iscte INSTITUTO UNIVERSITÁRIO DE LISBOA

QUESTIONNAIRE ON PERSONAL DATA PROCESSING

TABLE 1 - PERSONAL DATA PROCESSING		
A.	**Does the study involve processing of personal data?[i]**	
A.1	Yes	□
A.2	No	□
If the study does not involve the processing of personal data, all the rest of the answers to table 1 and table 2 should be left blank		
B.	**Apart from Iscte, are any other persons or entities responsible for the personal data processing (data controllers)?[ii]**	
B.1	Yes Identify the data controllers: Click here to enter text. (Please consult the Research Support Office (GAI) for formalising a joint responsibility agreement, pursuant to Article 26 of the GDPR).	□
B.2	No	□
C.	**What is the legal basis for the processing of personal data?**	
C.1	Consent of the data subjects – Article 6(1)(a) of the GDPR	□
C.2	Consent of the data subjects (for processing special categories of personal data - 'sensitive data')[iii] – Article 9(2)(a) of the GDPR	□
C.3	Other: Click here to enter text.	□
D.	**How are the personal data collected?**	
D.1	From the data subject	□
D.2	Personal data of other studies, whose data controller is Iscte	□
D.3	Personal data of other studies, whose data controllers are other institutions	□
D.4	Publicly available data	□
D.5	Other (specify) Click here to enter text.	□
E.	**What is the nature of the processed personal data?**	
E.1	Special categories of personal data ('sensitive data')[iv] Indicate the categories: Click here to enter text.	□

E.2	Data of highly personal nature[v] Indicate which data are processed: Click here to enter text.	□
E.3	Personal data related to criminal convictions and offences Indicate which data are processed: Click here to enter text.	□
E.4	Voice, image or video recordings	□
E.5	Other Indicate which:[vi] Click here to enter text.	□
F.	**Who are the data subjects?**	
F.1	Children or young people aged less than 18 years old Planned number of data subjects: Click here to enter text.	□
F.2	Vulnerable groups, implying a considerable imbalance between the data subject and the data controller meaning that the data subjects may be unable to easily consent to, or oppose, the processing of their data or exercise their rights.[vii] Planned number of data subjects: Click here to enter text.	□
F.3	Students of Iscte Planned number of data subjects: Click here to enter text.	□
F.4	Iscte employees and contract workers (e.g., lecturers, civil servants, etc.) Planned number of data subjects: Click here to enter text.	□
F.5	Other Indicate the planned number of data subjects and who they are: Click here to enter text.	□
G.	**How many persons in the study team are foreseen to have access to the personal data?**	
H.	**Technical and organisational measures for protection of personal data and retention periods:**	
H.1	Anonymisation Indicate the period of retention of personal data up to their anonymisation: Click here to enter text.	□

H.2	Pseudonymisation[viii]	□
H.3	Destruction Indicate the retention period: Click here to enter text.	□
I.	**Mark the applicable choice for the software used for the personal data processing:**	
I.1	Software licensed by Iscte (e.g., Excel of Office 365)	□
I.2	Software not licensed by Iscte, and whose operation is compliant with the GDPR Specify the software used: Click here to enter text.	□
J.	**Indicate the form and place of storage of the personal data:**	
J.1	In Iscte servers or through cloud services provided by Iscte (e.g., Sharepoint of Office 365)	□
J.2	In Iscte institutional computers	□
J.3	In personal computers	□
J.4	Other (specify): Click here to enter text.	□
K.	**Other technical and organisational measures – mark the adopted measures:**	
K.1	The personal data access sessions are protected and authenticated with personal credentials	□
K.2	Encryption of the personal data in the storage devices	□
K.3	Members of the study team who have access to the data and do not have a contract with Iscte (e.g., students) sign the responsibility and non-disclosure agreement	□
K.4	Describe additional risk mitigation measures that you are considering to apply, especially if you ticked any of the items E.1, E.2 or E.3: Click here to enter text.	
L.	**Are there any data processors (outsourcing), i.e., any third party or body that does not belong to the study team and that processes all or part of the personal data on behalf of the data controller?**	
L.1	Yes Indicate the data processed on behalf of the controller and the name of the data processor: Click here to enter text. (Please consult the Research Support Office (GAI) for formalising a contract that ensures compliance with Article 28 of the GDPR).	□

L.2	No	□
M.	**Are there transfers of personal data to individuals or organisations in countries outside the European Economic Area and without 'adequacy decision'?**[ix]	
M.1	Yes Indicate the countries. If the legal basis for the processing is the consent of the data subject, indicate the risk that could arise from the transfers to the participants and mitigation measures. If the legal basis is other than consent, describe the appropriate safeguards pursuant to Article 46 of the GDPR. Click here to enter text. Pertinent documentation may be attached.	□
M.2	No	□
N.	**If you marked one or more of the choices D.2, D.3, D.4 or D.5 and the legal basis for the processing is not the consent of the data subjects, were the participants informed or will the participants be informed on the new data processing, pursuant to Article 14 of the GDPR?**	
N.1	Yes	□
N.2	No Justify in detail: i) why it does not appear to be possible to provide that information; or ii) why it would imply a disproportionate effort or would seriously impair the achievements of the objectives of the processing; and iii) the measures taken to protect the rights, freedoms and legitimate interests of the data subjects. Click here to enter text.	□
O.	**For the period before the data are anonymised or destroyed, does the study have plans, in any manner, to restrict the rights of access, rectification, limitation of processing, or objection established in Articles 15, 16, 18 and 21 of the GDPR?**	
O.1	Yes Indicate which rights are curtailed, and how and to what extent they are curtailed. Explain: i) why they could preclude or severely jeopardise the accomplishment of the study's aims; ii) how you assess the possible impact this could have on the data subjects. Click here to enter text.	□
O.2	No	□

