PROTECTION PLAN OF PERSONAL DATA

CENTRE D'ESTUDIS DEMOGRÀFICS

Bellaterra, October 25, 2019

CED
Centre d'Estudis Demogràfics

HR EXCELLENCE IN RESEARCH

1. EXECUTIVE SUMMARY

This document refers to the application of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of individuals with regard to the processing and free movement of personal data and the LOPD 3/2018 of 5 December on the protection of personal data and guarantee of digital rights, by the CONSORCI CENTRE D'ESTUDIS DEMOGRÀFICS, ENTITAT PÚBLICA DE DRET PRIVAT.

The basic concepts to be taken into account according to the aforementioned Regulation (hereinafter RGPD) are as follows:

- **- Personal data:**

Any information about an identified or identifiable natural person ("the data subject"). An identifiable natural person is considered to be any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of the physical, physiological, genetic, psychological, economic, cultural or social identity of the person.

- **- Consent of the interested party:**

Any free, specific, informed and unequivocal manifestation of will by which the data subject accepts, by means of a clear affirmative statement or action, the processing of personal data that affects him/her.

- **- Processing:**

Any operation or set of operations applied to personal data, whether automated or not, i.e.: collection, recording, organisation, structuring, storage, processing, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other available means, comparison or combination, restriction, deletion, destruction.

- **- Processor:**

The natural or legal person, public authority, service or any other body that processes personal data on behalf of the data controller.

- **- Risk management:**

This is the set of activities and tasks that make it possible to control the uncertainty of a threat by means of a series of activities that include the identification and evaluation of the risk, as well as the measures to reduce or mitigate it.

The CED has worked to have a "Protocol of Privacy and Security Measures for the Personal Data of the CED", which has been supervised by a Data Protection Officer (DPD) whose function is to monitor its correct application.

The deployment required by the RGPD regulations is detailed in the aforementioned Protocol and this document, within the framework of the HRS4R strategy, summarises its most relevant aspects.

All CED staff must be aware of these regulations and follow the Protocol when designing or developing a research activity or project that involves the use of personal data.

2. INTRODUCTION

In April 2016, Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC (General Data Protection Regulation), was adopted (OJEU 4.5.2016).

The most important new feature of the new legislation is the principle of active responsibility. This means that the organisation, through all staff working with personal data, must be proactive with regard to obligations on confidentiality and risk management, and with regard to the rights of the persons concerned, through explicit clauses and consents, serving records, signed documentation, reporting possible security breaches, etc.

At the end of 2017, the CED began work on adapting to the new European regulations that fundamentally changed the management of personal data processing and the rights of individuals with respect to the legislation that would be in force from 25 May 2018, the final date for the application of the regulations.

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

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

In March 2019, the CED hired a Data Protection Delegate, who joined the team to advise on the final drafting of the "CED Privacy Protocol and Personal Data Security Measures "*.

All the required deployment is detailed in the aforementioned Protocol and this document, within the framework of the HRS4R strategy, summarises its most relevant aspects.

3. RESPONSIBLE FOR THE PROCESSING OF PERSONAL DATA

Name: CONSORCI CENTRE D'ESTUDIS DEMOGRÀFICS, ENTITAT PÚBLICA DE DRET PRIVAT

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

CIF: Q5855973C

Contact mail: personaldata@ced.uab.cat

Tel: 935813060

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

Web: www.ced.uab.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.

The processing of personal data is defined as "any operation or set of operations carried out on personal data or sets of personal data, whether by automated procedures or not, such as collection, recording, organisation, structuring, conservation, adaptation, storage, adaptation, processing and processing of personal data", the conservation, conservation, adaptation or

modification, extraction, extraction, consultation, use, communication by transmission, dissemination or any other form of enabling access, storage or interconnection, limitation, suppression or destruction".

3.2. It is the responsibility of the Data Controller:

- Apply the principles of the Regulation (RGPD) in the processing of personal data in order to guarantee and be able to demonstrate that the processing complies with the provisions of the RGPD both at the time of determining the means of processing and at the time of processing.

- Guarantee that only those personal data that are necessary are processed.

- Apply appropriate security measures in relation to the processing activities to guarantee the confidentiality and integrity of the data.

- Appoint data processors who guarantee the application of appropriate technical and organisational measures.

- Cooperate with the supervisory authority that requests it.

