GUIDELINES FOR RESEARCHERS ON PERSONAL DATA PROTECTION IN SCIENTIFIC RESEARCH ACTIVITIES AT ISCTE – INSTITUTO UNIVERSITÁRIO DE LISBOA

Iscte-Instituto Universitário de Lisboa (hereinafter Iscte) is assigned with carrying out scientific research and study cycles, including masters and doctorates, in which scientific or historical research activities are pursued.

The processing of personal data for scientific research purposes is understood in a broad sense, covering, for example, technological development and demonstration, fundamental or applied research, historical research, research for genealogical purposes or research funded by the private sector.[1]

The researchers as well as the lecturers, employees, students, and collaborators involved in research activities of Iscte are duty-bound to comply with ethical standards concerning respect for the privacy of participants in research work and the legislation on data protection in force.

This document summarises Iscte's perspective on the legislation on data protection for scientific and historical research, in particular the framework arising from the General Data Protection Regulation (GDPR) and Law 59/2019 of 08/08 – Implementing Law, in the Portuguese legal system, of the GDPR.

The guidelines expressed in this document do not prejudice the scientific autonomy of the researchers, nor exempt the researchers from consulting the Data Protection Policy of Iscte, any other guidelines of the competent bodies of Iscte, applicable legislation and the Code of Ethical Conduct in Research of Iscte.

A. Data protection, research and the accountability principle 3

B. Am I using personal data? 4

B.1 The concept of personal data 4

B.2 Special categories of personal data 5

B.3 Data of a highly personal nature 5

B.4 Image, voice or video recording 5

C. Anonymisation or pseudonymisation? 6

C.1 Anonymisation 6

C.2 Pseudonymisation 7

[1] GDPR, recital 159.

D. Roles and responsibilities 7
D.1 Data controller 7
D.2 Who is charged with the obligation of ensuring the compliance of scientific research projects with the GDPR? 8
D.3 Who is charged with the obligation of ensuring the compliance of thesis and dissertation work with the GDPR? 8
D.4 Joint controllers 8
D.5 Data processors of Iscte 8
D.6 Iscte as a data processor 9
E. Technical and organisational measures 9
E.1 General measures 9
E.2 Additional measures for processing likely to result in a high risk (e.g., special categories of data) 10
F. Purpose of the processing, principles of data protection and the participant's right to be informed 11
F.1 Purpose of the processing, limitation of purposes, lawfulness and transparency 11
F.2 Participant Information Sheet (PIS) 11
G. Processing on the legal basis of the data subjects' consent 12
G.1 Expression of intent that is free, specific, informed, unambiguous or explicit 12
G.2 What if the processing purpose is not entirely known? 14
G.3 Consent of the data subjects *versus* consent of human participants in research 14
H. Processing on the legal basis of performance of a task carried out in the public interest or on pursuit of legitimate interests 15
H.1 Performance of a task carried out in the public interest 15
H.2 Pursuit of legitimate interests 15
H.3 What information should be provided to the participant? 16
H.4 Public interest in the processing of special categories of data 16
I. Storage periods 17
I.1 Maximum storage periods at Iscte 17
J. Rights of the data subjects 18
J.1 What are the rights of the data subjects and who should address in that regard? 18
J.2 Can data subject's requests for exercising their rights be denied? 18
J.3 Time limits for responding to data subjects' requests 19

K. Application of questionnaires to the Iscte community for scientific research purposes ... 19
L. Use of personal data of other sources ... 19
M. Transfers to countries outside the European Economic Area (EEA) and collection outside the EEA ... 20
M.1 Transfers to countries with an «adequacy decision» ... 21
M.2 Transfers to countries without an «adequacy decision» ... 21
N. Access to archives with personal data of deceased persons ... 21
O. Data protection impact assessment ... 22
O.1 When is it necessary to conduct an impact assessment? ... 22
O.2 Who is responsible for conducting the impact assessment? ... 25
P. Personal data breach ... 25
Q. Ethics Committee and Data Protection Officer ... 26
R. Useful documents and links ... 26
S. Definitions ... 28

A. DATA PROTECTION, RESEARCH AND THE ACCOUNTABILITY PRINCIPLE

Data protection plays a crucial ethical and legal role in scientific research.[2] This is closely linked to the right of the research data subjects to the protection of their private life, giving them control over the way that their personal information is collected and used.

Inadequate ethical conduct in data processing and/or non-compliance with the legislation may have devastating consequences for the data subjects and legal, reputational and financial consequences for Iscte and/or others responsible for the processing.

Two principles should be considered in compliance with the legislation on data protection in Portugal: the GDPR and the Implementing Law, in the Portuguese legal system, of the GDPR.[3] The GDPR is applicable throughout the entire European Economic Area and directly to Portugal as a member of the European Union (EU). The Implementing Law provides for a series of GDPR rules with particularities of enforcement in Portugal.

The GDPR regime for scientific research foresees some derogations relating to the obligations of those responsible for the processing, in particular in Article 89, conferring some flexibility in the application of various rules. This flexibility reflects the intention to adapt the data protection rules

[2] The right to data protection is enshrined in the European Charter of Fundamental Rights of the European Union (EU), in the Treaty on the Functioning of the EU and in Article 35 of the Constitution of the Portuguese Republic.
[3] Law 58/2019 of 8 August, published in *Diário da República* [Portuguese Official Gazette] number 151/2019, Series I, of 08/08/2019.

to the specific interests and public interest of scientific research, but with the consequential greater weight and relevance of the *accountability principle*.

The *accountability principle*[4] reflects the emphasis on self-regulation, assigning those responsible for the processing with the duty of ensuring and being able to demonstrate compliance with the principles of data protection, assessment of the risks to the rights and freedoms of the data subjects, and implementing appropriate technical and organisational safeguards for that protection. The higher the risk to the data subjects, the higher the level of protection should be, and likewise the obligations and the safeguards to be implemented.

In Portugal, the derogations suggested in Article 89 of the GDPR are regulated by the GDPR Implementing Law. The GDPR and the Implementing Law are both indispensable references to be consulted by the researchers, with which researchers should be familiar, in addition to other more specific regulatory frameworks where applicable to research projects, such as the processing of personal data related to criminal convictions and offences, the processing of genetic information, the protection of personal data in the electronic communications sector, video surveillance, among others. A compilation of the legislation can be consulted on the website of the Comissão Nacional de Proteção de Dados (CNPD) [Portuguese National Data Protection Authority].

B. AM I USING PERSONAL DATA?

B.1 The concept of personal data

The GDPR and the Implementing Law are applicable to any research project that uses personal data.

Personal data is defined as any information, of any nature and in any medium (e.g., voice recording or image), relative to an identified or identifiable natural person ('data subject'). A identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an indicator, such as a name, an identification number, location data, an online identifier (e.g., IP) or to one or more specific elements of the physical, physiological, genetic, mental, economic, cultural, social identity of that natural person.

