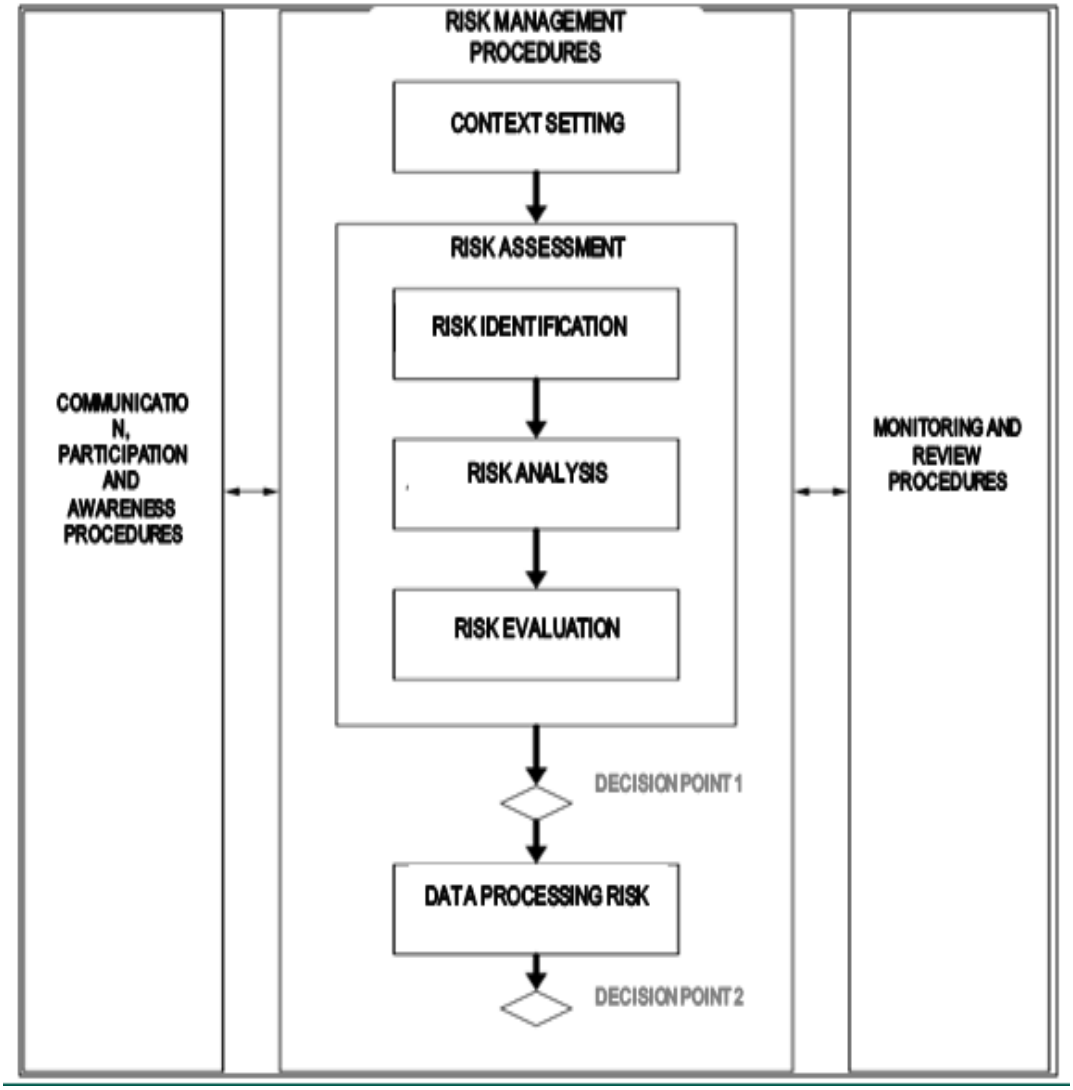
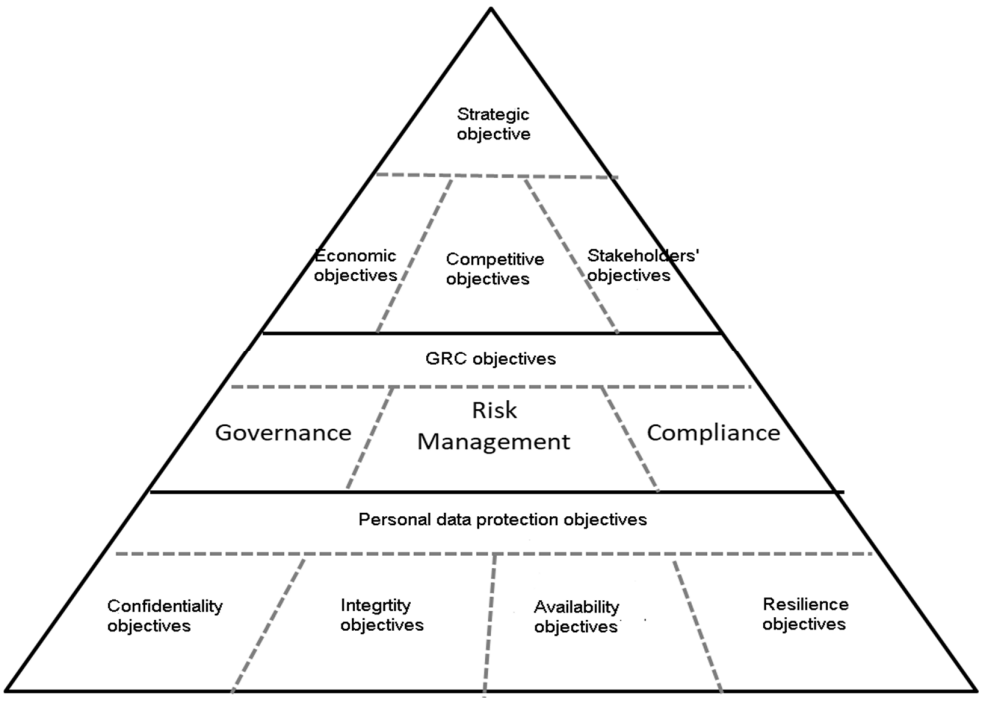


