RESEARCH PROTOCOL AND

MANDATORY INFORMATION

FOR

RESEARCHERS OF THE MIGUEL HERNÁNDEZ

UNIVERSITY OF ELCHE

EDITION CONTROL

DATE	VERSION	PERSON RESPONSIBLE	CHANGE DESCRIPTION
17/12/2020	01	UMH Data Protection Officer	Initial edition.

CONTENTS

1. **INTRODUCTION:**

The goal of this guide is to inform about the main aspects that affect the fields of research conducted at the UMH regarding data protection, while raising awareness on this topic among the community of researchers and providing a useful tool to help research projects comply with this reference law.

It is important for the researcher to carefully study the notions, terms and explanations included, as well as the external documents (contained herein by way of links), in order to facilitate the process of preparing an application for their research project before submitting it to the Ethics Committee of the UMH for its approval.

The information included in this document is not a response to the specific circumstances of any particular research project or person. In light of the above, its purpose is to inform in a general way about the most notable and important aspects on the topic of data protection for studies, projects and research (hereinafter research) with human beings. It therefore in no case represents binding legal advice.

The applicable reference law is basically the following:

- 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 repealing Directive 95/46/EC (GDPR) General Data Protection Regulation (**hereinafter, GDPR**).

- Spanish Organic Law 3/2018, of 5 December, on Personal Data Protection and Guarantee of Digital Rights (**hereinafter, OLDPGDR**), known in Spain as the LOPDGDD.

Regarding the regulation on health and research:

- Spanish Law 14/1986, of 25 April, on General Health
- Spanish Law 33/2011, of 4 October, on General Public Health
- Spanish Law 41/2002, of 14 November, for the basic regulation of the patient's autonomy and of rights and obligations on the issue of clinical information and documentation.
- Spanish Law 16/2003, of 28 May, on the cohesion and quality of the National Health System.
- Spanish Law 44/2003, of 21 November, on the organisation of health professions.
- Spanish Law 14/2007, of 3 July, on biomedical research.
- Royal Legislative Decree 1/2015, of 24 July, approving the revised text of the Guarantees and Rational use of Medicines and Health Products Act.

If researchers need greater guidance, they may contact the Office for

Responsible Research (OIR) or the data protection officer when needed, in order to make as many queries as they view necessary to appropriately process the personal data involved in their research project.

CONTACT DETAILS	
Office for Responsible Research (OIR)	**Data Protection Officer (DPD)**
Tel no. 965222687 oir@umh.es	Tel no. 965222223 dpd@umh.es

2. WHAT IS DATA PROTECTION?

From a legal standpoint, the goal of data protection is to achieve a balance between:

(a) The data protection rights of natural persons, and
(b) the need for organisations to process such data in a legal, fair and reasonable way.

This in no way means that researchers may not process personal data while conducting their research, but it does entail assuming obligations (legal, organisational and technical) and respecting principles (security, minimisation, purpose, retention period, etc.) in order to guarantee people's rights and freedoms.

We must not forget that the right to data protection is a fundamental right, and that in the context of research there are situations that could breach it. This includes compiling health data without guarantees, using BIG DATA, artificial intelligence, etc. Therefore, although the GDPR clearly supports scientific research, it has also been created to be protectionist and safeguard the rights of persons taking part in research.

3. THE IMPORTANCE OF THE RIGHT TO DATA PROTECTION

Complying with the GDPR and the OLDPGDR is not optional, as they are part of our legal system. This means that is must be followed by the UMH in general and by the research staff in particular. In fact, breaching it can result in the UMH receiving requirements from the Spanish Data Protection Agency (hereinafter, AEPD) or any other relevant authority which can lead to sanctions proceedings, warnings, adverse publicity and civil or criminal liability. Likewise, data protection regulation makes it possible to sanction the person responsible. (Art.77 OLDPGDR).

Thus, the UMH – and in turn, its staff – must have an attitude of commitment and responsibility to the personal data it processes, including during research. Therefore, the principal investigators (hereinafter, PI),

collaborating researchers and third parties involved in research must strictly follow and comply with this regulation.

4. DOES MY RESEARCH HAVE TO COMPLY WITH DATA PROTECTION?

The GDPR and OLDPGDR are only applicable to the "**processing**" of "**personal data**" of natural persons. Therefore, if the research does not involve processing data from living individuals it would, in principle, be excluded from the application of said regulation.

On the other hand, if the research does entail said processing, the individuals performing the research must take the following matters into account:

I) Are you "processing" personal data?

"Processing" means almost any action that a research team can perform with personal data, including: gathering them; saving or storing them; recovering, consulting or using them; organising or adapting them; publishing, disseminating or sharing them; and even destroying them.

More specifically, the GDPR defines "processing" as "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."

II) Is personal data included in your research?

"Personal data" is defined as any information that refers to a natural person and which can identify that person in a direct or indirect way:

- Direct way: name and surnames, a photo, etc.
- Indirect way: an identifier, a pseudonomised code, etc.

This definition is detailed in greater depth in Opinion 4/2007 on the concept of personal data of the Article 29 Working Party (hereinafter, WP29).

Thus, by "personal data" we understand a name, an identification number, location information or an online identifier, such as an IP address or cookies. Personal data also includes referring to the features of an individual and the combination of physical, physiological, genetic, biometric, cultural or social factors.

It is often wrongly believed in the framework of certain research projects that personal data is not "processed" because no "directly identifiable" data is

requested, such as the name, surnames or a photo of the person. However, if the project provides a high probability of identifying a specific person (without requiring excessive effort), this enters the scope of the concept "personal data", and the data protection regulation would be applicable.