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

The fact that a study does not report individualised answers of participants is not, in itself, an indicator that there is no personal data processing. It may be considered that a study never processes personal data only on the condition that the researcher does not have access to any medium with personal data records during collection and subsequent processing. Whenever a researcher has access to data that contain information related to a person that has been or could be identified directly or indirectly by reference to identifiers, these data should be processed as personal information up to the time of their anonymisation or destruction. The process of

[4] GDPR, Article 5(2).

anonymisation converts personal data into anonymous data (see section C). If the anonymisation occurs at a stage after data collection, for example, when the personal identification information is removed from an audio transcription of an interview, or when the collected data are copied to another database and anonymized, the raw data are still personal, and all the study data should be processed as personal up to the point when the raw data are deleted or are also anonymised.

B.2 Special categories of personal data

The GDPR acknowledges the existence of personal data that are sensitive, as their processing is likely to result in higher risks for the data subjects. The regulation identifies *special categories of personal data* as those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.[5]

The processing of special categories of data is not prohibited if there is *explicit* consent[6] of the data subject.

It is also not prohibited for scientific or historical research, on the basis of European or Portuguese legislation that establishes appropriate and specific measures for the protection of the fundamental rights and interests of the data subject, and provided that the actual processing complies with the safeguards listed in Article 89(1) of the GDPR, relative to processing for scientific research.[7]

B.3 Data of a highly personal nature

Although not categorised as special personal data, some personal data are considered as being of a *highly personal nature*[8], whose processing is likely to result in higher risks for the data subjects. These personal data are considered as sensitive because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud).

B.4 Image, voice or video recording

The physical portrait of a person (photograph or other) and voice or video recording are personal data, and as such are subject to the rules on data protection.[9]

---

[5] GDPR, Article 9.
[6] The explicit requirement is described in section G.1.
[7] GDPR, Article 9(2)(j).
[8] Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (AIPD) and that determine whether the processing is «likely to result in a high risk», for purposes of Regulation (EU) 2016/679, 2017 in https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.
[9] The portrait of a person is also protected by image rights, and cannot be exposed without the consent of the persons concerned. However, in this context, the consent of the portrayed person is not required when, among other situations, this is justified by their public visibility, the position held, scientific purposes, when the reproduction of the image is framed in public places, or in facts of public interest or that have taken place publicly, pursuant to Article 79 of the Civil Code.

It should be noted that the mere assumption from a physical portray of features that could possibly be categorised as special data (e.g., ethnicity based on colour), does not imply the processing of special categories of data. However, if information is processed based on these assumptions, this can be considered as the processing of special categories of data. For example, the processing of photographs by technical means that enable the unambiguous identification or the authentication of a natural person, corresponds to the processing of biometric data and, consequently, the processing of special categories of data.

C. ANONYMISATION OR PSEUDONYMISATION?

C.1 Anonymisation

One way to attenuate the ethical and legal risks of the use of personal data is to anonymise them so that they cannot be related to identifiable persons.[10] Whenever the data processing purposes in scientific or historical research can be attained with datasets that do not permit, or no longer permit, the identification of the data subjects, the purposes should be achieved in this manner. *Anonymisation* is defined as the techniques for conversion of personal data into anonymous data, such as suppression of attributes, encoding, the generalisation or introduction of noise.

Data that are not related to identifiable persons, such as aggregated and statistical data, or data that has been anonymised in any other form, are not, in principle, personal data and are outside the scope of the GDPR. However, this is only valid when the researcher only has access to anonymised data, and/or if the collection process ensures anonymity right from the start. If the researcher collects personal data and subsequently creates a series of anonymised data based on the first data, the new data may still be considered personal data if the researcher has access to the initial raw data. Thus, for example, the creation of a dataset as a result of information collected from participants through interviews, even if the personal identification information is subsequently removed, may not be amount to anonymisation until the raw data are destroyed or also anonymised.

It is interesting to note that anonymisation is a challenging area in view of the potential *re-identification*. Re-identification is defined as the process of transforming anonymised data back into personal data by data matching or similar techniques. A growing number of studies show that it is possible to identify individuals based on anonymous datasets, for example, through matching techniques in big data, revealing limitations of the anonymisation techniques in protecting the privacy of individuals. It is difficult to assess the risk of re-identification with absolute certainty. In case of doubt, or if there is a significant likelihood of re-identification of the individuals whose data were collected, the research should treat the data as personal.

The Article 29 Data Protection Working Party, appointed by the European Parliament and European Council, provides a set of best practices, techniques, risks and common errors in applying anonymisation techniques.[11]

[10] GDPR, Article 89.
[11] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

C.2 Pseudonymisation

Anonymisation is always preferable to pseudonymisation. However, in some projects it is necessary to maintain a link between the research subjects and their personal data. In that case, data processing should be subject to safeguards, in order to protect the privacy of the data subjects and minimise risks of accidental or unauthorised access, including the adoption of technical and organisational measures, such as pseudonymisation.

Anonymisation and pseudonymisation are not the same. The GDPR defines pseudonymisation as 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.[12] In other words, pseudonymisation does not remove the personal nature of the data: it reduces the link of a dataset to the original, identifying information of data subjects. For example, by creating a copy of the dataset, but where the personal identifying information (e.g., the name of a person) has been replaced by encoded identifiers, with the subsequent processing of a new dataset that, in itself and without the decryption key, does not permit the identification of the data subjects.

The Article 29 Data Protection Working Party, appointed by the European Parliament European Council, provides a document referred to above with a set of best practices, techniques, risks and common errors in the application of pseudonymisation techniques.[13]

D. ROLES AND RESPONSIBILITIES

D.1 Iscte as the data controller[14]

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

Iscte is the data controller of the research projects based at Iscte, irrespective of whether the data processing takes place within or outside Portugal or the European Economic Area, whether the processing is carried out by third parties or not, within or outside Iscte's premises, and in equipment belonging or not to Iscte.

Iscte is also the data controller of any work involving personal data in the context of the courses it ministers, such as master's dissertations or doctoral theses.

The accountability principle enshrined in the GDPR requires that Iscte, as the data controller, should document the compliance of the specific means of personal data processing used with the principles and rules contained in the GDPR, and has the duty to demonstrate this.

[12] GDPR, Article 4(5).
[13] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360
[14] In Portuguese, the data controller is referred to as the *Responsável pelo Tratamento*.

D.2 Who is charged with the obligation of ensuring the compliance of research projects with the GDPR?

In the case of research projects, the coordinator at Iscte is charged with ensuring that the project is implemented in accordance with the guidelines in force at Iscte and the legislation on personal data protection.

D.3 Who is charged with the obligation of ensuring the compliance of thesis and dissertation work with the GDPR?

In the case of supervision of academic work, such as in curricular units, master's dissertations and doctoral theses, the supervisor(s) is(are), in collaboration with the student, charged with ensuring that the work is carried out in accordance with the guidelines in force at Iscte and the legislation on personal data protection.

D.4 Joint data controllers

When other natural or legal persons determine, together with Iscte, the purposes and means of processing, they are *joint controllers*.[15]

Therefore, if Iscte and another institution are partners in a research project, it is possible for both to be joint controllers of the processing. In that situation, an agreement should be reached between the parties that lays down, in a transparent manner, their respective responsibilities in the project for the compliance of the data processing with the legislation. To this end, it is suggested that the project leaders contact the Research Support Office (GAI).

