PERSONAL DATA PROTECTION POLICY

(approved by order of the Rector on 9 December 2021)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – General Data Protection Regulation (hereinafter "GDPR") establishes the rules with regard to the processing of personal data and on the free movement of such data, with a view to safeguarding the fundamental rights and freedoms of natural persons and, especially, the protection of their personal data.

This Data Protection Policy of Iscte – Instituto Universitário de Lisboa (hereinafter referred to as Iscte), reflects Iscte's commitment and responsibility to uphold a level of personal data protection in accordance with the GDPR, with GDPR Implementing Law 58/2019 in the Portuguese legal system (hereinafter referred to as GDPR Implementing Law) and all other national or european legislation on data protection, promoting the involvement of all the teaching staff, researchers, employees, partners/contributors, all students and other stakeholders.

A. INTRODUCTION

Iscte collects and processes personal data for management, administration, teaching, research and other purposes which are legally required. Iscte is committed to everything with respect to the protection of personal data of its managers, teaching staff, researchers, employees, students, suppliers, partners and all other data subjects related to Iscte, as a fundamental right protected by national and European legislation. This Personal Data Protection Policy (hereinafter referred to merely as Policy) seeks to establish Iscte's commitment to the rules on privacy and personal data protection.

A.1 SCOPE

a) This Policy is applicable to all the managers, teaching staff, researchers, employees and contributors under a service provider arrangement (hereinafter jointly referred to as "**workers**"), as well as the students of Iscte's study cycles who, in that context, produce work that may process personal data, and who should consult and be familiar with this Policy, comply and ensure compliance with its terms.

b) This Policy also aims to inform all of Iscte's students, suppliers / service providers, partners and stakeholders of Iscte's commitment to personal data protection.

c) Iscte may complement or amend this Policy with other policies, regulations or guidelines.

A.2 OBJECTIVES

a) This Policy's objective is to uphold high-level protection to the collected data, in accordance with the applicable legal rules and under terms that promote the engagement and motivation of the managers, teaching staff, researchers, employees, contributors, subcontractors, suppliers/service providers, partners and students towards the need to maintain the confidentiality of the collected personal data.

b) It also seeks to frame the procedures for the processing of personal data by the workers and third parties who have access to personal data as a result of the performance of their duties.

c) The existence of this Policy infers its regular consultation by the workers who perform any activity involving the processing of personal data.

B. DATA CONTROLLER

1. The Data Controller is responsible for compliance with the data protection rules. The Data Controller is responsible for ensuring and being able to demonstrate that the personal data processing is carried out in conformity with the legislation on data protection.[1]

2. Whenever Iscte exclusively determines the purposes and the material and human means of personal data processing, the Data Controller is Iscte, with head office at Avenida das Forças Armadas, 1649-026 Lisboa.[2]

3. When Iscte determines, together with other entities or individuals, the purposes and means of a processing, both parties are jointly responsible for the processing, in which case they determine, by mutual agreement in a transparent manner, the respective responsibilities in compliance with the General Regulation of Data Protection (GDPR).

C. ETHICAL AND LAWFUL PERSONAL DATA PROCESSING

Iscte processes personal data in accordance with the legislation in force and in accordance with the rules on professional ethics and conduct defined in its policies and codes of conduct, guidelines and internal regulations, with a view to permanent compliance with and adjustment to the regulatory framework, meaning that this Policy also consists of a supporting process in the general mapping of processes in Iscte's Integrated Quality Assurance System (SIGQ-Iscte)

D. POSITION OF THE DATA PROTECTION OFFICER

1. Iscte mandatorily appoints a Data Protection Officer (DPO) and ensures the conditions for this officer to perform duties with autonomy and independence.

2. Iscte provides the necessary resources for performance of the duties of Iscte's DPO and for the maintenance of this officer's knowledge, giving the officer access to personal data and processing operations.

[1] GDPR, Article 24.
[2] For purposes of the provisions in Articles 4 and 24 of the GDPR.

3. Iscte's DPO is entrusted, among others, with the following duties:

a) Controlling the compliance of the data processing with the applicable regulations.

b) Maintaining relations with the data subjects on matters covered by the GDPR, the GDPR Implementing Law and all other national legislation on data protection.

c) Informing and advising Iscte, subcontracted entities and workers that process data on their obligations concerning data protection.

d) Cooperating with the National Data Protection Authority and acting as a point of contact of this authority on issues related to data processing.