In surroundings that gather large amounts of data, where OPEN DATA techniques or BIG DATA technologies are used, in principle, the data may seem non-personal. However, there is a distinct possibility of aggregating them and re-identifying them.

An example would be the "combination of identifiers". In this case, at first glance, the range of available identifiers would not, in principle, make it possible to identify a specific person. However, if said information is combined, there would be a high probability of identifying an individual from a group of people without too much effort.

Examples:

> Example 1: Unique features: "The rector of the UMH" or a class where data is gathered from students and their age is requested. If there is just one person who is 65 years old, they could already be identified from the group.
>
> Example 2: A combination of details that identify an individual: in a supposedly anonymous poll, respondents are asked about their age range, job position and place of work (the likelihood of identifying a specific person is very high).

On the other hand, we have to consider **the format or medium that has the relevant information.** Thus, the concept "personal data" includes information available in any way, whether alphabetical, numerical, graphical, photographic, acoustic, etc. including physical (on paper) and/or digital information.

Personal data may come from any type of research activity:

Lifestyle
Health
Genetic records
Education
Behaviour records
Samples, tissues, DNA
Location and tracking (geolocation, etc)
Physical attributes
Economic characteristics,
Etc.

- **Anonymous data.**

We have already established that the ability to identify a person is decisive in order to establish the existence of processing. Thus, if said identification is not possible, the regulation on data processing shall not be applicable.

Example: Completely anonymous polls (those that do not gather any piece of data that may directly or indirectly identify an individual) are considered outside the scope of application of the data protection regulation.

- **Anonymisation. Anonymisation techniques.**

Researchers can resort to the various anonymisation tools in order to safeguard the identity of research individuals.

Article 3 of Spanish Law 14/2007 on Biomedical Research establishes the following concepts:

- "Anonymisation": the process whereby it is no longer possible to establish a connection between a piece of data and the individual it refers to by reasonable means. This is also applicable to biological samples.

- "Anonymous data": data registered without a connection to an identified or identifiable person.

- "Anonymised or irretrievably unlinked data": data that cannot be linked to an identified or identifiable person as a result of destroying the connection along with all the information that identifies the individual, or because of said association requiring an unreasonable effort, understanding as such the use of disproportionate amounts of time, expense and work.

The AEPD understands anonymisation as "breaking people's chain of identification", whose purpose is "to remove or decrease the risk of re-identification of the anonymised data". In other words, making it impossible to link anonymised data to a specific person.

Therefore, if the use of anonymisation techniques is considered within the framework of a research project, a study must be performed on the risks of re-identification or the likelihood of the data being linked to a specific natural person. This could happen due to the following circumstances, among others:

- loss of information
- lack of a suitable anonymisation protocol
- lack of diligence of the staff involved

To do so, there must be several working teams that are independent from one another, which will perform the following activities, among others:

- Assessing risks that may derive from the anonymisation
- Establishing the suitable techniques
- Complying with and monitoring the necessary safety measures to preserve anonymisation
- Etc.

In this sense, the AEPD has published a specific guide[1] to perform the anonymisation, a technical note on "k-anonymity"[2] with guidelines for the organisations that use Big Data and artificial intelligence processes to process data, which includes a series of software tools[3] that make it possible to anonymise sets of data in an efficient way.

Despite the above, and in the current framework, anonymisation techniques are being put into question[4], as several studies conclude that zero risk does not exist, as there are techniques (such as quantum computing) that make it possible to revert the process and find out the identify of the people who are behind said data and whose privacy is trying to be protected.

- **Pseudonomysed data**

Pseudonymisation is defined as the act of concealing the identity of the natural persons that the research refers to. This usually entails eliminating the data that identify them and using a pseudonym (often a number assigned at random), so that data can be continuously gathered from the same person without recording their identity. The purpose is to minimise the risk of the data subject being identified to the extent possible.

Main elements:

- The likelihood of the data subjects being indirectly identified is very high.
- It is a very useful security measure, but not an anonymisation method.
- Processing data in a pseudonymised way does not eliminate the need to comply with data protection regulation.

According to the GDPR, this is "information that, without including an individual's denominative data, makes it possible to identify them with additional information, as long as the latter is kept separately and is subjected to technical and organisational measures aimed at ensuring the personal data is not attributed to an identified or identifiable natural person". **Thus, pseudonymised data is considered personal data and its processing would entail complying with the regulation.**

Pseudonymisation can be done by some of the following procedures, among others:

.

- By coding the information. This code can be reverted with its decryption key.

---

1 See Guidelines and guarantees of the data anonymisation procedures (in Spanish)
2 See https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf
3 ,ARX Data Anonymization Tool ,UTD anonymisation tool Amnesia and Amnesia online
4 https://www.nature.com/articles/s41467-019-10933-3

- When the information is stored under a randomised number that has no relation to the original information
- Replacing figures and codes with words
- Exchanging a random number with a set of data

In this regard, the European Union Agency for Cybersecurity (ENISA) has published a report on the main scenarios and procedures on the topic of pseudonymisation[5].

There is the erroneous belief of using the I.D. number as a code. This method would in no way be considered a pseudonymisation technique.

Meanwhile, when pseudonymised data is received or supplied to third parties without the means to identify the individuals, the efficiency of the pseudonymisation will depend on a series of factors (for example, security against backward tracing and the size of the population that includes that person).

