PERSONAL DATA PROTECTION PLAN

CENTRE D'ESTUDIS DEMOGRÀFICS

4 February 2025

CED
Centre d'Estudis Demogràfics

HR EXCELLENCE IN RESEARCH

ÍNDEX

1. EXECUTIVE SUMMARY

This document is a revision of document P03.3 from October 2019, as of January 2025.

The Personal Data Protection Plan refers to the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights, by the CONSORCI CENTRE D'ESTUDIS DEMOGRÀFICS, a public entity under private law.

The basic concepts to be considered according to the aforementioned Regulation (hereinafter GDPR) are as follows:

- **Personal data:**

Any information relating to an identified or identifiable natural person ("the data subject"). A natural person is considered identifiable if they 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

- **Consent of the data subject:**

Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them, either by a statement or by a clear affirmative action.

- **Processing:**

Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- **Data processor:**

A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

- **Risk Management**

The set of activities and tasks that allow uncertainty of a threat to be controlled through a sequence of actions including risk identification and assessment, as well as the measures for its reduction or mitigation.

- **Measures and Protocols to Ensure Data Security:**

These are intended to ensure the security of personal data, considering the state of the art, the cost of implementation, the scope, context, and purposes of the processing, as well as the risks and threats to the rights and freedoms of individuals, so that compliance and effectiveness of the measures applied can be demonstrated where applicable. The appropriate time to define the control and security measures to be applied is at the service design phase.

The CED has a "**Privacy Protocol and Security Measures for Personal Data at CED**," which is supervised by a Data Protection Officer (DPO) whose role is to ensure its correct application. The CED also has a "**Data Protection Policy**," signed by the CED management. Both documents are updated as of July 2024.

The implementation required under the GDPR is detailed in the aforementioned Protocol, and this document, within the framework of the HRS4R strategy, summarizes its most relevant contents.

All CED personnel must be aware of this regulation and follow the Protocol whenever they design or develop an activity or research project that involves the use of personal data.

2. INTRODUCTION

On 27 April 2016, Regulation (EU) 2016/679 of the European Parliament and of the Council was approved, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU 4.5.2016).

The most notable innovation of this legislation is the principle of active responsibility. This means that the organization, through all personnel working with personal data, must be proactive in complying with confidentiality obligations, risk management, and the rights of data subjects, through explicit clauses and consents, using records, signed documentation, informing of possible security breaches, etc.

At the end of 2017, CED began adapting to the new European regulation, which fundamentally changed the management of personal data processing and the rights of data subjects in accordance with the law that would come into force on 25 May 2018, the final date for the application of the regulation.

At the beginning of 2018, CED created a working team trained in the concepts and procedures required by the new regulation.

In December 2018, Spanish legislation supplemented these provisions with LOPD 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights.

In March 2019, CED appointed a Data Protection Officer (DPO), who joined the team to advise on the final drafting of the "**Privacy Protocol and Security Measures for Personal Data at CED**."* This document is updated whenever necessary, with the most recent version dating from July 2024.

Since 2020, the CED DPO has updated and monitored the data protection protocols developed at CED through audits, resulting in an annual **verification report**. The DPO also advises CED on all matters related to our policy; for example, in 2024, the "**CED Digital Disconnection Protocol**" was developed.

All required implementation is detailed in the aforementioned Protocol, and this document, within the framework of the HRS4R strategy, summarizes its most relevant contents.

3. DATA CONTROLLER

Name: CONSORCI CENTRE D'ESTUDIS DEMOGRÀFICS, PUBLIC ENTITY OF PRIVATE LAW

Activity: research, training, and knowledge transfer in the field of demography

VAT Number (CIF): Q5855973C

Contact email: personaldata@ced.uab.cat

Phone: +34 935813060

* This Protocol contains full details of the actions that must be carried out, as well as the different types of documents to be used for each of the measures aimed at protecting the privacy and security of personal data. The complete list can be found in the annex.

Address: Edifici E2, Campus UAB, 08193, Cerdanyola del Vallès

Website: https://ced.cat/

3.1. Obligations

The data controller is the natural or legal person, public authority, service, or any other body that, alone or jointly with others, determines the purposes and means of the processing.

Processing of personal data is defined as "any operation or set of operations performed on personal data or sets of personal data, whether by automated or non-automated means, such as collection, recording, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction."

3.2. It is the responsibility of the Data Controller to:

- Apply the principles of the Regulation (GDPR) in the processing of personal data in order to ensure and demonstrate that the processing complies with the GDPR, both when determining the means of processing and during the processing itself.
- Ensure that only personal data that are necessary are processed.
- Implement appropriate security measures related to processing activities to guarantee the confidentiality and integrity of the data.
- Select data processors who ensure the implementation of appropriate technical and organizational measures.
- Cooperate with the supervisory authority upon request.
- Communicate any security breaches that occur: the processor to the controller, and the controller to the supervisory authority and the data subject.
- Appoint a Data Protection Officer when required.