4. The autonomy of Iscte's DPO, including control of compliance, is circumscribed to this officer's duties. Iscte remains responsible for compliance with the data protection regulations and should be able to demonstrate that compliance.[3]

5. Data subjects may contact Iscte's DPO about any issues related to the processing of their personal data and on the exercise of their rights granted by the GDPR.

6. Iscte's DPO is bound to the duty of professional secrecy and confidentiality when performing her/his functions, but may, nevertheless, perform other functions and duties, where Iscte ensures that these functions and duties do not give rise to a conflict of interest.

[3] GDPR, Article 5(2). Control of compliance does not mean that the Data Protection Officer is held personally accountable in the event of non-compliance. The GDPR clarifies that the Data Controller, and not the Data Protection Officer, is responsible for implementing the "appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." (Article 24(1)). In turn, the Article 29 Data Protection Working Party Guidelines on Data Protection Officers, of 13 December 2016, clarify that "The autonomy of DPOs [Data Protection Officers] does not, however, mean that they have decision-making powers extending beyond their tasks." Compliance with the data protection rules is a corporate or institutional responsibility of the Data Controller, and not of the Data Protection Officer.

E. DATA PROTECTION TEAM

1. Iscte may create a Supporting Team for Data Protection. The team would preferably include the following members, among others:

a) Iscte's DPO.
b) A member of the legal office with specialised knowledge of public law and/or data protection law.
c) A specialist in information security.

2. The team members collaborate, in the context of the duties attributed by Iscte, in articulation and/or mutual consultation for the accomplishment of the tasks in the sphere of data protection.

F. LEGAL GROUNDS FOR PROCESSING PERSONAL DATA

1. Iscte processes personal data provided that at least one of the following legal grounds are observed:

a) The data subject has given consent based on free, specific, informed and unambiguous willingness as to the processing of their personal data for one or more purposes;

b) The processing is necessary for the performance of a contract in which the data subject is a party or for pre-contractual procedures at the request of the data subject;

c) The processing is necessary for compliance with a legal obligation to which Iscte is subject;

d) The processing is necessary for defence of vital interests of the data subject or another natural person;

e) The processing is necessary for performance of a task carried out in the public interest or in the exercise of the public authority vested in Iscte;

f) The processing is necessary for the purposes of the legitimate interests pursued by Iscte or third parties, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2. Whenever the processing is based on the need to pursue the legitimate interests of Iscte or third parties (item (f)), and in view of the theoretical and interpretative complexity of the concept, prior consultation of Iscte's DPO, whose contacts are presented in point J of this Policy, is recommended.

3. Iscte documents the grounds of lawfulness of the data processing. Processing carried out by functional units is documented in the "Records of Processing Activities" system, available for internal consultation on the Fénix system.

G. RIGOROUS CONTROL OF SENSITIVE DATA

1. When Iscte processes sensitive data, including special categories of data and data of highly personal nature, it does so in strict compliance with the principle of data minimisation, all other legal regulations and in accordance with this Policy.

2. The processing of special categories of personal data is prohibited, namely data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of these sensitive data is prohibited, except for the exemptions established in Article 9 of the GDPR.

3. When Iscte processes special categories of data, the prior and explicit consent of their data subjects is the legal grounds which should preferably, and whenever possible, be used.

4. In view of the added risks of processing special categories of data, new data processing of this nature, whenever of the initiative of the functional units, shall be previously articulated with Iscte's Rectory and the DPO.

5. In the context of scientific research, whenever special categories of data are processed, or the processing involves any other criteria stipulated in section III.B of the 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 (EU) 2016/679, the principal investigator should consider the submission of the project in question to Iscte's Ethics Committee.

H. PRINCIPLES FOR PERSONAL DATA PROCESSING

H.1 Lawfulness of the Processing and Provision of Information to the Data Subject

1. When processing personal data, Iscte ensures that the processing has one of the legal grounds mentioned above *(principle of lawfulness)*.

2. The Data Controller provides the data subjects with information on the processing to be carried out *(principles of fairness and transparency)*:

a) Iscte provides this information to the data subjects through "Privacy Notices" or, in the case of data processing in scientific research projects, through "Participant Information Sheets."

b) The information to be provided includes Iscte's identification as Data Controller, the provision of a contact at Iscte responsible for communicating with the data subjects, the contacts of Iscte's DPO, the purposes and legal grounds of the processing, identification of the rights of the data subjects, the personal data storage period or the criteria used to define that period, among other information.