- Communicate the security breaches that have occurred: the person in charge to the person responsible, and the person responsible to the supervisory authority and the interested party;

- Appoint a data protection officer when necessary.

4. PERSON DELEGATED FOR THE PROTECTION OF PERSONAL DATA (DPD)

The Regulation introduces the figure of the data protection officer when the processing is carried out by an authority or public body, as is the case of the CED. The person appointed to this role at the CED was: Maria Company Jiménez, Lawyer specialising in Digital Law and Data Protection.

The data protection delegate has, among other duties, the following functions:

- Informing and advising the person responsible or in charge and the employees on the obligations imposed by data protection regulations.

- Supervise compliance with the regulations.

- Assess the impact evaluation relating to data protection.

- Cooperate with the supervisory authority.

- Act as a contact point for questions relating to processing.

Those responsible and those in charge must make public the designation of the data protection officer and their contact details and communicate them to the competent supervisory authorities.

The position of the DPO in organisations must meet the requirements that the GDPR expressly establishes: total autonomy in the exercise of their functions, the need for them to relate to the higher level of management and the obligation for the person responsible or in charge to provide them with all the necessary resources to carry out their activity.

5. CHARACTERISTICS OF THE PROTOCOL

The Protocol on the Privacy and Security Measures for the CED's Personal Data contains the definition of the basic concepts, the legal bases and the different areas of application of the regulation. There are 120 pages with the following information on the aspects summarised here, such as:

- - Àmbit d'aplicació del protocol.
- - Responsible for the processing of personal data.
- - Legal basis for data processing.
- - Data protection representative.
- - Basic concepts.
- - Register of processing activities.
- - Information to interested parties.
- - Exercise and protection of citizens' rights.
- - Data processors.
- - Non-compliance with obligations.
- - Measures, procedures and protocols to guarantee data security.
- - Impact assessment, risk management, data transfer.

5.1. Scope of application

The Regulation extends the territorial scope of application to data controllers and processors established in the EU, and when the activities of those not established in the EU are related to the supply of goods or services or to the monitoring of the behaviour of persons in the EU.

5.2. Principles

The greatest innovation of the GDPR for data controllers are 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 organisational measures in order to ensure and be able to demonstrate that the processing complies with the Regulation.

This principle requires organisations to analyse what data they process, for what purposes and what types of processing operations they carry out. Based on this knowledge, they must explicitly determine how they will apply the measures provided for in the GDPR. Likewise, they must ensure that these measures are adequate to comply with it and that they can demonstrate compliance to interested parties and supervisory authorities.

In short, this principle requires organisations to have a conscientious, diligent and proactive attitude towards all processing of personal data that they carry out.

5.2.2. El principi de “l’enfocament de risc”

Measures to ensure compliance must take into account the nature, scope, context and purposes of the treatment, as well as the risk to the rights and freedoms of individuals.

These two elements are reflected in all the obligations of the organisations. It is a deprivation by design and a deprivation by default.

The data controller must apply, both when determining the means of processing and during the processing itself, the appropriate technical and organisational measures designed to effectively apply the principles of protection and to integrate the necessary guarantees in the processing in order to comply with the requirements of the Regulation.

It must also apply the appropriate technical and organisational measures to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed.

Special categories of data

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

Biometric data: personal data obtained from a specific technical treatment, relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of this person (facial images, fingerprint data, etc.).

In-depth interviews that are carried out in the framework of some research projects also fall into this category of special data because they express opinions, describe behaviour and therefore contain information relating to ideology, sexual orientation or other sensitive data.

5.3. Consent

The GDPR requires the data subject to give consent by means of an unambiguous statement or a clear affirmative action. For the purposes of the new Regulation, 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 inactivity of the person concerned.

Consent may be unambiguous or implicit, for example, when it is inferred from an action by the data subject who decides to continue browsing a website and thus accepts the use of cookies to monitor their browsing.

Explicit consent is required in the processing of special categories of data, in the adoption of automated decisions and to make international transfers of data.

5.4. Right to information

Information is a right of the persons concerned and must include the following aspects: the contact details of the data protection officer; the legal basis for the processing; the legitimate interests pursued in which the processing is based, if applicable; the intention to transfer the data to a third country or to an international organisation and the basis for doing so, if applicable; the period for which the data will be kept; the right to request portability; the right to withdraw any consent given at any time; whether the communication of data is a legal or contractual requirement or a necessary requirement to enter into a contract; the right to lodge a complaint with a supervisory authority; the existence of automated decisions, including the logic applied and their consequences.