The essential difference between anonymisation and pseudonymisation is that, in the former, the identifiable data is totally dissociated from the personal data in an **IRREVERSIBLE** way. In pseudonymisation, the identifiable data is decoupled, but additional pseudonymised data that can re-identify the data subjects are preserved, making it a **REVERSIBLE** process.

Article 89.2 of the GDPR establishes that, on the issue of processing for the purpose of filing for public interest, for scientific and historical research purposes or statistical purposes, there must be technical and organisational measures implemented to guarantee the principle of data minimisation, including pseudonymisation **to the extent possible to achieve the goals.**

- **Aggregated or statistical data**

Aggregated data is part of the process of combining information on several data subjects in broad classes, groups or categories, making it impossible to distinguish the information connected to them. This means that the data must not be personal, and its efficiency will depend on factors such as the size of the population that includes that person, or whether the original sample is large enough. Therefore, the research team must be careful when classifying it as "aggregated data", because in some cases it can be considered identifiable personal data.

- **Biometric data, DNA and human tissue samples**

The GDPR understands as biometric data that which refers to the physical, physiological or behavioural attributes of a person which allow or ensure

5 https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/at_download/fullReport

Their unique identification.

Biometric data is characterised by having three elements:

It is universal: it is present in all people without distinction.
Unique: they differentiate each individual.
Permanent: it is always present.

There are three main types of biometric data:

- Data that refers to physical and physiological aspects: digital fingerprints, analysing an image of the finger, iris or retina, facial recognition, results from samples from the hands, recognition of the shape of the ear, detecting body odour, voice recognition, an analysis of DNA samples, analysis of skin pores, etc.

- Data based on behavioural aspects that measure a person's behaviour, including analysing the handwritten signature, analysing how they hit the keys when typing, analysing gait or the way of moving, patterns that denote subconscious thoughts such as lying, etc.

- Data obtained from techniques based on psychological elements, including the response to specific situations or specific tests that fit a psychological profile.

However, "human tissue samples" are not considered biometric data in themselves, but a source from which it can be extracted. In other words, extracting information from samples can lead to gathering personal data.

According to the AEPD, in its Opinion 36/2020, "biometric data would only represent a special category of data if subjected to specific technical processing aimed at unequivocally identifying a natural person". Recital 51 also reflects this statement.

Thus, as regards Opinion 3/2012 on the evolution of biometric technologies of WT29, it differentiates between:

- Biometric identification: identifying an individual through a biometric system is usually the process of comparing their biometric data (acquired upon identification) with a series of biometric templates stored in a database (in other words, a one-to-many search for matches).

- Biometric verification or authentication: identifying an individual through a biometric system is usually the process of comparing biometric data (acquired upon verification) with a single biometric template stored in a device (in other words, a one-to-one search for matches).

The AEPD says that, according to this distinction, the concept of biometric data would include both cases, identification and

Verification or authentication. However, in general, only cases of biomedical identification (one-to-many) will be considered part of the special category.

- **Photographs, videos and sound recordings**

Researchers must be aware that the existence of photographs, videos and sound recordings of people (regardless of whether these people voluntarily reveal information or not) in an investigation represent information about said people which identifies them. Therefore, its processing must meet data protection obligations.

- **Special category data**

The GDPR defines this type of data as that which, due to its nature, is particularly sensitive and therefore **deserves special protection, because processing it could entail a significant risk for fundamental rights and freedoms.**

Said data includes the following:
- that which reveals ethnic or racial origin,
- political opinions,
- religious or philosophical beliefs
- or trade union membership,
- and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- or data concerning the sexual life
- or sexual orientation of a natural person.

In this sense, proper consideration must be given to processed data that may indirectly reveal a person's special category data.

Example 1: Photographs and names can give a clue as to a person's race or religious beliefs. However, this does not mean that they are always considered special category data because of this assumption. The issue will arise if the information is processed based on those assumptions or not (for example, grouping people based on their skin colour or the probable ethnic origin of their attributes).

Example 2: There are methods that are clearly apt for obtaining these types of data. For example, interviews where a person can reveal a lot of information, or forms with open questions that allow the person to write what they wish.

- **Data from minors**

In principle, data relative to minors is not considered special category data. However, given their vulnerability due to their youth and lack of experience, the regulation establishes special protection because of the

lack of knowledge on the repercussions of processing their data.
Depending on the characteristics of the research, special attention must be paid to the intervention of their legal representatives.

Thus, in general, research with invasive data must obtain the consent of the legal representatives as well as the minor's consent if they are over 12 years of age.

Persons over the age of 14 may give their consent to take part in research with non-invasive data, which relegates the consent of legal representatives to under-14s (along with the minor's consent, as they are over 12 years of age).

- **Data on sentences and criminal offences**

The GDPR establishes that processing this type of data may only be done under the supervision of public authorities or when authorised by Union or Member State law which establishes suitable guarantees for the rights and freedoms of the data subjects.

As a result, said data may only be processed by governments, even if they have been obtained from sources available to the public.

The OLDPGDR also adds the following points:

- ·A full record of personal data on sentences and criminal offences, as well as related protective and safety measures and procedures, may be created pursuant to the regulation of the Administrative record system for the support of the Justice System.

- Outside the mentioned cases, it may only be possible when conducted by lawyers and legal representatives whose goal is to compile information provided by their clients to carry out their duties.

III) Who is responsible for complying with the GDPR? ¿The PI? Other figures: Data processor, Joint controller, Data addressee.

Data controller (DC)

In data protection, the DC is defined as the person or organisation which, (alone or jointly with others) determines the purposes and means of the processing of personal data.

In essence, it is the figure who answers the following question: Do you control and define the use of the personal data?