4. DATA PROTECTION OFFICER (DPO)

The Regulation introduces the role of the Data Protection Officer when the processing is carried out by a public authority or body, as is the case with the CED. The person appointed to this role at the CED is Maria Company Jiménez, a lawyer specializing in Digital Law and Data Protection.

The Data Protection Officer's functions include, among others:

- Informing and advising the controller or processor and the staff about the obligations imposed by data protection legislation.
- Monitoring compliance with the legislation.
- Advising on Data Protection Impact Assessments.
- Cooperating with the supervisory authority.
- Acting as a contact point for issues related to data processing.

The data controllers and processors must make the designation of the Data Protection Officer public, including their contact details, and communicate it to the relevant supervisory authorities.

The position of the DPO within organizations must comply with the requirements explicitly established by the GDPR: full autonomy in the exercise of their duties, the need to report to the highest management level, and the obligation for the controller or processor to provide all necessary resources to carry out their activities.

5. CHARACTERISTICS OF THE PROTOCOL

The **CED's Privacy and Personal Data Security Protocol** contains the definition of basic concepts, the legal bases, and the different areas of application of the regulation, with the following information in which the aspects summarized here are further developed, such as:

5.1. Scope of application

The Regulation extends the territorial scope to data controllers and processors established in the EU, as well as to activities of those not established in the EU when such activities are related to the offering of goods or services or to the monitoring of the behavior of individuals located in the EU.

5.2. Principles

The greatest innovation of the GDPR for data controllers consists of two general elements:

5.2.1. The principle of "proactive accountability"

The GDPR describes this principle as the need for the data controller to implement appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing complies with the Regulation.

This principle requires organizations to analyze which data they process, for what purposes, and what types of processing operations they carry out. Based on this understanding, they must explicitly determine how they will apply the measures provided by the GDPR. They must also ensure that these measures are adequate to achieve compliance and that they can demonstrate compliance to both the data subjects and the supervisory authorities.

In summary, this principle requires organizations to adopt a conscious, diligent, and proactive approach to all personal data processing activities they undertake.

5.2.2. The principle of "risk-based approach"

The measures aimed at ensuring compliance must take into account the nature, scope, context, and purposes of the processing, as well as the risk to the rights and freedoms of individuals.

These two elements apply across all organizational obligations. They represent "privacy by design" and "privacy by default."

The data controller must implement, both when determining the means of processing and during the processing itself, the appropriate technical and organizational measures designed to effectively apply the protection principles and integrate the necessary safeguards to meet the Regulation's requirements.

Additionally, the controller must apply adequate technical and organizational measures to ensure that, by default, only personal data that are necessary for each specific processing

purpose are processed.

5.3. Special Categories of Data

Genetic Data: Personal data relating to the inherited or acquired genetic characteristics of a natural person, which provide unique information about that person's physiology or health, obtained in particular from the analysis of a biological sample.

Biometric Data: Personal data obtained through a specific technical processing, relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that person (e.g., facial images, fingerprint data, etc.).

In-depth interviews conducted as part of certain research projects also fall under this category of special data, as they may reveal opinions, describe behaviors, and therefore include information related to ideology, sexual orientation, or other sensitive personal data.

5.4. Consent

The GDPR requires that the data subject gives consent through an unambiguous statement or a clear affirmative action. For the purposes of the new Regulation, pre-ticked boxes, tacit consent, or inactivity do not constitute valid consent.

Consent by omission is not compatible with the GDPR, as it is based on the inaction of the data subject.

Consent can be unambiguous or implicitly given, for example when it is inferred from an action of the data subject who chooses to continue browsing a website, thereby accepting the use of cookies to monitor their navigation.

Explicit consent is required for the processing of special categories of data, for automated decision-making, and for international data transfers.

5.5. Right to Information

Providing information is a right of the data subjects and must include the following aspects: the contact details of the Data Protection Officer; the legal basis for the processing; any legitimate interests pursued on which the processing is based, if applicable; the intention to transfer data to a third country or to an international organization and the legal basis for doing so, if applicable; the period for which the data will be retained; the right to request data portability; the right to withdraw consent at any time; whether the provision of data is a legal or contractual requirement, or necessary to enter into a contract; the right to lodge a complaint with a supervisory authority; the existence of automated decision-making, including the logic applied and its consequences.

The GDPR requires that information provided to data subjects be concise, transparent, intelligible, easily accessible, and presented in clear and plain language.

5.6. Main Rights:

The GDPR incorporates the right to erasure, the right to restriction of processing, and the right to data portability, in addition to maintaining the rights provided under previous legislation. Therefore, all the rights listed below must be considered:

- Access: allows the data subject to know and obtain information about the processing of their personal data free of charge.
- Rectification: a right to ensure the accuracy of the processed information. It allows correcting and modifying inaccurate or incomplete data.
- Erasure: allows the deletion of data that is inadequate or excessive without affecting the

obligation to block certain data.
- Objection: the right to demand the cessation of processing or to prevent the processing of the data of the data subject.
- Restriction: the right to suspend the processing operations of the data subject's personal data.
- Portability: a complement to the right of access. It allows the data subject to obtain the data provided to one organization or to transmit it directly to another entity.
- Right to be forgotten: the manifestation of the rights of erasure and objection applied to internet search engines. It allows preventing the dissemination of personal data online if certain requirements are not met.