TABLE 2 - SPECIFIC PERSONAL DATA PROCESSING THAT COULD ENHANCE RISK

P.	**Indicate whether the personal data processing involves any of the following risk operations:**[x]	
P.1	Evaluation or scoring, including profiling and prediction[xi]	□
P.2	Automated-decision making with legal or similar significant effect on data subjects[xii]	□
P.3	Systematic monitoring[xiii]	□
P.4	Data processing on a large scale[xiv]	□
P.5	Matching or combining datasets[xv]	□
P.6	Innovative use or applying new technological or organisational solutions[xvi]	□
P.7	Processing that prevents the data subjects from exercising a right or using a service or a contract[xvii]	□
Q.8	If you have marked any of the operations in P.1-P.7, describe them in the context of the research work and indicate why they are necessary. Click here to enter text.	
If you ticked two or more points concerning the following set of criteria, you may consider doing a Data Protection Impact Assessment, which you can attach. Such Data Protection Impact Assessment may also be requested at a later date by the Ethics Commission or Data Protection Officer:[xviii] One of the items E.1, E.2 – 1 point E.3 – 1 point One of the items F.1, F.2 – 1 point P.1, P.2, P.3, P.4, P.5, P.6, P.7 – Each one of these criteria is worth 1 point		

[i] Personal data is defined as any information, of any nature and in any format (e.g. voice recording or image), relating to an identified or identifiable natural person. 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 (e.g. an IP) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[ii] The data controller is the legal or natural person, public authority, agency or other body that, individually or jointly with others, determines the purposes and means of personal data processing. When two or more controllers jointly determine the purposes and means of this processing, both are jointly responsible for the processing. The joint controllers determine, by agreement in a transparent mode, the responsibilities of each for compliance with the General Data Protection Regulation (GDPR) (Articles 4(7), 24 and 26).

[iii] Applicable to the processing of special categories of personal data, i.e., personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, and to the processing of genetic data, biometric data that unambiguously identify a person, data related to the health, sexual life or sexual orientation of a person.

[iv] Special categories of personal data, or 'sensitive data', are personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership, genetic data, biometric

data that unambiguously identify a person, data related to the health, sexual life or sexual orientation of a person.

[v] Data linked to private or family activities (such as electronic communications whose confidentiality should be protected) or that affect the exercise of a fundamental right (such as location data whose collection 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 fraud).

[vi] Examples: name, identification numbers, contact details, address, location data, marital status, financial data, image, voice or video recordings, sociodemographic data, etc.

[vii] This is the case, for example, of children, employees, vulnerable segments of the population that need special protection, e.g., people with mental disorders, asylum seekers, the elderly, the sick, etc.

[viii] Processing of personal data that are no longer able to be attributed to a specific data subject without using supplementary information, provided that this supplementary information is kept separately and subject to technical and organisational measures that ensure that the personal data cannot be attributed to an identified or identifiable natural person. For example, by creating a copy of the dataset, but where the personal identification 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 decoding key, does not permit the identification of the data subjects.

[ix] In certain cases, it may be declared that a third country offers an appropriate level of protection by decision of the European Commission («adequacy decision»), which means that it is possible to transfer data to an institution located in a third country without the data exporter having to submit supplementary 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 EU. 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. The list of of countries that have been given 'adequacy decisions' can be consulted at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt

[x] Examples of the meaning of each criterion are available in the GT29 document for data protection: 'Guidelines on Data Protection Impact Assessment (AIPD) and determining whether the processing is «likely to result in a high risk» for purposes of Regulation (EU) 2016/679', in particular the criteria presented therein and the examples of pages 10-14 (Portuguese version), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[xi] 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 data of student activities and behaviour for the teacher to apply differentiated teaching methods and improve learning goals; A financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database; A biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks; or Research for a company that develops behavioural or marketing profiles based on website use or browsing.

[xii] Processing that aims at taking decision on the data subjects producing «legal effects concerning the natural person or similarly significantly affect the natural person» (Article 35(3)(a) of the GDPR). For example, the processing could imply the exclusion or discrimination against individuals. Processing that produces few or no effects on individuals does not meet these specific criteria.

[xiii] 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» (Article 35(3)(c) of the GDPR). 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. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s)

[xiv] 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 concerned, either as a specific number or as a proportion of the relevant population, for example, a high percentage of Iscte students;
- The volume of data and/or the range of different data items being processed;
- The duration, or permanence, of the data processing activity;
- The geographic extent 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 traces contacts, 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 following GT29 document:

https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

[xv] For example, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that could exceed the reasonable expectations of the data subjects. For example, the processing of the personal data of the curricular path and performance of students of a university institution which, for this purpose, also uses personal data of these same students that is publicly available on social networks.

[xvi] When the technology's use could involve new forms of data collection and use, possibly with high risk to personal rights and freedoms. For example, combining the use of fingerprint and face recognition for improved physical access control to a building. The use of big data, artificial intelligence techniques or internet of things applications could meet this criterion.

[xvii] For example, processing operations aimed at allowing, modifying or refusing the access of the data subjects to a service or entering into a contract. For example, where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

[xviii] Consult the GT20 document: 'Guidelines on Data Protection Impact Assessment (AIPD) and determining whether the processing is «likely to result in a high risk» for purposes of Regulation (EU) 2016/679', https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236