Data processor (DP)

The person or organisation who processes the data on behalf of the data controller. In this case, the processed data belong to the DC and their access to them is exclusively defined by the service, work or process to conduct as requested by the DC.

They would answer the following matter: Are you acting in accordance with the instructions of another person or organisation?

If we situate this in the framework of the university, and specifically in the framework of research projects, the UMH will likely be the DC and there may be third party organisations (or people) who are commissioned certain tasks in order to conduct the research, such as contracting a data centre to host the research data, making them the data processors.

There may also be cases where the UMH acts as the DP, when a researcher collaborates in research whose initiative and control belong to third parties and who is assigned certain duties or tasks but is not part of the research (for example, those formalised in the framework of article 83 of Spanish Organic Law 6/2001, of 21 December, on Universities).

Joint Controllers (JC)

In practice, this situation occurs when there are two (or more) organisations that decide and collaborate by jointly establishing the purposes and processing method (the research). In this case, said organisations take on the role of joint controllers.

This means that there is a general level of complementarity and unity of purpose. To this end, in principle it is not necessary for all joint controllers to execute all operations included in the research. In other words, they may interact in several processing operations while conducting others by their own means and purposes.

If this situation occurs, the responsibilities of each joint controller regarding the research must be clearly assigned before the data subjects.

According to the CRUE guide on personal data protection in the university environment during COVID-19:

> "In principle, there may be two theoretical situations:
> • on one hand, if there is a leading entity, then it shall be the data controller, whereas the rest must sign a data processor agreement (as they will process data on behalf of the controller);

- on the other hand, if there is no sole leader because the entities jointly

establish the goals and the data processing methods, then they shall all be joint controllers and must sign an agreement to this effect."

Data addressee (DA)

Sometimes, the data must be communicated to another organisation (natural or legal person or entity). For example, when a law establishes said communication. In this case, the data subject must be expressly informed of said communication.

In any case, if the collaboration of a third party is required during a research project, the PI must address the OIR to receive guidance, as the relationships with other organisation or people must be formalised through specific agreements or contracts.

Thus, whether the university is the DC or becomes the DP or JC, **the PI is the internal person responsible** regarding the role fulfilled by the university, as there is a binding working/statutory relationship between them and the UMH. Thus, the PI must act in accordance with the instructions on data protection included in the relevant data protection regulation, this document and any other applicable regulation or documents at the UMH.

5. DUTIES AND OBLIGATIONS

I) Principles of data protection

This section is one of the most important of the regulation on the issue of data protection (art. 5 GDPR), as it establishes the criteria to follow when processing personal data:

i.- It shall be processed **lawfully, fairly and in a transparent manner.**

ii.- It shall be collected for **specified, explicit and legitimate** purposes, and shall not be processed in a manner that is incompatible with said purposes (however, further processing for scientific or historical research purposes shall not be considered incompatible with the initial purposes).

iii.- It shall be **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed.

iv.- It shall be **accurate** and, where necessary, **kept up to date.**

v.- **It shall not be stored** as identified data for longer than is necessary for the purposes concerned.

vi.- It shall be processed with a guarantee of **security,** including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical

or organisational measures.

i.-Lawful, fair and transparent processing

Lawful processing: This principle entails that researchers initiating a research project must consider how it could affect the rights and freedoms of the research subjects before it begins. After doing so, they must weigh the use of personal data and the interest of the project, especially if said project may damage the data protection right of the data subjects. In this case, the researcher would have to prove that said damage is justified.

The legality is evidently also tied to transparency and to the ability of the person to refuse having their data processed.

Fair processing: Data processing must have a legitimate basis (a legally acceptable reason for processing the data), which must be substantiated by the DC and effectively conducted by the PI.

Legitimate basis for personal data

According to article 8 of the Charter of Fundamental Rights of the EU, "such data must be processed fairly for specific purposes and **on the basis of the consent of the person concerned or some other legitimate basis laid down by law.**

The GDPR establishes six possible legal foundations on which to legally base the processing:

a) Consent – this legal basis entails reliably obtaining the consent of the data subject directly or indirectly by way of a third party who is a contributor to the research project.

In this sense, the European Data Protection Board (hereinafter, EDPB) stated that, in certain cases in the framework of research (especially regarding clinical trials), there can be an imbalance between the parties. This can cause the requirements established by the GDPR for the consent to be valid not to be met (the free, 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, signifies agreement to the processing of personal data relating to him or her).

Thus, the research team must assess the existence or lack of said imbalance.

b) The processing is necessary to **execute a contract** that the data subject is a part of.

c) **Vital interest of the data subject** – The processing will be fair when it is necessary to protect the vital interests of the data subject or of another natural person.

e) Public interest – Research conducted at the university can be considered as necessary for the performance of a task carried out in the public interest in connection with article 1 of Spanish Organic Law 6/2001, of 21 December, of Universities [6].

f) The processing is necessary to **fulfil legitimate interests.** (does not apply to governments)

The legal bases preferentially applicable in the framework of research conducted at the university, as a public body, are:

a) Consent,

e) public interest.

In the case of special category data (sensitive data)

In the context of a university, it is very common for there to be research that processes data not only concerning health but of other very sensitive types such as vulnerable groups, from gender-based violence victims, genetic or biometric data, etc.

As previously mentioned, special category data is regulated in article 9 of the GDPR. The following are classified within this group:

- Data that reveal the ethnic or racial origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic data,
- Biometric data,
- Data concerning health,
- Data concerning a natural person's sex life or
- Sexual orientation.