D.5 Data processors of Iscte

The term *data processor*[16] refers to the natural or legal person, public authority, agency or other body that processes personal data on behalf of the data controller.

The relationship between the controller and a processor must be regulated by a contract. Therefore, when personal data held by an Iscte's research project are transferred for processing by an outsourced service, this transfer must be regulated by a contract, that binds the subcontractor (as the data processor) to Iscte (as the data controller), and establishes the processing conditions.[17] To this end, it is suggested that the project leaders contact the Research Support Office (GAI).

It should be noted that the transfer of personal data to a third party, for example, to a research project at another institution, does not always imply an outsourcing relationship. It may be the case that the data controller, under certain circumstances, transfers data to another entity, without charging that entity with the processing of the data on behalf of the controller. The entity thus becomes, separately or jointly with Iscte, the controller of the data it has received. For example, under the *secondary use* of data for scientific research purposes, data transfers between research projects at the same or in different institutions, provided that appropriate safeguards are ensured (see section L - Use of personal data of other sources, and section D.4 above - Joint data controllers).

[15] GDPR, Article 26.
[16] In Portuguese, the data processor is referred to as the *subcontratante*.
[17] GDPR, Article 28.

D.6 Iscte as a data processor

When Iscte processes personal data on behalf of a third party, that third party acts as the data controller, and Iscte as the processor. In this case, Iscte does not determine the purpose and means of processing, but the data protection obligations arising from the GDPR and Implementing Law continue applicable, such as the use of technical and organisational measures to ensure compliance with the legislation and ensure the protection of the rights of the data subjects.

E. TECHNICAL AND ORGANISATIONAL MEASURES

The *principle of integrity and confidentiality* implies that the data controllers must guarantee that the data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[18] The measures to be implemented should ensure a security level that is suitable to the identified risks.

The scientific research undertaken at Iscte should include at least the following, among others.[19]

E.1 General measures

a) Minimise the data: The *principle of minimisation* implies that the data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[20] The minimum personal data required for the purpose of the processing should be used; therefore, no more than the necessary data should be processed.
b) Use only anonymised data, if it is possible to achieve the project's goals in that manner.
c) Use pseudonymised personal data, whenever possible, if it is not possible to use anonymised data.
d) Encrypt your research data and/or the devices on which they are stored, and ensure that keys/passwords are adequately protected. This is a mandatory measure of general nature, and crucial in the case of special categories of data or any type of personal data stored in laptop computers or removable devices (e.g., pens, external drives, etc.).
e) Ensure that you are working in a system access session that is duly protected and authenticated with personal credentials, and do not reveal to anyone your personal passwords. Do not leave the workplace without closing the session, preventing possible undue access by third parties.
f) Ensure that computers with personal data have all the security updates, that they are protected against harmful software (such as virus or other malicious software), that the firewalls are active and that the browsers are executed with secure configurations.
g) Do not store personal data in cloud storage services, except those with a contractual agreement with Iscte. If the researcher decides to use cloud services that do not have a contract with Iscte, the personal data therein should be encrypted using robust encryption methods, using symmetric or asymmetric encryption. Furthermore, the researcher is responsible for checking the compliance of the storage service with the data protection principles.

[18] GDPR, Article 5(1)(f).
[19] A checklist of measures can be consulted in the European Commission document "Ethics and Data Protection", 2018, https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf.
[20] GDPR, Article 5(1)(c).

h) Do not replicate personal data files in various devices (pens, portable computers, personal computers), except to the extent strictly necessary and for the time that is strictly necessary and/or exclusively to ensure backups.
i) When personal data are deleted, make sure that the recycling bin or equivalent is emptied after deleting them, and make sure that all copies are deleted from all the devices.
j) Avoid storing data in non-institutional computers.[21] When this is not possible, i.e., when the researchers store data on their own computers, make sure that the personal data for which Iscte is the data controller are processed with software licensed for use at Iscte. When this is not the case, the researcher is responsible for checking the compliance of the software with the data protection principles.
k) Do not send personal data files by unprotected e-mail, and instead, use a protected sharing method. Note that sending emails and attachments creates copies on both the sender's and recipient's e-mail servers and applications.
l) Use or implement appropriate information security policies and protocols. In particular, you should not: send datasets with personal data by e-mail; collect personal data or communicate with data subjects through platforms (e.g., social networks) without ascertaining the implications concerning data protection; expose personal data to unauthorised access, such as using remote access through open wireless networks, etc.
m) Ensure that the project team members with access to personal data are subject to duties of confidentiality and accountability, certified by a written document (clauses in an employment contract or, in the case of students, accountability and confidentiality agreements).

E.2 Additional measures for processing likely to result in a high risk (e.g., special categories of data)

n) If the personal data processing involves at least one of the criteria likely to result in high risk, listed in section O.1[22], for example, processing of special categories of data or large scale data processing, the following additional measures should be taken:

- Raw, non-pseudonymised data should not be stored in personal computers. If necessary, the data collection can take place with the assistance of personal computers, and as soon as possible deleted from the personal computer and transferred to institutional servers or services of Iscte or institutional computers disconnected from the network, where they should remain with restricted access.
- Whenever possible, implement rules of access and records of access (logs) to the data.

[21] Institutional computers are acquired by Iscte with its own funds. Computers are non-institutional when acquired by the actual user, although they may also be used as work computers.
[22] Namely, the criteria listed in the document of the Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (AIPD) and that determine whether the processing is «likely to result in a high risk» for purposes of Regulation (EU) 2016/679, https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

F. PURPOSE OF THE PROCESSING, PRINCIPLES OF DATA PROTECTION AND THE PARTICIPANT'S RIGHT TO BE INFORMED

F.1 Purpose of the processing, limitation of purposes, lawfulness and transparency

Data processing is always conducted for one or more purposes and is subject to certain principles[23], including the *principles of lawfulness, fairness, transparency* and *purpose limitation*.

The *purpose of the processing* means the purposes for which the personal data may be used. The *principle of purpose limitation* implies that the data are collected for specific, explicit and legitimate purposes, and cannot be processed subsequently in a manner incompatible with those purposes. However, scientific research has a differentiated status, where further processing for research purposes (secondary use of data) is not incompatible provided that appropriate measures are taken (see section L - Use of personal data of other sources).

In order to be *lawful*, the processing must be carried out on the basis of one or more *legal bases* of Article 6 of the GDPR and/or, in the case special categories of data, on the basis of one of the grounds established in Article 9(2).

The *principles of fairness and transparency* require the researchers to comply with the obligation of providing the research participants with information about the purpose of the data processing, the legal basis for the processing, what will happen to the data and the risks involved. The information should be provided in an intelligible manner, in clear and simple language.

F.2 Participant Information Sheet (PIS)

One way of providing information to the research participants could be through a Participant Information Sheet (PIS) or, when the legal basis for the data processing is the data subject's consent, by incorporating that information in an informed consent.