H.2 Purpose of the Processing

Iscte collects personal data for specific, explicit and legitimate purposes. Data collected for a specific purpose are not subsequently used for a purpose incompatible with the initial purpose *(principle of purpose limitation)*.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes, but should, in all cases, respect the ethical standards and privacy of the participants in research work and any other guidelines of Iscte relative to data processing in a scientific research context.

H.3 Data Minimisation

Personal data processed by Iscte are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed *(principle of data minimisation)*.

H.4 Accuracy

Personal data shall be accurate and kept up to date *(principle of accuracy)*. Data subjects should notify Iscte of any change in order to enable the personal data to be rectified or updated accordingly. The contacts for updating requests are presented in the Privacy Notices or, in the case of scientific research, in the Participant Information Sheets.

H.5 Storage of Personal Data and Storage Periods

1. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed *(principle of storage limitation)*.

2. When processed exclusively for statistical, scientific research or historical purposes, and provided that the ethical standards and privacy of the participants in research work and any other guidelines of Iscte relative to data processing in a scientific research context are respected, personal data may be stored for longer periods of time.

3. When there is an applicable legal storage rule, personal data are stored for the legally established period.

4. At Iscte, personal data are stored and subsequently destroyed or anonymised pursuant to the requirements established in the "Iscte Archival Regulation" defined by Order no. 1271/2004, complemented, for everything absent therein, by the grounds and time limits defined by Iscte in the "Records of Processing Activities" system, available for internal consultation on Fénix.

H.6 Security and Confidentiality

1. Iscte processes personal data in a manner that ensures their security and confidentiality, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures according to the risk of each processing operation (*principles of integrity and confidentiality*). These measures include, among others, those endowing the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

2. Iscte's workers and students shall respect the duty of secrecy and confidentiality established herein, and shall not reveal personal data to which they had access while performing their duties, or pursuing academic work, to third parties without the proper authorisation.

3. Manual records of personal data shall not be kept in places where they can be accessed by unauthorised personnel and cannot be taken outside Iscte's facilities without explicit written authorisation. Personal data are accessible only to those who need to use them. In general, personal data are kept:

- In a closed room with controlled access; and/or
- In a closed drawer or closed filing cabinet.

4. If computerised, personal data shall be protected by appropriate technical and organisational measures to ensure an adequate security level for the risk, taking into account, namely, the risks represented by the processing, in particular due to the destruction, loss and accidental or unlawful alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

5. In order to ensure adequate protection of personal data, it is crucial that access to personal data should be limited and restricted to the scope of that strictly necessary for accomplishing the applicable purpose.

6. With a view to the fulfilment of Iscte's mission and obligations, the provision of services, coordination, efficiency, flexibility and sound organisational articulation, the processing of personal data may be carried out by more than one functional unit of Iscte. The identification of the functional units or workers with access to personal data is documented in the Records of Processing Activities. The implementation of the access authorisations in the information system is carried out through configuration of the respective permissions, in accordance with the access information documented in the Records of Processing Activities. In cases where occasional sharing by common methods proves necessary, the functional units shall coordinate among one another in order to ensure compliance with the principles and good practice for personal data processing.

7. Under no circumstances whatsoever shall it be permitted for third parties to access personal data held by Iscte, unless there is a non-disclosure contract and/or agreement with that third party adequately safeguarding the protection of personal data.

8. In the case of doubt as to the third party's legitimacy to access personal data held by Iscte, the functional units shall previously consult the Rectory and/or request advice from Iscte's DPO.

H.7 Demonstrated Accountability

1. As Data Controller, Iscte is not only responsible for ensuring compliance with the principles listed above, but also for demonstrating that each processing operation complies with those principles *(principle of accountability)*.

2. Iscte's workers, suppliers and partners that use personal data are individually responsible for compliance with the applicable legal and regulatory provisions.

3. Workers should proceed in conformity with the information and training that has been received, and comply with the guidelines defined in this Policy.