Figure 5 – Risk and Impact Assessment

Depending on the addresses adopted, IIT has decided to pursue the following strategic objectives with regard to protection of personal data:

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 of the related resilience objectives;
3. integrity of personal data processed.

Figure 6 – Objectives for the Protection of Personal Data



As part of the activities to adjust to the GDPR, within IIT assessments of organizational measures, technical measures and of the security risk have been carried out. These assessments have been reported in the assessment report, and in the processing register, to which reference is made.

Based on the level of risk, the criteria of acceptability of the risk level are defined as shown in the following table.

ESTIMATION TABLE OF RISK ACCEPTABLITY		
CRITERIA	ACCEPTABLITY ASSESSMENT	OPTIONS
Risks level equal to or greater than medium-low	Not acceptable	Adopt adequate technical organizational measures to minimize risk as far as reasonably possible
Risks that imply non-compliance with mandatory requirements	Not acceptable	Adopt adequate technical organizational measures to minimize risk as far as reasonably possible
Risks that have significant impacts on the freedoms and fundamental rights of data subjects	Not acceptable	Adopt adequate technical organizational measures to minimize risk as far as reasonably possible

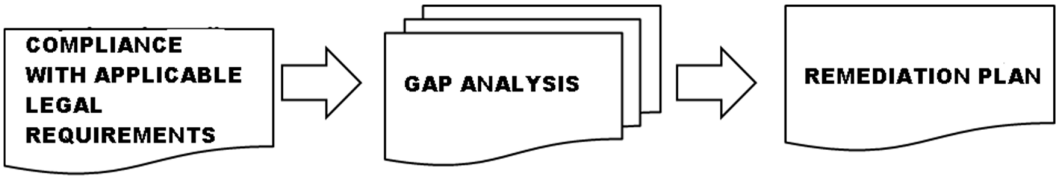
Risks estimated to be not acceptable must be addressed by defining and applying technical and organizational measures (operational controls).