When the personal data are collected from the data subject, the information to be provided must mandatorily include:[24]

- The information that Iscte is the data controller (identify other controllers if there are joint controllers);
- The name of the researcher or person responsible for the study at Iscte;
- The purpose of the processing;
- The legal grounds for the processing (e.g., consent of the data subject, performance of a task carried out in the public interest, legitimate interests or other legal basis of Articles 6 or 9 of the GDPR);
- The rights that the data subject participant may exercise, and the contacts details of the researcher or person responsible to be addressed; as well as the right to submit a complaint to the National Data Protection Authority (CNPD);
- If the legal basis is the data subjects' consent, the the right to withdraw consent at any time, and the information that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;

[23] GDPR, Article 5.
[24] GDPR, Articles 13 and 14.

- The period of retention of personal data, after which the data are destroyed or anonymised;
- Information as to whether the data are transferred to third parties and for what purposes, for example, to data processors (persons or entities that process personal data on behalf of Iscte), other research teams or any other entities authorised to process personal data;
- If the data is transferred to a third country or international organisation outside the European Economic Area, the existence or absence of an «adequacy decision»[25] by the European Commission, and other required information on the transfers pursuant to Article13(1)(f) of the GDPR;
- If the data processing involves potential risk to the participants' rights and freedoms, the importance and foreseen consequences of this processing for the participants;
- If there are automated decision making[26], including profiling referred to in Article 22(1) and (4) of the GDPR, meaningful information concerning the underlying logic, as well as the significance and envisaged consequences of such processing for the participant;
- Contact details of the Data Protection Officer of Iscte.

The information may also include a description of the safeguards endorsed, including the technical and organisational measures taken by the researcher, such as:

- Whether the personal data are pseudonymised or anonymised at any stage of the research;
- The information that all the researchers with access to the personal data are bound to the duty of secrecy and confidentiality.

If the processing conditions change during the project, it is necessary to inform the participants.

G. PROCESSING ON THE LEGAL BASIS OF THE DATA SUBJECTS' CONSENT

G.1Expression of intent that is free, specific, informed, unambiguous or explicit

In most cases, for scientific research purposes, the legal basis for the personal data processing is consent.

The *data subjects' consent* is given based on the Participant Information Sheet (PIS), and refers to the expression of intent by which the data subject participants accept that their personal data in be subject to processing.[27] This should take the form of a written statement, and may be collected by electronic means, for example:

[25] See section M - Transfers to countries outside the European Economic Area (EEA) and collection outside the EEA.

[26] Automated individual decision-making occurs when decisions are taken about a natural person by technological means and without human involvement. This may be carried out without profiling. For example, if the decision of a bank to grant a bank loan to a natural person is taken by an algorithm, without human intervention. If a person controls the final decision supplied by the algorithm, with effective power or ability to influence the final result, the decision may be considered not "exclusively" automated.

[27] GDPR, Article 6(1)(a); Article 7; and Article 9(2)(a). Also, see the guidelines related to consent in observance of Regulation (EU) 2016/679, Article 29 Data Protection Working Party, https://www.cnpd.pt/home/rgpd/docs/wp259rev0.1_PT.pdf.

(1) I consent to the use of my personal data under the research project *[identify the research project]* in accordance with the purpose and all other information provided to me in the Participant Information Sheet.
Yes ☐ No ☐

The data can only be processed (including collection) after the participants have been given the PIS and positively expressed their consent. Their expression of intent must be *free, specific*, *informed and unambiguous*. In certain cases, it should not only be unambiguous but *explicit*:

i) the *free* requirement means that there is real choice and control for the data subjects. If the participant cannot exercise a real choice, if there is an imbalanced relationship with the data controller (e.g., a relationship between employee and employer, between lecturer and student), if the participant feels coerced to give consent, or suffers negative consequences by not consenting, then the consent is not valid.

ii) the unambiguous requirement means that the consent is accomplished by a statement or clear affirmative action in which the participant agrees to the processing of personal data relating to him or her; Silence, pre-validated options or omissions are not acceptable methods in consent.

iii) The *explicit* requirement reinforces the unambiguous nature of the consent. It is mandatory in the case of the processing of special categories of data, as well as in the case of international transfers to countries without an «adequacy decision» when outside the European Economic Area.[28] To be explicit, the data subject must *expressly* manifest consent, for example through a written statement and the signature of the data subject or, in the digital context, by completing an electronic form, followed by the sending of an e-mail message for uploading the scanned document with the data subject's handwritten or electronic signature.[29]

iv) the *specific* requirement implies that the data subject's consent should be given in relation to one or more specific purposes, and that the data subject has a choice in relation to each one of them. Consent can cover different operations, provided that these operations serve the same purpose. The data subjects shall give their consent knowing that they have control over their data and that those data shall only be processed for the specified purposes. If the controller processes the data based on consent and later intends to process the data for other purposes, the controller should endeavour to obtain another consent for the new purpose unless there is another legal basis for that processing which better reflects the situation.

It is not always possible to comply with the requirements for the data subject's consent. For example, if the data subjects are students at Iscte, their *free* consent may be questioned. In the event of difficulty in meeting the requirements, it is suggested that the researcher assess an alternative possibility, instead, invoking the legal basis of a task carried out in the public interest or pursuit of legitimate interests. Nevertheless, this does not preclude obtaining, in the ethical sphere, an *informed consent of research participants*. The differences between this consent and the data subject's consent in the legal sphere of data protection are explained below.

[28] On the meaning of *adequacy decisions*, see section M - Transfers to countries outside the European Economic Area (EEA) and collection outside the EEA.
[29] Section 4 of the Guidelines of the 29 Data Protection Working Party relative to consent in observance of Regulation (EU) 2016/679 of 28 November 2018, provides various examples of explicit consent.

G.2 What if the processing purpose is not entirely known?

In some research projects, it may not be possible to fully identify the processing purpose at the time of data collection. In such cases, the data subject's consent may be prepared for a more broader purpose, for various research areas or be given solely for certain specific research domains or projects.[30] This possibility should be used with moderation, where the ethical standards acknowledged by the scientific community should be respected.

The lesser specificity of the purpose can be offset by regularly providing the participants with information on the evolution of that purpose, as the research project progresses, so that, over time, the consent can be more specific. The participants should be able to understand the project situation in basic terms, in order to assess whether they intend to exercise their rights, for example, the right to withdraw consent pursuant to Article 7(3) of the GDPR.[31]

G.3 Consent of the data subjects *versus* consent of human participants in research

The *consent of the personal data subjects* should be distinguished from the *informed consent* of human participants in research, such as, for example, the consent provided pursuant to Iscte's Code of Ethical Conduct in Research.

The former refers to consent for personal data processing in the sphere of personal data protection enshrined in the GDPR and Implementing Law, the latter to the consent of the research subject to participate in the project, in the sphere of ethics and good practices in scientific research, enshrined in Iscte's Code of Ethical Conduct in Research.

Thus, a project that does not process personal data (e.g., collected from participants through digital means that ensure anonymity) does not require a PIS under the terms listed above nor a consent from data subjects, but cannot, in the ethical sphere, be exempt from providing information or some type of consent under the terms of Iscte's Code of Ethical Conduct in Research. The latter does not refer to the processing of personal data, but only to participation in the project and/or any other circumstances of the project in the ethical sphere.