The GDPR establishes **a general ban** on the processing of such sensitive data, except for the exceptions defined in article 9 of the GDPR and which are applicable to research.

Therefore, to use sensitive data in research, as well as identifying a legal basis for processing it in research (as mentioned in the

[6] Art. 1.1 of the Spanish Organic Universities Act (L.O.U.) "The university carries out the public service of higher education through research, teaching and study".

previous section, consent or public interest), the ban on processing sensitive data must be "lifted" through any of the following exceptions:

Explicit consent – Apart from the characteristics assigned to consent by the GDPR[7], in the case of processing sensitive data, said consent is required to be explicit. This means that the consent and prior information must be provided individually for each specific research, study or project, or at least for certain scopes or fields[8] (if it cannot be defined by the type of research at that time), especially in research concerning health[9].

Thus, the research team must obtain explicit consent to use special category data. This means that it must be provided in an express declaration for this purpose ("I give my consent for my data to be processed for…") Or through "double opt-in" mechanisms in digital processing. (article 9.2.a GDPR).

As mentioned, it must be verified that the person who takes part in the research **is not in a situation of imbalance** with regards to it (in bad health conditions, belonging to economically or socially weak groups or in a situation of institutional hierarchy, etc.), in which case other legal bases would have to be sought.

Furthermore, research participants have the right to withdraw their consent at any moment in this case, meaning that the main PI would have to immediately delete the personal data of the project, study or research if a request for withdrawal is submitted.

Substantial public interest: processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the

7 Art.4.11 GDPR "…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, signifies agreement to the processing of personal data relating to him or her."

8 Recital 33 GDPR: "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

9 Seventeenth additional provision, section 2d: The processing of data in research concerning health shall be governed by the following criteria: The data subject or, where relevant, their legal representative, may award the consent to use their data with health research purposes – biometric data in particular. Said purposes may include categories related to general fields linked to a medical or research speciality.

aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (9.2.g GDPR) (According to the OLDPGDR it must be covered in a requirement with the status of law).

Medical purposes - this context includes the purposes of preventive or labour medicine, assessing the working capacity of an employee, medical diagnosis, providing health care and treatment and managing health services. The condition applies when the processing is performed **by virtue of an agreement with a health professional.** (Researchers must take into account that the definition of health professional is very restrictive); This exception will be applicable as long as the processing is performed with suitable guarantees. (article 9.2.h GDPR) (According to the OLDPGDR it must be covered in a requirement with the status of law).

Public interest: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (art. 9.2.I) (According to the OLDPGDR it must be covered in a requirement with the status of law).

Processing is necessary for archiving purposes in the public interest, **scientific or historical research purposes** or statistical purposes in accordance with Article 89[10] based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (9.2.j)

9.2.A or 9.2.j are usually preferentially applied in the framework of projects, studies and research

[10] Art.89.1 GDPR: Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

performed at the university (explicit consent and/or scientific research purposes).

Sensitive data, especially concerning health

When data concerning health or biomedical data are processed in the framework of research, in order to apply exception 9.2.j. we must look at the seventeenth additional provision of the OLDPGDR, which includes the state regulation that enables the processing:

- Spanish Law 14/1986, of 25 April, on General Health.
- Spanish Law 31/1995, of 8 November, on the Prevention of Occupational Hazards.
- Spanish Law 41/2002, of 14 November, for the basic regulation of the patient's autonomy and of rights and obligations on the issue of clinical information and documentation.
- Spanish Law 16/2003, of 28 May, on the cohesion and quality of the National Health System.
- Spanish Law 44/2003, of 21 November, on the organisation of health professions.
- Spanish Law 14/2007, of 3 July, on biomedical research.
- Spanish Law 33/2011, of 4 October, on General Public Health
- Spanish Law 20/2015, of 14 July, on the organisation, supervision and solvency of insurance and reinsurance entities.
- The consolidated text of the Guarantees and rational use of the 105 medicines and healthcare products act, approved by Spanish Royal Legislative Decree 1/2015, of 24 July.
- The consolidated text of the General act for the rights of people with disabilities and their social inclusion, approved by Spanish Royal Legislative Decree 1/2013, of 29 November.

Research with pseudonymised data

Projects, studies and research can be performed by accessing pseudonymised data.

This is based on the seventeenth additional provision of the OLDPGDR, substantiated on article 9.2.j of the GDPR in connection with article 89.1, regarding when processing is necessary for the performance of a task carried out in the public interest (art. 6.1. e GDPR).

To be able to use pseudonymised data in specific research, we must fulfil certain guarantees:

1. Technical and functional separation of the research team and those performing the pseudonymisation and who store the information that enables

identification.

2. The pseudonymised data may only be accessible to the research team when:
    a. There is an express commitment of confidentiality and to not perform any re-identification activity.
    b. Specific security measures are implemented to prevent re-identification and the access of unauthorised third parties.

Likewise, section f establishes that the following actions will be performed pursuant to article 89:

1.-An impact assessment that establishes the risks derived from processing in the cases established in article 35 of the GDPR.

2.-Subject scientific research to the quality standards and, where relevant, the international guidelines on good clinical practice.

3.-Adopt, where relevant, measures aimed at ensuring that researchers do not access the identification data of the data subjects.

4.-Appoint a legal representative established in the European Union pursuant to article 74 of Regulation (EU) 536/2014, if the clinical trial sponsor is not established in the European Union. Said legal representative may coincide with the person established in article 27.1 of Regulation (EU) 2016/679.