2.6.5. ASSESSMENT: GAP ANALYSIS

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

1. any deviations from the requirements (gap analysis);
2. any realignment plans (remediation plan).

Figure7 – Gap Analysis and Remediation Plan



The risk treatment actions, i.e. the technical and organizational measures identified by IIT, have been defined by the Legal Affairs Directorate and by the Information Systems and Telecommunications Directorate in the final assessment report to which reference is made.

2.6.6. REMEDIATION: PRINCIPLES

Following the assessment carried out, IIT deemed it necessary to adopt the following appropriate measures:

- Privacy reports and consents: updating and drafting of privacy information (e.g. for employees, collaborators, candidates, suppliers, visitors, customers, volunteers involved in research projects) and related consents;

- Procedures: adoption of procedures specifically in the field of privacy, such as the procedure relating to the pseudonymisation of personal data, to management of data breach, to the preliminary assessment of the impact on data protection (PIA - Privacy Impact Assessment), to CV management, to the management of Tenure Track CVs, data retention, etc.;

- Appointments of internal actors: appointments of data processor, internal data processor and system administrator in order to define the scope of processing granted to internal actors who process 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 authorized actors only;

- Appointments of external subjects: appointments of third-party companies accessing data as external data processor and system administrator, providing for periodic checks of third-party suppliers, in particular the processing of employee data, so as to have control over data processing carried out on behalf of IIT. In this context, periodical updates of the list of external suppliers are envisaged – and in particular of those that process personal data;
- Video surveillance: drafting and/or updating of reports, of appointments of person tasked with processing and of the data processor, of the regulation on video surveillance;
- System administrators: updating of appointments;
- Organizational Model for protection of personal data;
- Security measures: adoption and/or drafting of adequate processes with reference to the security of personal data and adoption or reinforcement of system security measures;
- Training: providing for the periodic training of employees and collaborators on personal data protection;
- Processing register: obligation to adopt a register to track all processing carried out;
- DPO: obligation to appoint a DPO that guarantees better control of data governance and constitutes proof of the controller's accountability;
- Maintenance: adoption of periodical verification processes of conformity to the GDPR.

2.6.7. REMEDIATION: ROLES AND TASKS – GOVERNANCE AND THE ORGANIZATION

IIT therefore has considered the identification of the following roles and tasks an adequate measure, formalized with appropriate appointments and instructions:

TABLE OF PARTIES INVOLVED IN THE PROTECTION OF IIT PERSONAL DATA		
INTERESTED PARTY	INVOLVEMENT	NEEDS AND EXPECTATIONS
Data Controller	Ensures compliance with the requirements of the applicable legislation	Ensure compliance with applicable requirements regarding personal data protection. Evaluate and address data processing risks. Define and assign roles and responsibilities with regard to the processing of personal data within the company, the data controller, and to external parties that process data on its behalf.
External Data Processor	External party that processes personal data on behalf of the data controller	Be appointed external data processor in accordance with the requirements of the GDPR. Receive clear and documented instructions from the data controller regarding processing to be performed.
Internal Data Processor	Internal party that processes personal data within IIT	Be an instrument of accountability and control on behalf of the controller. Be appointed as internal data processor in accordance with the requirements of the GDPR. Receive clear and documented instructions on the processing of personal data by the data controller and provide it to the internal tasked person. Receive training for the correct application of the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures

		(operational controls) regarding the protection of personal data.
Internal Person Tasked with Processing	Processes personal data within IIT (e.g. employee, collaborator)	Receive clear and documented instructions on the processing of personal data by the data controller and/or the internal data processor. Receive training for the correct application of the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures (operational controls) regarding the protection of personal data.
External Person Tasked with Processing	Processes personal data within IIT and is tasked by the external data processor	Receive clear and documented instructions on the processing of personal data by the external data processor. Receive training for the correct application of the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures (operational controls) regarding the protection of personal data.
System Administrator.	Processes personal data within IIT, is tasked by IIT or by the external data processor	Receive clear and documented instructions regarding the processing of personal data by the controller. Receive training for the correct application of the personal data processing requirements. Be made aware of the risks and the appropriate technical and organizational measures (operational controls) regarding the protection of personal data.
Data Subjects	Subjects whose personal data are processed	Obtain from IIT, 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 processing carried out by IIT. Be able to express consent to individual processing, where necessary. Have an easily usable contact point to exercise rights.
Data Protection Officer (DPO)	Party entrusted with IIT data protection	Provide clear and documented advice and instructions on the processing of personal data. Provide training for the correct application of the personal data processing requirements. Raise awareness of the risks and appropriate technical and organizational measures (operational controls) regarding protection of personal data. Be in contact with the Guarantor. Act as a contact point for data subjects and for the Guarantor. Provide support in the area of Risk and Privacy Impact Assessment and Data Breach notification. Keep the data breach register up to date. Additional tasks are highlighted in Section 3 of this Model.
Legal Affairs Directorate	Entrusted with the management of privacy legislation in IIT	Manage issues of relevance to data protection, acting as an internal reference point for the other

		Directorates and/or Offices and/or Research Lines. Collaborate with the DPO. Keep the processing register, appointments and instructions to the appointees, internal/external managers, system administrators, and information for data subjects updated. Organise training.
Privacy Guarantor	Supervise the correct application of the regulatory requirements	Receive timely reports from IIT, the data controller, in the event of accidents or violations regarding information protection. Receive collaboration from IIT, in the context of requests concerning the application of regulatory requirements.

2.6.8. REMEDIATION: POLICIES

- ***Policies for the protection of personal data***

IIT has deemed it necessary to commit to ensuring that all personal data processing performed by IIT takes place in compliance with the applicable mandatory requirements, with particular reference to the principles and rules to be observed.

In the context of this Model and of the procedures adopted and disclosed internally at IIT, IIT formalizes the guidelines regarding behavioural principles and new rules, pillars of compliance regarding protection of personal data, raising awareness through appropriate information activities and training of all personnel, including personnel collaborating with IIT, on the systematic and timely compliance with the same principles and rules.

In particular, the following procedures have been adopted, for example:

- Preliminary assessment on the impact on data protection (PIA - Privacy Impact Assessment), which describes the risk-based methodology for assessing the processing of personal data;
- Pseudonymisation of personal data, which describes the methodology with which to carry out and manage pseudonymisation of data;
- Data Retention, which describes which data are processed by IIT, the necessary processing period and therefore the retention period, and how the relative erasure must be carried out;
- Data Breach Management, which describes the process of notification to the DPO and therefore to the authority and to the data subjects, where deemed necessary, of violations of personal data;
- CV Management, which provides indications on the process of managing CVs of candidates and employees and collaborators within IIT;
- Management of Tenure Track CVs provides information on the process of managing the CVs of those involved in the Tenure Track of IIT.

For more details, procedures published on the IIT intranet are referred to.

2.6.9. REMEDIATION: REPORTS, CONSENT

IIT has deemed it necessary to commit to ensuring that all the subjects whose personal data are processed are adequately informed.

For this reason, IIT has planned to update all reports for data subjects and relative consent, and has planned activities to raise awareness for employees and collaborators. This has also been stressed on the intranet, as well as with specific training.

2.6.10. REMEDIATION: APPOINTMENTS AND INSTRUCTIONS

IIT has deemed it necessary to commit to ensuring that subjects whose personal data are processed are adequately informed and instructed.