The RGPD stipulates that information to interested parties must be provided in a concise, transparent, intelligible and easily accessible form, in a clear and simple language.

5.5. Main rights

The GDPR incorporates the right to oblivion and the right to limitation of processing and the right to portability, as well as maintaining the rights provided for in the previous legislation, so all the rights listed below must be taken into account.

- - Access: allows the interested party to know and obtain information about the processing of their personal data free of charge.
- - Rectification: the right to guarantee the accuracy of the information processed. It allows you to correct and modify inaccurate or incomplete data.
- - Deletion: allows the elimination of data that is inadequate or excessive without interfering with the right to blocking.
- - Opposition: the right to demand the cessation or refusal of the processing of the data subject's data.
- - Limitation: the right to suspend the processing of the data subject's personal data.
- - Portability: complementary to the right of access. It allows data provided to an organisation to be obtained or transmitted directly to another entity.
- - Obligation: this is the manifestation of the rights of cancellation and opposition applied to Internet search engines. It allows you to prevent the dissemination of personal data over the Internet if certain requirements are not met.

5.6. Procedure for exercising rights

The GDPR does not establish a specific procedure for exercising rights, but it does require data controllers to ensure that procedures are visible, accessible and simple and that requests are submitted electronically, especially when processing is carried out by electronic means.

The exercise of rights must be free of charge for the interested party.

The person responsible can count on the collaboration of the persons in charge to attend to the exercise of the rights of the interested parties.

5.7. Register of treatment activities

Data controllers and data processors must document a record of the processing activities they carry out. This register must contain, for each activity, the information established in the RGPD:

- - Name and contact details of the person responsible and, if applicable, of the person jointly responsible, as well as of the data protection representative, if there is one.
- - Purposes of the processing.
- - Description of the categories of interested parties and categories of personal data processed.
- - International transfers of data.
- - Where possible, the time periods foreseen for deleting the data.
- - Where possible, a general description of the technical and organisational security measures.

5.8. - Security measures

The Regulation does not establish a list of security measures to be applied according to the type of data being processed, but rather establishes that the data controller and data

processor must apply technical and organisational measures appropriate to the risk involved in the processing.

This implies having to carry out an assessment of the risks involved in each treatment in order to determine the security measures to be implemented.

The type of analysis varies according to:

- - Els tipus de tractament.
- - The nature of the data being processed.
- - The number of stakeholders affected.
- - The quantity and variety of processing carried out by the same organisation.
- - The technologies used.

A risk analysis must be carried out to determine whether the measures implemented are correct or whether there are any shortcomings.

The specific measures to be applied must guarantee:

- The permanent confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore availability and access to personal data quickly in the event of a physical or technical incident.
- The existence of a process for regularly verifying and assessing the effectiveness of the technical and organisational measures established to guarantee the security of processing.

If a breach of security occurs, the person responsible must notify the supervisory authority within 72 hours, provided that it is unlikely to constitute a risk to the rights and freedoms of individuals.

The measures to be implemented by the CED are to keep the following documents up to date:

- - Relation of the staff
- - List of persons accessing the data
- - List of computers/servers
- - Domain
- - Computer programs
- - List of external parties that have access to the Centre's data
- - List of companies that have access to the CED

Follow up and establish a control of:

- - The security copies
- - The possible security breaches
- - The rights of users
- - The register of supports
- - The use of the equipment
- - Destruction

6. TYPES OF DATA SUBJECT TO THE NEW REGULATIONS

- Personal data: All data that allow a person to be identified: names and surnames; DNI, NIE, Passport; photo, video; e-mail address; postal address, etc.

- Sensitive data: All information that could violate the right to privacy: health data; race; sexual orientation; marital and family status; disability; opinions, etc.

In order to organise the management related to data protection regulations, it is necessary to define the different activities in which this type of information is processed. The following have been defined in the CED:

1. RESEARCH

2. TRAINING

3. TEACHING

4. COURSES, SEMINARS AND SUMMER SCHOOL

5. CONFERENCES

6. STAGES

7. CONTACTS

8. HUMAN RESOURCES

It is also necessary to distinguish whether these data are the responsibility of the CED or whether they are data for which the CED is responsible for their processing.ANNEX: Relació dels documents del Protocol de seguretat i privacitat del CED.