When a project processes personal data on legal grounds other than the data subjects' consent, it remains legally required to provide the PIS. As an additional safeguard, to protect the rights and freedoms of the data subject, it is advisable, in the ethical sphere, to provide to the participants an informed consent pursuant to Iscte's Code of Ethical Conduct in Research. The latter should not be expressed in relation to the processing of personal data, but only to participation in the project and/or any other circumstances of the project in the ethical sphere.

Finally, a project processing personal data that chooses the legal basis of the data subject's consent in not exempt, in the ethical sphere, from requirements of providing additional information to the participant or from obtaining consent pursuant to Iscte's Code of Ethical Conduct in Research. In that case, the researcher may decide to merge the two consents into a single consent, which should be explicit in relation to the personal data processing.

[30] GDPR Implementing Law, Article 31(4).
[31] See the guidelines of the Article 29 Data Protection Working Party on consent, in section 7.2 relative to scientific research, pp. 33, https://www.cnpd.pt/home/rgpd/docs/wp259rev0.1_PT.pdf.

The relationship between the two consents may be summarised as follows:

1. A project that does not process personal data (e.g., collected from participants by digital means that ensure anonymity):

Legal sphere of data protection: Does not require the PIS, nor the data subjects' consent.

Ethical sphere: May require the provision of information or some type of informed consent pursuant to Iscte's Code of Ethical Conduct in Research.

2. A project that processes personal data on legal grounds other than the data subjects' consent, e.g., legitimate interests:

Legal sphere of data protection: The PIS is mandatory; the data subjects' consent is neither mandatory nor should be used.

Ethical sphere: An informed consent pursuant to Iscte's Code of Ethical Conduct in Research may be used as an additional safeguard or be required due to the specific circumstances of the project. This should not refer to the processing of personal data, but only to participation in the project and/or other circumstances of the project, in the ethical sphere.

3. A project that processes personal data on the legal basis of the data subjects' consent:

Legal sphere of data protection: The PIS and the data subject's consent is mandatory.

Legal and ethical sphere: The project is not exempt, in the ethical sphere, from providing additional requirements to the participant and obtaining consent pursuant to Iscte's Code of Ethical Conduct in Research. In that case, the researcher may decide to merge the two consents into a single consent, which should be explicit in relation to the personal data processing.

H. PROCESSING ON OTHER LEGAL GROUNDS

H.1 Performance of a task carried out in the public interest

The *performance of a task carried out in the public interest* may constitute a legal basis for data processing. This basis may be advantageous over the data subject's consent, such as when in it turns out that the consent would not meet the requirement of being *free*. However, this is only possible based on national or EU law and requires evidence that the purposes of the research are of public interest.[32]

H.2 Pursuit of legitimate interests

In cases in which the research is necessary for the purposes of *legitimate interests* pursued by Iscte or third parties, this legal basis may be considered, taking into account the reasonable expectations of the data subjects based on their relationship with Iscte, and provided that the

[32] GDPR, Article 6(e). The case of projects reviewed by panels and funded by public agencies could be an indicator of its public interest. But in any case, the rationale for the necessity of processing for performing a task carried out in the public interest would require having been laid down by some law. See the Preliminary Opinion on data protection and scientific research, European Data Protection Supervisor, January 2020. https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en.

interests, fundamental rights and freedoms of the data subjects do not prevail over the interests of the data controller. The existence of legitimate interest requires the careful assessment of the question of knowing whether the data subject could reasonably foresee, at the time and in the context in which the personal data are collected, that these data could be processed for that purpose.

In other words, the legal basis of legitimate interest enables the processing subject to the application of a weighing and balancing test that considers the legitimate interests of the data controller – or the third party to whom/which the data is conveyed – in relation to the interests, rights and freedoms of the persons in question.

There may be a legitimate interest, for example, where a relevant and appropriate relationship exists between the data subject and Iscte as the data controller, such as the relationship with a student, a faculty or an employee. The processing of personal data of Iscte students aimed at investigating ways to improve teaching and learning processes, provided that it is authorised by a superior, could be a case of a legitimate interest of the institution. The processing of data strictly necessary for the purposes of fraud prevention and control constitutes a legitimate interest acknowledged by the GDPR.[33]

H.3 What information should be provided to the participant?

It should be noted that for both legal bases, the performance of a task carried out in the public interest and the pursuit of legitimate interests:

1. The duty to inform the participant remains, for example, by providing the PIS containing the legal basis for the data processing and all the other information referred to in section F.2 - Participant Information Sheet (PIS).
2. As additional safeguards, it is recommended, whenever possible, that an informed consent of participation of humans in research should be obtained, e.g., pursuant to Iscte's Code of Ethical Conduct in Research. This refers to the consent to participate in the project and not to the processing of personal data, because the legal basis for the data processing shall be another.

If the researcher considers that the project purpose falls within the performance of a task carried out in the public interest or under legitimate interests, and could benefit from the application of one of those legal bases for processing personal data, it is suggested that the researcher, before doing any processing, ask for confirmation and guidelines from the Research Support Office (GAI) and the Data Protection Team of Iscte.

H.4 Public interest in the processing of special categories of data

Special categories of data can also be processed on the basis of the following legal bases of public interest, among others: i) public interest in the field of public health, based on the European or Portuguese law which proved for suitable and specific measures to safeguard the rights and freedoms of the data subjects, in particular professional secrecy[34]; ii) provided that the processing complies with Article 89(1) of the GDPR, for scientific or historical research purposes, based on

[33] GDPR, Recital 47.
[34] GDPR, Article 9(i).

European or Portuguese law, that should be proportionate to the aim pursued, respect the essence of the right to personal data protection and foresee appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.[35]

I. STORAGE PERIODS

Pursuant to the principle of *storage limitation,* the personal data should 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.[36]

The storage period is that established by legal or regulatory provisions, or in their absence, as revealed necessary for pursuit of the purpose. When the purpose that motivated the processing ceases, the data controller must proceed to destroying or anonymising the data.[37]

However, for the purpose of scientific or historical research, if it is not possible to determine in advance the time when the personal data are no longer necessary, it is lawful to keep the data for a longer period, provided that appropriate technical and organisational measures are taken to ensure the rights of the data subjects, in particular the provision of information on their storage.[38]

I.1 Maximum storage periods at Iscte

The following maximum storage periods have been endorsed at Iscte for scientific research purposes:

a) Master's Dissertations - 6 months after the defence of the master's dissertation;

b) Doctoral Theses – 12 months after the defence of the doctoral thesis;

c) Projects funded by the FCT – 10 years after the project completion period (implementation);

d) Projects funded by other financing sources (including European) – 10 years after the project completion period.

Whenever justified by the need to extend these periods, or the possibility of reusing the personal data for other scientific research purposes (secondary use of data, see section L - Use of personal data of other sources), the periods may be extended. This extension requires approval by a superior, which should be requested from the Research Support Office (GAI).

At the time of the data's destruction, and in particular when storage service providers are used, it is important to check that the data has been entirely eliminated in a secure manner, together with any backups. If the data were shared with third parties, it must be ensured that they were also destroyed, unless there are legal grounds to keep them.

