Basic guide for Researchers on the Protection of Personal Data

Within the framework of the R&D activities carried out by the Technical University of Cartagena it is essential to take into account the requirements of the **regulations on the protection of personal data**. For that reason, every researcher must consider the following directives counting on the support of the UPCT Data Protection Delegate (DPD) who they must contact by email: dpd@upct.es.

1. **If we can avoid doing so, we will not use personal data.** Therefore, for example we will use anonymous surveys, avoiding questions that enable the person who gave the answers to be identified. If the data are audiovisual then techniques will be planned that make it possible to obtain the data anonymously, such as modifying the person's voice or image so as to render it impossible to identify them.
2. It is recommended to design the research to avoid gathering **especially protected personal data** as far as possible. In the event that it is essential to do so, an assessment of the impact that the fact that the University processes this data has on the persons' rights and freedoms. In these cases, the DPD will advise on how to process the data.
3. **If we process personal data we must inform the DPD at the University.** The processing must be reflected in the Register of Processing Activities that is published in the electronic headquarters of the UPCT.
4. **We will always use the minimum of personal data possible to fulfil the principle of data minimisation**: the personal data that are gathered within the framework of an R&D activity must be limited to what are strictly necessary to achieve the objectives of said activity**.**

   Thus, for example:

   a. If we are only interested in having control over who answers a questionnaire to avoid duplicated answers, we shall maintain the answers obtained and an identification list of who has answered, without the answers being linked to the person who gave them.

   b. If the age of the person is relevant we will request them to indicate their age or their year of birth, but not the complete birthdate.
5. **Whenever possible we will carry out a process of pseudonymisation of the personal data that make it difficult to know who they belong to.** Thus, for example, if we have

human biological samples we must code them so that the person they belong to cannot be identified with only the sample's name. The link of the sample code with the person it corresponds to must be kept in a safe place to which only authorised personnel have access.

6. **The personal data will be gathered with the informed consent of the person with a clear affirmative declaration** and which must be available to be shown later if needed. The identity of the person must be verified to check that in fact the person who gives consent is who they say they are. For online questionnaires it is necessary to attach a compulsory question, together with the data protection clause, which is ticked in a box accepting that they have read it and whenever possible authentication by the person will be required in the Virtual Campus.
7. **For those younger than 14 years of age, the consent must be obtained from the person who has parental authority or the legal guardian.** If the minors are from other European Union countries and aged between 13 and 16 years, then the member states have specifically regulated this requirement within the permitted range.
8. **The person must always be informed of the following, even when the data do not come from the person themself:**
    a. Who will process the data and who they will be ceded to.
    b. If applicable, where the data have been obtained if they do not come from the same person.
    c. What data will be processed and under what security measures.
    d. The purpose of processing the data. It is important to identify:
        i. If in the future other uses than those of the current study may be sought. This must be informed at the time that the data are being gathered since, if this is not the case, they cannot be used without new consent from the person.
        ii. If profiling the person will be carried out with the data, under what criteria and procedures that would enable conclusions to be reached on the information therein and if automated decisions will be taken from that profile, such as inviting them to participate in other studies.
    e. For how long they will be processed, taking into account the applicable regulations and the probability of other requirements such as subsequent audits.
    Once that time has lapsed the data must be securely eliminated.
    f. What the rights with respect to the processing of data are and how they can be exercised. Indicate that the rights are of access, rectification, suppression, portability, limitation and opposition to processing.

g. Who the Data Protection Delegate is and how they can be contacted.

Models of **Informed Consent** and **Information Sheet** are available in the webpage of the Ethics in Research Committee; these can be used as a guide and adapted to the specific characteristics that your R&D activity requires (https://www.upct.es/vicerrectoradoinvestigacion/es/etica/modelos-y-formularios).

9. **Prior to processing data, the security measures that will be used when processing the data must be defined so as to ensure the principle of security from the design**. If especially protected data are to be processed then the security measures must be tightened. In this regard, the DPD, in conjunction with the person Responsible for Security at the UPCT, will advise on the most appropriate information systems to be used and the measures to apply. The researchers must inform about the type of support in which the data will be gathered (written documents, web forms, voice recordings, videos, monitoring by means of geolocators, etc.)