For this reason, IIT has planned to appoint internal and external data processors and to provide persons tasked with processing with updated instructions. This has also been stressed with dedicated training.

2.6.11. REMEDIATION: TRAINING – AWARENESS

IIT has deemed it necessary to commit to ensuring that all subjects who process personal data are properly trained.

For this reason, IIT has planned to provide appropriate training both for the persons tasked with processing and for the internal data processors, with reference to the contents of the GDPR and the new procedures adopted by IIT.

2.6.12. REMEDIATION: PROCESSING REGISTER

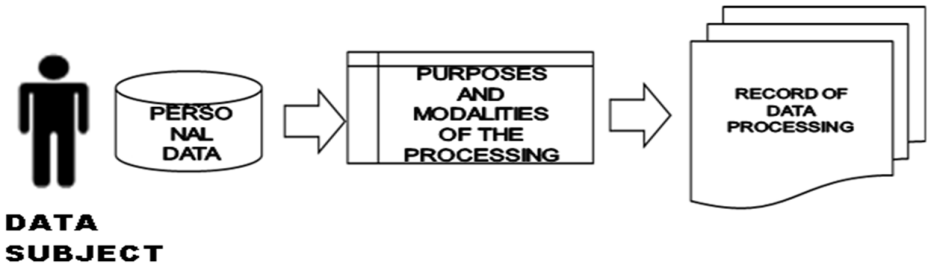
Following the assessment activities carried out, it has emerged that IIT processes data that can be classified as personal data pursuant to the GDPR.

IIT has deemed it necessary to update the descriptive list of this processing contained in the processing register.

The processing register includes the processing activities carried out under the responsibility of the data controller/processor. The document contains the name and contact details of the data controller and data protection officer; the purposes of processing; the description of the categories of data subjects and personal data; the categories of recipients of personal data; where applicable, transfers of personal data to a third country or to an international organization, identification of the third country or international organization and documentation of adequate guarantees; where possible, the deadlines set for the erasure of the different categories of data.

This has also been stressed on the intranet and with dedicated training

Figure 8 – Personal Data Processing Register



In this regard, for more details, please refer to what has been highlighted in the IIT processing register.

2.6.13. REMEDIATION: THE RIGHTS OF DATA SUBJECTS

IIT 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.

2.6.14. REMEDIATION: THE IIT INTERNAL CONTROL SYSTEM

IIT has deemed it necessary to commit to ensuring the adoption of adequate control, monitoring, audit and privacy review tools.

To this end, it has prepared this 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 IIT in that operational tasks are distinct from control tasks, reasonably reducing any potential conflict of interest.

In particular, the IIT internal control system is based not only on the rules of conduct established in this Organizational Model, but also on the following elements:

- the Organization, Management and Control Model adopted pursuant to Legislative Decree 231 of 2001 and to the Code of Conduct and Code of Scientific Conduct;

- the system of procedures adopted by IIT;

- the hierarchical-functional structure (organization chart), the parties involved in the protection of personal data (including internal and external subjects, processors and persons tasked with the processing and the organizational structures of governance and supervision of IIT);

- the system of proxy and delegation;

- integrated information systems aimed at separating functions and protecting the information they contain, with reference both to management and accounting systems and to the systems used to support the operational activities of IIT;

- the operations' traceability, according to which the operations have to be – as much as possible - adequately documented and the processes of decision, authorization and development of the operations must be verifiable *ex post* also through appropriate documental support;

- the support provided by the Legal Affairs Directorate to the other Directorates and/or Offices in the management of those activities that involve profiles of compliance with specific regulations (e.g. personal data protection management);

- periodic activities of verification of the actual functioning of the controls carried out by the Internal Control and Risk Management Directorate (Internal Audit and Compliance).