[35] GDPR, Article 9(j).
[36] GDPR, Article 5(e).
[37] Implementing Law, Article 21(4).
[38] Implementing Law, Article 21(2).

J. RIGHTS OF THE DATA SUBJECTS

J.1 What are the rights of the data subjects and who should address in that regard?

The optional nature of participation in a study is a fundamental ethical requirement of scientific research. Scientific advance largely depends on the willingness, voluntarism and good-will of the participants to be part of the studies, under the assumption that they are contributing to scientific progress and the public interest. When personal data are processed in a study, the timely response to requests for the exercise of rights of the data subjects is a fundamental condition for the protection of their rights, freedoms and guarantees, and, at the same time, is a fundamental condition for the actual operation of scientific research.

The Participant Information Sheet (PIS) must specify the form and contacts details of the researcher to whom requests for the exercise of rights may be addressed.

In addition to the data subject's right to be informed, other rights include the right of access to the data (Article 15 of the GDPR), the right to rectification (Article 16), the right to erasure (Article 17), right to restriction of processing (Article 18) and the right to portability (Article 20).

If the legal basis for the processing is the pursuit of legitimate interests, the data subject has the right to object to the processing (Article 21 of the GDPR), including object to profiling.

The data subject also has the right to object whenever the personal data are processed for scientific or historical research purposes, pursuant to Article 89(1), for motives related to his/her particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.[39] If the legal basis is consent, the data subject has the right to withdraw his/her consent at any time, although this does not affect the lawfulness of the processing before its withdrawal.[40]

J.2 Can data subject's requests be denied?

As the personal data are being processed for scientific or historical research purposes, the GDPR establishes the possibility of the non-applicability of the right to erasure, inclusively after the withdrawal of consent, if that right is likely to render impossible or seriously impair the achievement of the objectives of that processing.[41]

The GDPR Implementing Law also foresees that the rights of access, rectification, restriction of processing and object may be impaired, to the extent necessary, if those rights are likely to render impossible or seriously impair the achievement of the objectives of the processing.[42]

The rejection of requests related to the exercise of rights is a last resort solution that should be approached with extreme caution. If the researcher considers that it is not necessary to comply with a data subject's request for exercise of rights, it is mandatory to request permission for such, by submitting, at the Research Support Office (GAI), the data subject's request with a substantiated explanation of the reasons for which the researcher believes it should not be

[39] GDPR, Article 21(6).
[40] GDPR, Article 4(3).
[41] GDPR, Article 17(3)(d).
[42] Implementing Law, Article 31(2).

complied with, where it may also be necessary to attach the opinion of the Ethics Committee and/or the Data Protection Officer.

J.3 Time limits for responding to data subjects' requests

Following a data subject's request to exercise his/her rights, the GDPR determines that the information on the actions taken should be provided without unjustified delay. Although the established maximum time limits are longer[43], a maximum time limit of twenty consecutive days, counted from the date of receiving the request, is recommended, except in cases in which the complexity or number of requests justify longer time limits.

K. APPLICATION OF QUESTIONNAIRES TO THE ISCTE COMMUNITY FOR RESEARCH PURPOSES

The Iscte community may represent a relevant and useful universe for application of scientific surveys. Iscte's data protection policy establishes the possibility of distributing questionnaires via e-mail lists, that can be accomplished on different legal grounds. The criteria for distributing questionnaires to the student population are defined in the policy on application of questionnaires to the student population.

L. USE OF PERSONAL DATA OF OTHER SOURCES

Under appropriate conditions, it is possible to process personal data not obtained directly from the data subjects, such as data collected by third parties, including data collected by other Iscte's projects or provided by other institutions (secondary use of data).

It is necessary to confirm that there is permission from the person/entity responsible for the original dataset, and the processing should be subject to appropriate safeguards, ensuring the technical and organisational measures of Article 89(1) of the GDPR, consistent with the processing for scientific research, including, e.g., pseudonymisation or anonymisation.

The transfer of personal data from other institutions to an Iscte's project will normally require a joint controller agreement (see section D.4 - Joint data controllers).

Another situation is when a project at Iscte makes use of personal data provided by other Iscte sources or projects. This requires an analysis of the *compatibility* between the original purpose and the new purpose of the processing. If the new purpose is compatible, the processing does not require a new legal basis for the additional processing. Scientific research has a special status, as further processing is not considered incompatible with the initial purposes.[44] However, if the data from other sources have been collected based on consent of the data subject, the reuse of those data does not exempt new consent.

Irrespective of the origin of the data or the legal basis for processing, it is still necessary to provide the participants with a PIS, permitting the possible opt-out. The PIS should also add the following

[43] GDPR, Article 11(3).
[44] GDPR, Article 5(b).

information: from which source the personal data originate, the categories of personal data concerned, and if applicable, whether it came from publicly accessible sources.[45]

There are two exceptions to the duty of informing the data subject participants:

1) If the participants already have that information.

2) If it is demonstrated that it is impossible to provide the information to the participants, or that the effort involved would be disproportionate.[46] That possibility is considered subject to appropriate conditions and safeguards[47], and to the extent that the duty of providing information is likely to render impossible or seriously impair the achievement of the objectives of that processing.

In determining what constitutes impossibility or what would involve a disproportionate effort, Recital 62 of the GDPR refers to the number of data subjects, the age of the data and the appropriate safeguards in place as possible indicative factors. To this end, it is recommended that the project coordinator prepares, document and submit to Iscte's Data Protection Team an assessment of the effort involved in providing the information to the data subjects versus the impact and effects if they do not receive the information.

Where it is deemed not possible to ensure the data subject's right to be informed, appropriate safeguards should be adopted to protect the rights, freedoms and legitimate interests of the data subject, including through the disclosure of the information to the public, for example, through the project website. Cumulatively, if the processing involves special categories of data, data related to criminal convictions and offences or data of a highly personal nature, Regulation 1/2018 of the Portuguese National Data Protection Authority (CNPD) requires a data protection impact assessment to be carried out.[48]

M. TRANSFERS TO COUNTRIES OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA) AND COLLECTION OUTSIDE THE EEA

The GDPR is applicable to data controllers established in the European Economic Area (EEA), irrespective of whether the personal data processing occurs within or outside the EEA.

Data processing outside the EEA can imply further risks for the data subjects, if the legal system of the country does not offer a protection level equivalent to the GDPR. Consequently, the GDPR establishes specific provisions to transfer or process personal data outside the EEA. If an Iscte project transfers personal data outside the EEA, or collects and processes data outside the EEA, the project coordination should ensure and be able to demonstrate the compliance of that transfer with the GDPR.

Likewise, if a partner of a project or data processor established outside the EEA accesses personal data stored by Iscte, this is equivalent to a transfer outside the EEA, in which case the project

[45] GDPR, Article 14.
[46] GDPR, Article 14(5).
[47] Namely, the conditions and safeguards established in Article 89(1) of the GDPR.
[48] Regulation 798/2018, Diário da República number 231/2018, Series II of 2018-11-30: CNDP Regulation 1/2018 related to the list of personal data processing subject to Data Protection Impact Assessment, https://dre.pt/home/-/dre/117182365/details/maximized.

coordination should ensure and be able to demonstrate that the transfer is compliant with the GDPR.