   Examples of processing that may imply a high risk:

   - Elaboration of profiles upon which decisions may produce legal effects or significantly affect interested parties.
   - Processing on a large scale of especially protected data.
   - Systematic large-scale observation of a public access zone.

10. **Whenever possible, the University's own systems should be used to which the relevant security measures are centrally applied.** If it is necessary to use other systems, they must be securely configured to ensure fulfilment with the **principle of default security**. They must be designed to avoid any known errors, such as the use of default passwords of the administrator user. Moreover, functions and information fields of the program that are not needed will be blocked and it will be kept updated with the respective security patches.

11. **When handling data** everyone who participates in carrying out the study will be warned of the security measures that they must take into account and also know that the data must be used only and exclusively for the end that they were gathered for, avoiding any unauthorised access to them.

12. **In the event that a supplier participates in carrying out the study, they are considered to be In Charge of Handling** the data, which will still be the responsibility of the UPCT. In that case, a limiting contract must be subscribed with the supplier, clearly indicating, among other things, what data will be processed and under what security measures, as well as what they must do with the data after the end of the contract.

13. **If the data are handled by a supplier or an entity that participates in the study and which is located outside the European Area then it must be demanded that the data be handled according to the premises of European regulations**, which are among the most

demanding in the world on this issue. The DPD will advise on the demands to subscribe by means of a contract or collaboration agreement. The data will remain on European territory as far as possible, and the other party will be given access to them without being able to extract them.

14. With regard to the public function of the University to promote research **it may be possible to invite the university community to participate in research studies**. However, the members of the University Community must have a simple mechanism to unsubscribe themselves from receiving this type of communications, which would have to respect their decision to not send them additional requests.

ANNEX

Applicable legislative framework: https://privacidad.upct.es/container/normativa-vinculada-ala-proteccion-de-datos

Actors involved in the process

1. **Interested party:** identified or identifiable natural person. Any person whose identity can be determined, directly or indirectly from certain information will be considered as a natural identifiable person.
2. **Responsible for data processing:** when UPCT researchers gather personal data within the framework of R&D activities, the UPCT will be responsible for processing that data.
3. **In Charge of Data Handling:** natural or legal person, public authority, service or other organism that processes the personal data for the person responsible for their processing. The Researcher in Charge of the R&D activity will be in charge of their processing.
4. **Co-responsible for data processing:** When two or more people are responsible they determine the objectives and the means of processing of the personal data, they will be considered co-responsible for processing them, for example, in research projects carried out in cooperation with other Universities.
5. **UPCT Data Protection Delegate** (DPD).
6. **Responsible for Security at the UPCT**.

Glossary of terms used in the present guide (in accordance with the current legislation for the protection of personal data)

> **Personal data**: That related to an identified or identifiable natural person "the interested party". Therefore, although we do not have the name or ID number of a person, if we have a series of data that would enable the person to be determined, then they are equally considered personal data.
>
> **Especially protected personal data:** That data which reveals the ethnic or racial origin, political opinions, religion or other philosophical beliefs, trade union membership and the processing of genetic data, data relating to health, or data on the sexual life or criminal records, penal, administrative infractions or related security measures.

Processing: Any operation or series of operations carried out on personal data or sets of personal data, whether it be by automated procedures or not, such as gathering, recording, organisation, structuring, conservation, adaptation or modification, extraction, consulting, use, communication by transmission, diffusion or any other form of enabling access, comparing or interconnection, limitation, suppression or destruction.

Elaboration of profiles: Any form of automated processing of personal data consisting in using the personal data to assess determined personal aspects of a natural person, in particular to analyse or predict, aspects pertaining to professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements of said natural person (this point is very important in the application of Artificial Intelligence (AI) that develops automated profiles for predicting.

Pseudonymisation: It is the processing of personal data in such a way that they cannot be attributed to the interested party without using additional information, provided that said additional information is separate and is subject to technical and organisational measures aimed at guaranteeing that the personal data are not attributed to an identified or identifiable natural person.

Anonymisation: It is the definitive and irreversible disassociation of the personal data.

Consent of the interested party: In those possible cases in which the legal basis of processing is the consent, the cited demonstration of willingness must be given freely, specifically, informed and unequivocal by the person who accepts, by means of a declaration or clear affirmative action, the data processing that concerns them to the person who it is lent to. One of the ways to accredit this can be by means of checking a verification box. In any case, the processing will be limited to the end that it was requested for.