The IIT's current internal control system - meant as a process implemented by IIT in order to manage and monitor the main risks and allow the operational and organizational management to be conducted in a correct and proper way - is able to guarantee the achievement of the following objectives:

- effectiveness and efficiency in using resources, in protecting IIT from losses and safeguarding IIT's assets;

- compliance with laws and regulations applicable to all IIT's operations and actions;

- reliability of information, to be meant as timely and reliable communications able to guarantee the correct execution of each decision-making process.

Responsibility for the proper functioning of the internal control system lies with each Directorate and /or Office and/or Research Line for all processes for which it is responsible (in this regard, see letter a) below).

The structure of controls in IIT provides for:

a) line or first level controls, carried out by the single Directorates and/or Offices and/or Research Lines on the processes for which they have the management responsibility, aimed at ensuring the correct performance of the operations;

b) cross-cutting, second level controls, concerning the operational and the non-compliance risks, carried out by specific functions such as Compliance, Risk Manager, DPO, etc.;

c) third level controls, aimed at evaluating the plan and the effective functioning of the internal control system, carried out by the Internal Audit.

The control activities concerning Data Protection are better clarified in the next two sections of this Organizational Model.

SECTION THREE

3. BODIES AND FUNCTIONS INVOLVED IN DATA PROTECTION

3.1. THE DATA PROTECTION OFFICER

3.1.1. APPOINTMENT OF THE DATA PROTECTION OFFICER

As part of the program to adjust to the GDPR, IIT has provided for the appointment of the data protection officer (also DPO) pursuant to art. 37 of the GDPR.

3.1.2. DUTIES OF THE DATA PROTECTION OFFICER

Duty of the DPO is to facilitate the implementation of the GDPR on the part of the data controller/data processor, cooperate with the authority and act as point of contact, also with respect to data subjects, for questions related to the processing of personal data (arts. 38 and 39 of the GDPR).

The DPO must be able to offer, with the degree of professionalism appropriate to the complexity of the task to be performed, the advice necessary to plan, verify and maintain an organized system of personal data management, assisting the data controller in adopting a set of measures (also security measures) and guarantees appropriate to the context in which he/she is called to operate. He/she must also act in full independence (Recital 97 of the GDPR) and autonomy, without receiving instructions and reporting directly to top management.

In particular, the duties of the IIT DPO are the following:

a) to inform and provide advice to the data controller or to the data processor as well as to the employees who carry out the processing on the obligations deriving from the GDPR, as well as from other national or European Union provisions relating to data protection;

b) monitor the compliance of the data controller or of the data processor regarding the protection of personal data, including the assignment of responsibilities, awareness-raising and training of personnel involved in the processing and related control activities;

c) provide, if requested, an opinion on the impact assessment on data protection and monitor its performance pursuant to art. 35 of the GDPR;

d) cooperate with the Guarantor for the protection of personal data;

e) act as a point of contact with the Guarantor for the protection of personal data for issues related to processing, including prior consultation referred to in art. 36, and carry out consultations, as appropriate, in relation to any other matter;

f) support the data controller in keeping the processing register, following the instructions given by the data controller.

In particular, the DPO periodically checks the effectiveness and application of the IIT procedures and of the Organizational Model and provides support in the periodic updating of the processing register, as well as of the procedures and the Organizational Model where necessary.

The DPO also periodically reviews the effectiveness of the Privacy Impact Assessments carried out.

The DPO is also in charge of the notification of data breach and of updating the relative register.

3.2. LEGAL AFFAIRS DIRECTORATE, INFORMATION AND COMMUNICATION TECHNOLOGY DIRECTORATE AND OTHER FUNCTIONS OF SUPPORT

In order to be able to carry out his/her duties, the DPO collaborates with the Legal Affairs Directorate, with the Information and Communication Technology Directorate and with additional functions accordingly involved in the assessment and analysis of specific issues concerning data protection (e.g. HROD, Research Lines).