5.7. Procedure for Exercising Rights

The GDPR does not establish a specific method for exercising rights, but it requires that data controllers ensure the procedures are visible, accessible, and straightforward, and that requests can be submitted electronically, especially when processing is carried out by electronic means.

Exercising these rights must be free of charge for the data subject.

The data controller may rely on the cooperation of processors to facilitate the exercise of the data subject's rights.

5.8. Record of Processing Activities

Controllers and processors must maintain a record of the processing activities they carry out. This record must include, for each activity, the information required by the GDPR:

- Name and contact details of the controller and, where applicable, the joint controller, as well as the data protection officer, if any.
- Purposes of the processing.
- Description of the categories of data subjects and categories of personal data processed.
- International data transfers.
- Where possible, the envisaged time limits for erasing the data.
- Where possible, a general description of the technical and organizational security measures.

5.9. Security measures

The Regulation does not provide a specific list of security measures applicable according to the type of data being processed. Instead, it establishes that the controller and processor must implement technical and organizational measures appropriate to the risk associated with the processing.

The specific measures to be applied must ensure:

- The confidentiality, integrity, availability, and ongoing resilience of processing systems and services.
- The ability to restore the availability and access to personal data promptly in the event of a physical or technical incident.
- The existence of a process to regularly verify and evaluate the effectiveness of the technical and organizational measures established to ensure the security of the processing.

If a security breach occurs, the controller must notify the supervisory authority within a maximum of 72 hours, unless it is unlikely to pose a risk to the rights and freedoms of individuals.

The CED keeps the following documents up to date:

- Staff list
- List of individuals with access to the data
- List of computers/servers
- Domain
- Software applications
- List of external parties with access to the Centre's data
- List of companies accessing the CED

The CED monitors and controls:

- Backups
- Possible security breaches
- Users' rights
- Media registers
- Data storage
- Data destruction

6. TYPES OF DATA SUBJECTED TO THE NEW REGULATION

- Personal data: All information that can identify a person, such as full name, national ID (DNI/NIE), passport, photo, video, email address, postal address, etc.
- Sensitive data: Any information that could compromise privacy rights, including health data, race, sexual orientation, marital and family status, disability, opinions, etc.

To manage processes related to data protection regulations, it is necessary to define the different activities in which this type of information is processed. At the CED, the following activities have been defined:

1. RESEARCH: Data: relationships with institutions; in-depth interviews
2. TRAINING: Candidates; predoctoral; postdoctoral
3. TEACHING: Professors; students; candidates
4. COURSES, SEMINARS, AND SUMMER SCHOOL: Professors; students; candidates
5. CONFERENCES: Who gives the lecture; conditions set (image rights, etc.); inform attendees that they may be filmed
6. RESEARCH STAYS: Tutors; residents; candidates
7. CONTACTS: Email, domain or printer access
8. HUMAN RESOURCES: Secretariat and functioning of the CED; administration and governance; accounting and budgets; research and training

It must be distinguished whether the data are the responsibility of the CED or whether the CED is merely in charge of processing them.

Access to information in each of the CED's activities can be transversal and of different types, such as direct handling of the information or simply having knowledge of it as part of a committee, for example. In any case, the confidentiality commitment must still be formally recorded.

CED resources are also managed in a controlled manner, for instance, through the CED domain or access to folders on servers. Paper-based information is stored in locked furniture within designated offices, which must also remain locked.

ANNEX: List of documents in the CED Security and Privacy Protocol

1. Annex a. Record of processing activities
2. Annex b. Protected resources
3. Annex c. Clauses for data subjects
4. Annex d. Data processors
5. Annex e. Roles and obligations of persons with access to the data of the data controller
6. Annex f. Employee privacy policy
7. Annex g. Internal communication model for security breaches
8. Annex h. Analysis of security breaches and necessity to notify the supervisory authority and the data subject
9. Annex i. List of personnel and users
10. Annex j. Record of entry and exit of data carriers
11. Annex k. Authorization for entry and exit of data carriers
12. Annex l. Templates for exercising data subject rights
13. Annex m. Confidentiality clause
14. Annex n. Backup procedures
15. Annex p. Monthly verification of access control for processing special categories of data
16. Annex q. Software applications
17. Annex r. Identification and authentication
18. Annex s. Security officer
19. Annex t. Erasure and destruction of documentation
20. Annex u. Storage of documentation
21. Annex v. Inventory of IT media
22. Annex w. Legal notice for the website
23. Annex x. Code of good research practices