On the other hand, section g) establishes the obligation to subject research with pseudonymised data processing to a prior report by the research ethics committee.

Principle of lawfulness overview:

In summary, the lawfulness of processing in research will depend on the following conditions:

- If general data is processed (without special categories of data)

- If general data + special categories of data (not concerning health or biomedical) are processed

- If general data + special categories of data concerning health and biomedical data are processed

- If research is performed with pseudonymised data.

1.- General data

DATA	LEGITIMATE BASIS	REQUIREMENT	EXCEPTION	LAW	GUARANTEE
PERSONAL DATA	CONSENT ART. 6.1.a GDPR	EVIDENCE of being freely given, specific, informed and unambiguous in a statement or clear affirmative act.	N/A	N/A	**EVIDENCE** of the consent awarded by the participant If possible, by type of research: Pseudonymisation of identifying data (fulfilling the principle of data minimisation)
	PUBLIC INTEREST. ART. 6.1.e GDPR	APPLICABLE LAW: L.O.U. Artl1 Research purpose	N/A	N/A	If possible, by type of research: Pseudonymisation of identifying data (fulfilling the principle of data minimisation)

2.- Special category data NOT CONCERNING HEALTH OR BIOMEDICAL DATA

DATA	LEGITIMATE BASIS	REQUIREMENT	EXCEPTION	LAW	GUARANTEE
SPECIAL CATEGORY DATA: NOT HEALTH OR BIOMEDICAL DATA: - ETHNIC OR RACIAL ORIGIN -POLITICAL OPINIONS RELIGIOUS OR PHILOSOPHICAL BELIEFS TRADE UNION MEMBERSHIP BIOMETRIC DATA NOT HEALTH SEX LIFE SEXUAL ORIENTATION. SENSITIVE DATA: GENDER-BASED VIOLENCE, DISABILITIES, ETC.	CONSENT ART. 6.1.a GDPR	EVIDENCE of being freely given, specific, informed and unambiguous in a statement or clear affirmative act	EXPLICIT CONSENT Art. 9.2.a	L.O.U. Art.1 Research purpose	. EVIDENCE of explicit consent Awarded by the participant. If possible, by type of research: Pseudonymisation of identifying data (fulfilling the principle of data minimisation)

3.- Special category data CONCERNING HEALTH OR BIOMEDICAL DATA

DATA	LEGITIMATE BASIS	REQUIREMENT	EXCEPTION	LAW	GUARANTEE
SPECIAL CATEGORY DATA: CONCERNING HEALTH AND BIOMEDICAL DATA	CONSENT ART. 6.1.a GDPR	EVIDENCE of being freely given, specific, informed and unambiguous in a statement or clear affirmative act	EXPLICIT CONSENT Art. 9.2.a	N/A	If possible, by type of research: Pseudonymisation of identifying data (fulfilling the principle of data minimisation)
	PUBLIC INTEREST	APPLICABLE LAW: L.O.U. Research purpose	RESEARCH PURPOSES Art. 9.2.j	SEVENTEENTH ADDITIONAL PROVISION OLDPGDR as long as any of the following laws are applicable: SPANISH LAW 41/2002 SPANISH LAW 16/2003 SPANISH LAW SPANISH RD 1/2015 LEGISLATIVE SPANISH RD 1/2013	**Seventeenth Additional Provision** section f in relation with article 89.1 - Perform an impact assessment - Subject the research to quality standards and, where relevant, to the international guidelines on good clinical practice. - Adopt, where relevant, measures aimed at ensuring that researchers do not access research data. - In international transfers, appoint a legal representative based in the EU. Data pseudonymisation

4.- Special category data PSEUDONYMISED DATA

DATA	LEGITIMATE BASIS	REQUIREMENT	EXCEPTION	LAW	GUARANTEE
SPECIAL CATEGORY DATA: CONCERNING HEALTH AND BIOMEDICA DATA: **PSEUDONYMISED DATA**	PUBLIC INTEREST: ART. 6.1.e	APPLICABLE LAW: L.O.U. Research purpose	Art. 9.2.j	SEVENTEENTH ADDITIONAL PROVISION OLDPGDR as long as any of the following laws are applicable: SPANISH LAW 41/2002 SPANISH LAW 16/2003 SPANISH LAW 44/2003 SPANISH LAW 14/2007	**Seventeenth Additional Provision** **Section d.** The use of pseudonymised personal data is considered legal for the purposes of research concerning health and, in particular, biomedical research. technical and functional separation - pseudonymised data only accessible to researchers when there is a commitment of confidentiality and to not re-identify, and when security measures are implemented to prevent re-identification **section f** in relation to article 89.1 - Perform an impact assessment - Subject the research to quality standards and, where relevant, to the international guidelines on good clinical practice. - Adopt, where relevant, measures aimed at ensuring that researchers do not access research data. In international transfers, appoint a legal representative based in the EU **section g:** Prior report by the Ethics committee.

Researchers must take into account that each of the above conditions are in addition to any condition established by the relevant entity for the ethical revision and approval.

Transparent processing:

Data obtained directly from the participants:

Clear, open and transparent language must be used when gathering personal data, laying out what will be done with their data.

Specifically, the GDPR says they must receive the following information:

- The name of the data controller or controllers (in other words, the university and the eventual joint owners or joint controllers of the data, where relevant, and the person who has been appointed to protect the data;
- the purposes for which the data will be processed,
- the legal basis for the processing;
- the addressees or addressee categories with whom the data will be shared or may be shared.