3.3. INFORMATION FLOWS TOWARDS THE DATA PROTECTION OFFICER

In order to carry out his/her duties, the DPO must be involved, as soon as possible, in the activities of defining mitigation or prioritization measures, and in all matters relating to the processing of personal data, for the purposes of compliance with the requirements of the Regulation.

In this regard, the Heads of Directorates and/or Offices and/or Research Lines involved in the management of the processing of personal data must carry out communication activities and consultation with the DPO in accordance with the specific procedures referred to in paragraph n. 2.6.8.

3.4. MONITORING, EVALUATION AND CONTINUOUS IMPROVEMENT

IIT, in its capacity of data controller, and the internal data processors, must systematically monitor the adequacy, effectiveness and actual operation of the Organizational Model regarding personal data protection.

With regard to adequacy, effectiveness and actual operation, the assessment of the Organizational Model must be carried out, by way of example which is not exhaustive, in the following cases:

- 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 same data controller;
- review, on an annual or periodic basis, where defined. Re-examination, on an occasional basis, must be performed in the following cases:
    - serious or repeated non-compliance, including violations of the regulatory requirements or of the requirements defined by the data controller;
    - accidents concerning the protection of personal data (so-called “data breach”);
    - significant changes in the external reference context, including changes in the regulatory framework;
    - significant changes in the internal reference context.

Furthermore, IIT is aware of the importance of adopting and effectively implementing an Organizational Model for the protection of personal data pursuant to the GDPR, suitable for preventing the risks and damages deriving from the implementation of illicit processing of data, of promoting reviews and continuous adaptation of the Organizational Model according to the opportunities for improvement identified by risk assessment, monitoring, audit and analysis of accidents and non-compliance.

3.5. AUTHORS OF MONITORING, EVALUATION AND CONTINUOUS IMPROVEMENT

Monitoring is performed by the data protection officer within the scope of his/her functions.

3.6. REPORTING

In order to promote compliance with the GDPR, IIT 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.

To this end, a communication channel has been established for the direct consultation of the DPO (i.e. E-mail address dpo@iit.it).

IIT prohibits retaliatory behaviour or any other form of discrimination or penalisation against the reporting part.

All information and documentation relating to the reports referred to in this paragraph are collected and kept by the DPO.

SECTION FOUR

4. COMPLIANCE AND PENALTY PROVISIONS

In case of violation of the provisions of this Organizational Model by employees of IIT 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.

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

The violation of the provisions of the Organizational Model may constitute a breach of the obligations of the employment agreement and/or a disciplinary offense, in accordance with the procedures set forth in art. 7 of the Workers' Statute, entailing all legal consequences, also with regard to the continuation of the employment agreement and possible compensation for damages.

Furthermore, compliance with the principles of this Organizational Model represents an essential part of the contractual obligations undertaken by the collaborators.

The violation of the Organizational Model by third parties may constitute non-fulfilment of the obligations agreed to, entailing legal consequences also with regard to the faculty of IIT to terminate the contract and to possible compensation for damages.

5. DISSEMINATION OF THE ORGANIZATIONAL MODEL

IIT 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, has defined a communication and training program aimed at ensuring the dissemination of skills and the necessary knowledge to correctly and systematically apply company provisions on personal data protection, including this Organizational Model.

The information and training activity must involve all employees and collaborators, as well as all the resources that will be included in IIT in the future. In this regard, the relative training activities must be planned and concretely carried out both at the time of hiring, and on the occasion of any change of duties, as well as following updates and/or changes to the Organizational Model.

With regard to the dissemination of the Organizational Model, IIT commits to:

- send a communication to all personnel concerning the adoption of this Model;
- publish the 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 the applicable legislation regarding the protection of personal data;
    - treat personal data in a way that minimizes relative risks, being aware of the consequences of non-compliance with the regulations, procedures and operational controls defined by IIT;
    - 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 Affairs Directorate available for consultation by anyone who is authorized to view it.