M.1 Transfers to countries with an «adequacy decision»

In certain cases, a third country outside the EEA may be considered to offer an adequate level of protection by decision of the European Commission («adequacy decision»), meaning that it is possible to transfer data to an institution located in the third country without the data exporter having to provide additional safeguards and without being subject to additional conditions. In other words, transfers to an «adequate» third country will be similar to data transfers inside the EEA.[49] However, this does not waive the requirement that data subjects must be informed in advance of that transfer in the Participant Information Sheet.

The list of countries with adequacy decisions can be consulted on the pages of the European Commission.[50]

M.2 Transfers to countries without an «adequacy decision»

In the absence of an adequacy decision, the GDPR stipulates a number of legal instruments to ensure appropriate safeguards, on the condition that the data subjects benefit from enforceable rights and effective corrective measures.[51]

Nevertheless, in scientific research, the most expeditious and usual form of international transfers to countries without an adequacy decision is via *explicit* consent of the data subjects, after having been informed of the possible risks of such transfers to themselves due to the absence of an adequacy decision and appropriate safeguards.[52] To be explicit, the data subject must *expressly* manifest consent (on the explicit requirement, see section G.1).

If a research project foresees personal data transfers to countries outside the EEA without an adequacy decision, the project coordination should demonstrate the lawfulness of that transfer and require its prior approval by the Research Support Office (GAI), where it may also be necessary to attach the opinion of the Ethics Committee and/or the Data Protection Officer.

N. ACCESS TO ARCHIVES WITH PERSONAL DATA OF DECEASED PERSONS

The GDPR Implementing Law determines that the personal data of deceased persons are protected when they fall into the special categories of personal data, or when they refer to the intimacy of private life, to images or data related to communications, except under the conditions established in Article 9(2) of the GDPR.[53]

Thus, in the framework of these exceptional conditions, it is possible to access personal data of deceased persons if the processing is necessary for archiving purposes of public interest, for

[49] See https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt
[50] The list is available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt.
[51] GDPR, Article 46.
[52] GDPR, Article 49(1)(a).
[53] Implementing Law, Article 17.

scientific or historical research purposes or for statistical purposes, based on one or more Portuguese or European Union laws, provided that the technical and organisational measures indicated in Article 89(1) of the GDPR, related to processing for scientific research, are taken.[54]

In Portugal, the General Framework of Archives and Archival Resources[55] establishes free access to documents in public archives that contain personal data of natural persons within the following time limits:

> 1) After 30 years have elapsed since the death of the persons to whom the documents refer; or
>
> 2) When the date of death is unknown, after 40 years have elapsed since the issue of the documents, but not before 10 years have elapsed since the death has been known.

After these time limits, there is free access to administrative documents that contain personal data of deceased persons. The right of access before the time limits referred to above, in the absence of any Portuguese or European law establishing this, is exercised by whoever the deceased person has nominated for the effect or, in its absence, by the respective heirs.

In the case of private archives, the owners are responsible for proposing the rules and forms of access to the documentation, approved by the superintendent government member on archival policy.

O. DATA PROTECTION IMPACT ASSESSMENT

O.1 When is it necessary to conduct an impact assessment?

When the processing is likely to result in a *high risk* to the rights and freedoms of natural persons, it is necessary, *before starting the processing*, to conduct a *Data Protection Impact Assessment* (DPIA).[56] A DPIA is particularly important when new technologies are introduced.[57] The DPIA aims to identify risks to the data subjects, with a view to mitigating them with appropriate safeguards.

The GDPR does not define "high risk", but the DPIA is mandatory in the following cases:[58]

a) Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the data subject or similarly significantly affect the data subject.

> *Profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or

[54] Article 9(2)(j) of the GDPR. This law should be proportional to the envisaged goal, respect the essence of the right to personal data protection and foresee appropriate and specific measures for the protection of the fundamental rights and interests of the data subjects.
[55] Decree-Law 16/93 of 23 January.
[56] GDPR, Article 35.
[57] GDPR, Recitals 89-91.
[58] GDPR, Article 35(3).

movements.[59] A decision produces *legal effects* when aspects of the natural person's legal sphere are affected, for example, the right to vote. The processing may *significantly affect* a natural person if it influences his/her circumstances, behaviour or choices. For example, profiling may lead to rejection of a loan request at a bank.

b) Processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences.

The GDPR does not define "large scale". Some indicators could be the number of data subjects involved, the volume of data or the diversity of data to be processed, the duration of the data processing activity or its pertinence, or the geographic dimension of the processing activity.[60]

c) Systematic monitoring of a publicly accessible area on a large scale.

Systematic monitoring is defined as processing to observe, monitor or control the data subjects.

A DPIA is also mandatory when the processing features on the List of personal data processing subject to DPIA, published by the Portuguese National Data Protection Authority (CNPD).[61]

If none of the previous conditions are applicable, the combination of two or more of the following criteria could indicate high risk, and thus the need to conduct a DPIA:

1. Evaluation or scoring, including profiling and predicting.[62]

---

[59] GDPR, Article 4(4).

[60] There is no definition as to what constitutes large scale in the GDPR. The following factors could be considered in its appraisal:

- The number of data subjects affected as a specific number or percentage of the population in question, for example, a high percentage of Iscte students;
- The volume of data and/or scope of the different data items that will be processed;
- The duration, or permanence, of the data processing activity;
- The geographic scope of the processing activity.

Examples of large-scale data processing include: i) the processing of data of a technology for personal use of a population that tracks the contact details, such as Stayaway Covid; ii) the processing of data of patients in the normal performance of the activities of a hospital; iii) the processing of travel data of persons using the public transport system of a city; iv) the processing of data of clients in the normal performance of the activities of an insurance company or a bank.
Examples that do **not** constitute large scale processing include: i) the processing of data of patients by a doctor; ii) the processing of personal data related to criminal convictions and offences by a lawyer.
See section 3 of the GT29 document: https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

[61] 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

[62] Especially «aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements» (Recitals 71 and 91 of the GDPR). Examples of this criterion may include: A distance learning platform used for collection, analysis and classification of students' data activities and behaviour, with the aim of teachers applying differentiated teaching methods and improve learning goals; A financial institution that selectively

2. Automated decisions that produce legal effects or significantly affect the data subject in a similar way.[63]

3. Systematic monitoring: processing intended for observation, monitoring or control of the data subjects, including data collected through networks or a systematic monitoring of a publicly accessible area on a large scale.[64]

4. Processing of sensitive data or data of a highly personal nature, including special categories of personal data and data related to criminal convictions and offences.

5. Large scale data processing.[65]

6. Matching or combining datasets: for example, originating from two or more data processing operations performed for different purposes and/or by different data controllers, in a way that would exceed the reasonable expectations of the data subjects.[66]

7. Data related to vulnerable data subjects, whenever there is a strong power imbalance between the data subjects and the data controller, meaning that the data subjects might not be able to easily consent to, or object, the processing of their data or exercise their rights. This is the case, for example, of children, employees, vulnerable segments of the population that need special protection, e.g., mentally ill persons, asylum seekers, the elderly, patients, etc.