4. Non-compliance with the obligations of this Policy should be reported to the Rectory and the DPO.

H.8 Protection of Personal Data by Design and by Default

In the design of new processing operations, Iscte undertakes the commitment to use the principles of data protection by design and by default. New processing operations shall be subject, both at the time of definition of the means of processing and at the time of the actual processing, the appropriate technical and organisational measures aimed at the effective application of the principles of data protection and the protection of the rights of the data subjects. Technical and organisational measures shall also be applied to ensure that, by default, only personal data that are necessary for each specific processing purpose are actually processed.

I. CONSENT

1. Iscte understands 'consent' as an agreement, in which the data subject was fully informed of the intention to process her/his data and agreed with it, in an appropriate mental state and without the existence of external pressure. Consent obtained under duress or based on misleading/fraudulent information is not a lawful basis for processing.

2. Unless otherwise provided for in the law, the worker's consent does not consist of a requisite for the legitimacy of the processing of that worker's personal data:

a) If that processing gives rise to a legal or economic benefit for the worker; or

b) If that processing is covered by the performance of a contract.

3. The data subject's consent may be withdrawn at any time and from that time onwards Iscte shall suspend the data processing. Withdrawal of consent does not affect the lawfulness of the processing based on the consent before its withdrawal. Before giving consent, the data subject is informed of that fact via the Privacy Notice or, in the case of participants in scientific research work, via the Participant Information Sheet.

J. OBSERVANCE OF THE RIGHTS OF THE DATA SUBJECTS

1. Whether involving a worker, student or third party, all the individuals in relation to whom Iscte processes their personal data have the right to:

a) Submit requests for access in relation to the nature of the information held about them and to whom it was disclosed, and to promote the rectification of inaccurate data.

b) Object to the data processing, whenever the processing is necessary for the performance of a task in the public interest, necessary for the exercise of the public authority vested in Iscte, or necessary for the purposes of pursuing legitimate interests of Iscte or third parties.

c) Request and, under certain conditions, obtaining from the data controller the erasure of their personal data or the restriction of its processing.

d) Be informed about automated decision-making mechanisms that shall significantly affect them and not to be subject to this type of decision unless explicit consent has been given, it is necessary for the performance of a contract with Iscte or if the processing is authorised by the national or European law to which Iscte is subject.

e) Receive personal data concerning them in a structured and commonly used format, and to transmit it to another entity, if the processing is based on the data subject's consent or if the processing is necessary for the performance of a contract.

f) Submit a complaint to Iscte about the way that the processing of their personal data was carried out. Data subjects may submit their complaint directly to Iscte's DPO, using the contacts indicated below. They may also submit complaints directly to the national data protection authority, the *Comissão Nacional de Proteção de Dados* (CNPD).

2. Data subjects may request the exercise of their rights, as described in the "Privacy Notices" or, in the case of participants in scientific research work, in the "Participant Information Sheets", or

in the case of students and workers, in a specific form in the academic information management system (Fénix).

3. Data subjects may contact Iscte's DPO about any issues related to the processing of their personal data and on the exercise of their rights. Consultation of Iscte's DPO shall be made through the following contacts:

Encarregado de Proteção de Dados do Iscte
Iscte – Instituto Universitário de Lisboa
Av. das Forças Armadas 1649-026 Lisboa

E-mail address: dpo@iscte-iul.pt

K. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

1. New processing that may result in a high risk – taking into account the nature, scope, context and purposes – to the rights and freedoms of natural persons, shall be subject to a Data Protection Impact Assessment, DPIA (Article 35 of the GDPR). The Data Protection Impact Assessment aims to identify risks and mitigate them with appropriate guarantees. A Data Protection Impact Assessment is particularly important when new technology is introduced.

2. A Data Protection Impact Assessment is mandatory when there is i) a systematic and extensive evaluation of personal data based on automated processing; ii) processing on a large scale of special categories of personal data; or iii) a systematic monitoring of a publicly accessible area on a large scale.[4]

3. A Data Protection Impact Assessment is also mandatory when the processing is listed on the CNPD's List of personal data processing subject to Data Protection Impact Assessment.[5]

4. Where none of the conditions referred to above are met in new processing, this does not exempt it from being considered high-risk, and thus also being subject to a Data Protection Impact Assessment. Iscte undertakes the following commitments:

a) Previously determine, according to the nature, scope, context and purposes of the processing, the incidence that this new processing could have on the security and