- Where relevant, the fact that the data will be transferred outside the European Economic Area ("**EEA**") and the safeguards that will be applied to said transfer;

- the amount of time the data will be stored for or, if this is not possible, the criteria that will be used to establish the retention period;

- if the processing is based on consent, the right of the data subject to withdraw their consent at any time; and

- the rights of the data subjects by virtue of the GDPR (right to access, rectify and erase their data, the right to oppose the processing, the right to submit a claim before the AEPD).

In research, this information is usually provided as a privacy or information notification for the data subject.

Researchers must ensure that *all* data subjects (or where relevant, mothers/fathers or tutors of underage data subjects) receive the correct stipulated information.

The fact that said information is provided in writing or is made available to the data subjects any other way will depend on the nature of the project and on the usefulness of said format for the data subjects.

In any case, the information must be provided in an easy way, avoiding unnecessary jargon, and there must be a record that said information has been delivered, especially if the stipulated information is read out to the data subjects.

Data not obtained directly from the participants:

In the framework of research, gathering the personal data of data subjects is often done through other research projects or external organisations.

In these cases, the obligation of transparency remains, and the listed information must be equally provided to each of the data subjects, as detailed above, but with the following additional information:

- the categories of personal data that will be processed; and
- the source of the personal data, and if they come from public sources.

However, the information does not have to be provided if the data subjects already have the information; or if doing

so is impossible or would entail a disproportionate effort; or would hinder or severely affect achieving the research goals. These specific cases must obviously be appropriately justified and approved by the Ethics Committee.

If special category data is processed, particularly biomedical data or data concerning health, the OLDPGDR establishes in additional provision seventeen that, if data is reused in research, "the controllers must publish the information in an easily accessible section of the corporate website of the centre where the research or clinical study is conducted and, where relevant, of the sponsor, and to communicate the existence of this information to the data subjects by electronic means. If the latter cannot access said information, they may request it be sent in another format." A prior favourable report by the Research Ethics Committee is required for this processing.

ii.-Obtained for specified, explicit and legitimate purposes

This data protection principle is directly related to transparency and to the requirement of providing people with the stipulated information.

When the researcher obtains personal data for a specific purpose, its use should, in principle, not be allowed for other purposes (in other words, "further processing") that are incompatible with the initial purpose. However, the GDPR establishes that the further processing of data **for research purposes** is considered compatible with the initial purpose for which the data was gathered.

As was mentioned above, the OLDPGDR establishes in additional provision seventeen that "the reuse of personal data for research purposes concerning health and biomedicine shall be considered lawful and compatible when, having obtained consent for a specific purpose, the data is used for purposes or fields of research connected to the field that the initial study belonged to."

In this case, the controllers must publish the information in an accessible part of the corporate website of the centre where the research or clinical study is performed and, where relevant, of the sponsor, as well as notifying the existence of said information via electronic means (or other formats in their absence) to the data subjects.

iii.-Appropriate, relevant and limited to what is necessary for the purposes concerned (data minimisation)

The goal of this principle is to prevent gathering unnecessary data.

If we consider the sensitivity assigned to personal data, it can be deduced that no organisation should have personal data they do not need. Legislation also establishes the obligation to guarantee that said data are suitable for the research purposes.

This principle of data minimisation is considered one of the most important by the GDPR and is applied not only when gathering data, but throughout their life cycle (how to access, process or share them, the reason for using them, destroying them, storing them, etc.). For example, it may be necessary for all the members of the research team of collaborators to have access to all the data, and it may be possible to provide said data to them in an anonymous or pseudonymised way.

Accessing personal data must be limited to people with a legitimate need to know them. Researchers should ask themselves whether it is necessary to use personal data in their research or whether they could meet their goals with anonymous, aggregated or pseudonymised data.

iv. **Accurate and, where necessary, up to date**

This principle is directly related to the previous one, as data that are not up to date can stop being suitable and relevant for the purposes for which it is going to be processed.

All reasonable measures must be implemented to guarantee that inexact data, considering the purposes for which it is being processed, are deleted or rectified without delay.

However, we find there are many cases of research projects with static files which, if updated, would defeat the purpose for which they were gathered. In these cases, it is understood that researchers do not have to keep their personal data updated. This situation must be documented and justified.

v. **They shall not be stored as identifiable data for longer than is necessary for the purposes concerned**

Like the previous one, the principle of data storage is directly linked to the principle of relevance and suitability in accordance with the purposes[11]. If personal data are stored in an identifiable way for longer than necessary, they may not be relevant and suitable.

During that time, the personal data should be stored, if possible, in an electronic medium that makes it possible to block the data

(entirely and with no modifications).

vi. **Security guarantee**

The GDPR implements a security system based on proactive responsibility which establishes that it is the controllers and/or processors who shall implement the suitable technical and organisational measures to guarantee the security of the personal data.

As a result, the PI and researchers/collaborators are to adopt suitable technical and organisational measures to protect the personal data from their unauthorised or illegal processing and from their loss, destruction or accidental damaging.

Specifically, the GDPR says the following: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

"In any case, it is essential, taking into account the processing nature, scope, context and purposes, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, for the research team to implement the suitable technical and organisational measures to guarantee a suitable level of security for the risk detected. These measures, in the scope of public universities, must be in line with those included in the National Security System (ENS, in Spanish) (first additional provision of the OLDPGDR).

Likewise, on the issue of security, "all researchers must know that even more important than general security measures are the individual and specific security measures that must be implemented by all researchers to protect personal data"[12].

II) Other principles and obligations.

i. Accountability principle

This principle is included in article 5.2 of the GDPR and represents an essential concept for the document.