8. Use of innovative solutions or application of new technological or organisational solutions, that could involve new forms of data collection and use, possibly with high risk to personal rights and freedoms. For example, combining the use of finger print and facial recognition to improve the control of physical access to a building. The use of big data, artificial intelligence or "internet of things" applications, whenever this is likely to have a significant impact on the daily lives and privacy of individuals, are candidates for this criterion.

9. When the processing prevents data subjects from exercising a right or using a service or contract.[67]

---

screens its customers against a credit reference data base or anti-money laundering and counter-terrorist financing or fraud database; A biotechnology company offering genetic tests directly to consumers in order to assess and predict disease or health risks; or research that develops behavioural or marketing profiles based on usage of some company's website.

[63] For example, the processing could imply the exclusion or discrimination of persons. Processing with little or no effects on individuals does not match this specific criteria.

[64] For example, video capture for processing and investigation of the routes used by people when moving inside a publicly accessible building, e.g., at a university.

[65] On large scale, see footnote 60.

[66] For example, derived from two or more data processing operations carried out for different purposes and/or by different data controllers in a manner surpassing the reasonable expectations of the data subjects. For example, the processing of personal data of the curricular path and performance of students of a university which, for the same purpose, also uses personal data of these same students that are publicly available on social networks.

[67] For example, processing operations aimed at authorising, modifying or refusing data subjects' access to a service or entry into a contract. For example, when a bank screens its costumers against a credit reference database in order to decide whether to grant them a loan.

A detailed description of the criteria with examples can be consulted in the Article 29 Data Protection Working Party guidelines which determine whether the processing is «likely to result in high risk» for purposes of the GDPR.[68]

O.2 Who is responsible for conducting the impact assessment?

Iscte, as the data controller, is responsible for ensuring that the DPIA is carried out, which may be conducted by Iscte or outsourced. Iscte is also responsible for involving the Data Protection Officer in the preparation of the DPIA, and request his opinion.

In scientific research projects, the project coordinator is responsible for ensuring that the DPIA is carried out. In PhD theses and master dissertations, the student's supervisor is responsible for ensuring and supervising its accomplishment. In all cases, it is mandatory to seek the advice of the Data Protection Officer.

The Data Protection Officer's opinion and the decisions taken by the coordinators after the opinions have been issued are documented in the DPIA.

P. PERSONAL DATA BREACH

If a personal data breach occurs, the researcher and student undertake to report it immediately to the SIIC – Serviço de Infraestrutura Informática e de Comunicações and to Iscte's Data Protection Officer, using the institutional e-mail addresses or the specific electronic form available for this purpose.

A data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Personal data breaches entail one or more types of occurrences:

> Confidentiality Breach – an accidental or unauthorised disclosure of, or access to, personal data.
>
> Integrity Breach – an unauthorised or accidental alteration of personal data.
>
> Availability Breach – accidental or unauthorised loss of access to, or destruction of, personal data.

Examples of personal data breaches include the misappropriation or theft of a pen or laptop computer that stores personal data, the accidental or deliberate sending of personal data to third parties who are not authorised to access it, the infection of a computer with virus that destroys, alters or compromises the availability of personal data.

Timely reporting of the occurrence of personal data breaches is fundamental, so that the competent services execute a response plan to mitigate the risks to Iscte and/or the data subjects.

[68] Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (AIPD) and that determine whether the processing is «likely to result in a high risk» for purposes of Regulation (EU) 2016/679, https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

Q. ETHICS COMMITTEE AND DATA PROTECTION OFFICER

In case of doubts, the researchers may seek advice from the Research Support Office (GAI) and the Data Protection Team.

If the project involves at least one of the criteria referred to in section O.1, the researcher should submit the project for approval by the Ethics Committee or seek the advice of the Data Protection Officer.

If the project raises complex questions on data protection, it is advisable to conduct a Data Protection Impact Assessment (AIPD). The Data Protection Impact Assessment requires the opinion of the Data Protection Officer. When possible, it may be useful for the project to appoint a data protection consultant.

R. USEFUL DOCUMENTS AND LINKS

- Personal Data Protection_Policy of Iscte
- Web page of documents on personal data protection on Fenix ('Pessoal' tab)
- Code of Ethical Conduct in Research of Iscte
- Website of the Ethics Committee of Iscte
- GDPR https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679
- GDPR Implementing Law https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized
- Opinion on data protection and scientific research of the European Data Protection Supervisor of 6 January 2020 https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en
- Guidance notes on ethics and data protection for the preparation of research projects, drafted by a panel of experts at the request of the European Commission https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
- Comissão Nacional de Proteção de Dados [National Data Protection Authority] https://www.cnpd.pt/
- European Data Protection Board https://edpb.europa.eu/
- Opinions and guidelines on data protection of the Article 29 Data Protection Working Party https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360
- Guidelines on the principle of transparency https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
- Guidelines on consent https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
- Guidelines on data protection impact assessment https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- Opinion on anonymisation techniques https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- Guidelines on automated individual decisions and profiling https://www.cnpd.pt/home/rgpd/docs/wp251rev01_pt.pdf

- Other opinions of the Article 29 Data Protection Working Party: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

S. DEFINITIONS

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.
Data Subject	Any identified or identifiable natural person whose personal data are held by the data controller.
Special categories of data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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 a highly personal nature	Data linked to household or private activities (such as electronic communications whose confidentiality should be protected) or that impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or whose breach clearly involves serious impacts in the data subject's daily life (such as financial data that can be used for 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.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Consent of the data subject	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.
Pseudonymisation	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.
Anonymisation	Irreversible conversion of personal data into anonymous data so that they can no longer be attributed to identified or identifiable data subjects. The data should not allow re-identification.

Participant Information Sheet (PIS)	Sheet with information to be provided to the data subjects on the purpose of the data processing, the legal basis for the processing, what will happen to the data and the risks involved, pursuant to Articles 13 and 14 of the GDPR. See section F.2
Re-identification	Process of transforming data that are believed to be anonymous back into personal data by data matching or similar techniques.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Automated individual decision-making	*Exclusively* automated decision-making occurs when decisions are taken about a natural person by technological means and without human involvement. This may be carried out without profiling. If a person controls the final decision supplied by the algorithm, with effective power or ability to influence the final result, the decision may be considered not "exclusively" automated. However, the contribution or bias of the automated processing in the decision-making may not be easy to distinguish.
Personal data breach	A security breach that accidentally or unlawfully causes the destruction, loss, alteration, disclosure or access, in an unauthorised manner, to personal data transmitted, stored or subject to any other type of processing.

Record of changes

Version number	Description of the change	Date of issue
01	Initial version, proposal of the Data Protection Officer.	16 October 2020
02	Revision of the proposal by the legal services and Data Protection Officer.	26 March 2021
03	Revision of the proposal by the Data Protection Team after meeting with the Rectory and Research Support Office (GAI). Additional sections or information were included, related to international transfers, types of time limits for storage and personal data of deceased persons.	18 February 2022
04	Approved by order of the Rectory and authorised for publication.	28 March 2022