[4] GDPR, Article 35(3).
[5] Regulation 1/2018 related to the list of personal data processing subject to Data Protection Impact Assessment, CNPD, 16 October 2018, https://www.cnpd.pt/home/decisoes/regulamentos/regulamento_1_2018.pdf

confidentiality of the personal data and consequent need to carry out a Data Protection Impact Assessment and the measures to be taken when the results of that assessment are not satisfactory.

b) Consider the European guidelines on Data Protection Impact Assessments and the criteria suggested therein to assess whether the new processing requires a Data Protection Impact Assessment, namely the "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/67 of 4 April 2017, formulated by the Article 29 Data Protection Working Party.[6]

4. Iscte, as Data Controller, is responsible for ensuring that the Data Protection Impact Assessment is carried out, which may be conducted by Iscte or outsourcing. Iscte is also responsible for involving the DPO in its elaboration and requesting the officer's opinion. The opinion of the DPO and the decisions taken by Iscte shall be documented in the Data Protection Impact Assessment.[7]

L. DISCLOSURE OF PERSONAL DATA

1. Considering that there is a legitimate purpose for the processing of personal data, Iscte, as Data Controller, may disclose personal data only to specific categories of receivers, namely public authorities, subcontractors, service providers and partners.

2. When transferring personal data, Iscte requires demonstration that the receivers comply with the GDPR and that the contract between the parties, when applicable, include a clause relative to the protection of personal data.

3. Subcontracted processing is regulated by contract, in which case Iscte ensures that it only uses subcontracted processors that present sufficient guarantees of implementing appropriate technical and organisational measures in a manner ensuring that the processing meets Iscte's requirements in terms of compliance with the principles of data protection and defence of the rights of the data subject.

[6] The Article 29 Data Protection Working Party was instituted under Article 29 of Directive 95/46/EC. The European and national guidelines on DPIA can be consulted on the CNPD website.
[7] Idem.

M. TRANSFER OF DATA TO THIRD COUNTRIES

The transfer, archiving or processing of personal data in another country shall be carried out in accordance with the requirements of the GDPR. When personal data are transferred to a country outside the European Economic Area (EEA) without an "Adequacy Decision"[8], suitable guarantees shall be established using binding rules with legal enforcement, standard data protection clauses that are approved or with explicit consent of the data subjects.

N. USE OF PERSONAL IMAGES

1. Iscte may collect and/or publish images in the following situations and on the following legal grounds:

1.1. Consent of the data subject [Article 6(1)(a) of the GDPR]:

- Reporting related to initiatives or events with prior registration, such as conferences, social events, open days, promotion of different courses, schools and departments, visits to schools, Futurália, international fairs, among others.[9]
- The collection and disclosure of image and voice of speakers at events, whether open events with prior registration or not, requires consent of the data subjects.

1.2. Legitimate interests [Article 6(1)(f) of the GDPR], without prejudice to the right to object:

- External disclosure of the teaching body, research teams (website and Ciência-IUL).
- Internal identification of employees and students (Fénix and other internal platforms).
- Reporting at locations or events without prior registration, accessible to the public, provided that the participants are previously informed of the collection and possible disclosure of images.

[8] In order to enable the free circulation of data with third countries, the European Commission defined the "Adequacy Decision" mechanism, which certifies that other states, via domestic legislation or by signing international agreements, meet the data processing criteria defined by the GDPR. Up to date, the Commission has endorsed "Adequacy Decisions" for Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

[9] These images are primarily disclosed through the various existing channels: website of Iscte and its schools, social networks, blogs and internal television circuit.

2. The head of each functional area shall ensure that the image processing is carried out in accordance with the principle of data minimisation and pursuant to the legal grounds mentioned above.

O. E-MAIL, INSTITUTIONAL LISTS AND SURVEYS

O.1 Institutional E-mail Lists

1. As a rule, the workers and students have an institutional e-mail address, created by Iscte (relative to an iscte-iul.pt domain), used for correspondence concerning academic or professional subjects.

2. E-mail correspondence concerning academic, professional or administrative subjects, between workers and between workers and functional units, is conducted, whenever possible, through institutional addresses.

3. Iscte sends messages with contents for disclosure to institutional e-mail lists, provided that this is within the scope of Iscte's mission.

O.2Application of Surveys on the Iscte Community

1. Iscte's community represents an important and useful universe within which to carry out surveys of interest to the institution, whether in the sphere of the institution's management and administration, or scientific research projects, including, in some cases, in the context of doctoral theses or master's dissertations carried out at Iscte.

The distribution of questionnaires by correspondence to members of the community is carried out on the following legal grounds:

i) Processing that is necessary for purposes of pursuit of legitimate interests of Iscte or third parties;

ii) Processing that is necessary for performance of a task carried out in the public interest or in the exercise of the public authority vested in Iscte;

iii) Consent of the data subjects.

2. When a survey is considered necessary for purposes of legitimate interests pursued by the institution, necessary for performance of duties of public interest or necessary for exercise of public authority, Iscte sends the questionnaire to a set or to all of the members of the community. These surveys are conducted by Iscte's bodies and services, such as the Rectory, General Council,

Pedagogical or Scientific Councils, Social Action Service, Education Management Services, Documentation and Information Service, the Research Support Office, the Office of Studies, Planning and Statistics, among other services or functional units. The criteria for the distribution of questionnaires to Iscte's student population and community are defined by the Rectory.

3. For purposes of sending questionnaires based on legal grounds of consent, Iscte has a system for obtaining/withdrawing consent in its information system for managing consent from students, teaching staff, employees and other contributors.

P. REPORTING OF PERSONAL DATA BREACH

1. All the workers, students, suppliers, partners and data subjects related to Iscte are duty bound to report potential or actual personal data breaches to the Rectory and the DPO of Iscte, in particular, security breaches that could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2. This shall enable Iscte to:

a) Investigate the breach and take corrective measures, if necessary;

b) Keep a record of failures in compliance;

c) If necessary, notify the national data protection authority within the legally applicable time limit.

Q. RESPONSIBILITIES AND COMPETENCES

1. Each head of functional unit is responsible for ensuring that this Policy is complied with by the workers.

2. The workers should be familiar with this Policy and comply with its terms.

R. TRAINING

1. Iscte promotes training sessions on this Policy and about data protection matters in articulation with its DPO.

2. Additional training is ministered whenever there is a substantial change in the applicable legislation or in this Policy.

S. NON-COMPLIANCE

Non-compliance with this Policy may entail disciplinary consequences for the workers pursuant to the applicable labour legislation, or for students, pursuant to the Student Disciplinary Regulation, whenever the rules and provisions are blatantly breached and/or in a reiterated manner.

T. DEFINITIONS AND ABBREVIATIONS

The following concepts are used in this Policy:

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;
Personal Data 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Personal Data Protection	A fundamental right, protected not only by national legislation, but also by European legislation.
Sensitive Personal Data	For the purposes of this document, this includes special categories of personal data and *data of highly personal nature*. *Special categories of data*[10] are those that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. *Data of highly personal nature*[11] are those linked to private or family activities (such as electronic communications where its confidentiality should be protected) or that affect the exercise of a fundamental right (such as location data, the collection of which places in question the freedom of movement) or whose breach clearly implies that the daily life of the data subject will be severely affected (such as financial data that can be used for committing payment fraud).
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined

[10] GDPR, Article 9.
[11] 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 (EU) 2016/679, 2017, in https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

	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 Subject	Any identified or identifiable natural person whose personal data are held by Iscte.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, agrees to the processing of personal data relating to him or her;
Legitimate purpose	The purposes for which the personal data may be used by Iscte.
Adequacy Decision	Decision of the European relative to a state outside the European Economic Area which certifies that, via domestic legislation or by signing international agreements, the state meets the data processing criteria defined by the GDPR.

The following abbreviations or acronyms are used:

Workers	Any manager, teaching staff, researcher, employee, contributor working under a service arrangement.
GDPR	General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
GDPR Implementing Law	GDPR Implementing Law 58/2019 in the Portuguese legal system.
DPO	Iscte's Data Protection Officer
CNPD	Portuguese national data protection authority, *Comissão Nacional de Proteção de Dados*

Record of changes

Version number	Description of the change	Date of issue
01	Initial version, proposal of the Data Protection Officer.	22 October 2020
02	Revision of the proposal by the legal services and the Data Protection Officer.	3 February 2021
03	Revision of the proposal by the Vice-Rector for Information Systems and Quality and revision by the Office of Studies, Planning and Quality	17 November 2021
04	Revision of the proposal by the Data Protection Officer: Alteration of points J(1)(b), J(1)(e), of details, to clarify conditions of exercise of rights of the data subjects, and other alterations of details in G(5) and O(2)(ii).	22 November 2021
05	Approved by order of the Rector	9 December 2021