It is defined as the requirement (enforceable) for the DC to implement appropriate technical and organisational measures to guarantee and **be able to demonstrate** that the processing of personal data complies with the regulation.

Essentially, it entails that it is not enough to comply with data protection regulation, as researchers must be able to prove to third parties that they are complying with it.

In order to comply with the accountability principle, the GDPR lists a series of mandatory measures for the DC through which they can prove they are complying with the regulation, and which, in the specific framework of research at the UMH, are listed in this document (measures for protecting data by design and by default, registering processing activities, assessing the impact on data protection, communicating security breaches, etc.).

ii. Privacy by default and by design.

The GDPR includes these principles in its article 25.

Regarding research projects, technical and organisational measures must be applied in the first phases of the processing activities so that they guarantee the privacy and data protection principles from the onset (**data protection by design**).

Principles of privacy by design[13]

1. Proactivo, no reactivo; Preventivo, no correctivo
2. La privacidad como configuración predeterminada
3. Privacidad incorporada en la fase de diseño
4. Funcionalidad total: pensamiento "todos ganan"
5. Aseguramiento de la privacidad en todo el ciclo de vida.
6. Visibilidad y transparencia
7. Enfoque centrado en el sujeto de los datos

[12] Guide on the protection of personal data in the scope of university in times of COVID-19.
[13] Guide on privacy by design of the AEPD. Table 1. Page 5

The use of pseudonymisation and encryption techniques are examples of measures to implement under this principle.

On the other hand, from the viewpoint of **privacy by default**, we must guarantee that personal data are processed with the highest level of privacy protection. In other words, under the same prism as the data minimisation principle, and taking into account criteria on suitability, relevance and need with regards to the purposes when designing the different processing phases (measures to take into account on the amount of personal data gathered, the extent of the processing, the retention period or the accessibility of the data).

The AEPD has produced a "Guía de Privacidad desde el Diseño" ("Guide of Privacy by Design")[14], and a "Guía de Privacidad por Defecto" ("Guide of Privacy by Default")[15], which detail and explain these principles.

iii. **Security breaches.**

The GDPR defines "personal data breaches" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

The term "breach" entails more than a simple security incident. In other words, it must compromise the DC regarding compliance with the GDPR principles and must also entail risks for the rights and freedoms of the data subjects.

The GDPR imposes an obligation on the DC to notify the AEPD of any personal data breach in no more than 72 hours, which entails that the researcher must issue the corresponding notification to the DC or the DPD of the UMH as soon as they are aware of it, in order to comply with this obligation.

Thus, if there is a security breach within a research project that entails a risk for the rights and freedoms of natural persons, it must be immediately notified to the university, as the data controller, in order to notify, where relevant and in due time and proper form, the AEPD and the data subjects (where appropriate).

The AEPD has published a specific tool[16] that can be of great help to know when a certain event can entail a high risk to the rights and freedoms of natural persons, and therefore, can represent a security breach.

iv. **Impact assessment.**

The General Data Protection Regulation (GDPR) introduces the concept Impact Assessment relative to Data Protection (DPIA) in its article 35[17].

---

14 https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf
15 https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

16 https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd
17 Art. 35.1 GDPR: Where a type of processing in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing,

A DPIA is a process to analyse[18] and describe in a preliminary and early way a type of personal data processing that is likely to result in a high risk to the rights and freedoms of natural persons, specifically assessing the origin, nature, particularity and severity of the risk.

When can my research involve a type of personal data processing that is likely to result in a high risk to the rights and freedoms of natural persons?

Data processing is considered to entail a high risk to the rights and freedoms of research data subjects when there is profiling, the systematic monitoring of individuals or large-scale processing of special category data, or when intrusive data processing methods are used (such as monitoring, surveillance, audio and video recording, geolocation tracking, etc.).

In any case, the AEPD has published a list[19] with the types of processing that require a DPIA. Following these criteria, and considering the cases listed, a DPIA must be performed if two or more are present. That being said, due to the characteristics that are usually present in research projects, there is a high probability that a DPIA must be performed, especially for data concerning health.

To help perform the DPIA, the AEPD has produced a tool to perform data protection impact assessments:

https://gestiona.aepd.es – Evaluación de impacto (Impact assessment).

The following documents of interest must be taken into account in order to provide more information on the DPIA.

Data protection impact assessment report template for public administrations (in Spanish)

Impact Assessment Guide of the AEPD (in Spanish)

Documents of the European Data Protection Board on DPIA

More information (in Spanish)

In this case, you can request the advice of the Data Protection Officer in order to

---

carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

18 Art 35.5 GDPR A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
a) 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 natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
c) a systematic monitoring of a publicly accessible area on a large scale.

19 https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

fulfil this obligation.

v. Records of Processing Activities (RPA)

Art. 30 of the GDPR establishes the requirement for the controller to maintain a record of processing activities under its responsibility, as well as the processor when acting in this role.

The UMH has included research projects as processing activity in its Registry on a general level. Despite the above, and in the interest of complying with the principle of proactive responsibility, each PI must inventory the research project to catalogue it as supplementary to the general one. As part of the protocol for the authorisation of a research project by the Ethics Committee, an RPA template will be provided to the PI to fill it out.

vi. International data transfers

If the research requires international data transfers to countries outside the European Economic Area, guarantees of compliance with the legal system established in the data protection regulation must be filled out and supplied. (Articles 44 to 50).

Thus, the existence of guarantees to perform international transfers is understood when:

- They are performed in a country, specific sector or international organisation that has been declared as having a suitable level of protection by the European Commission.

- They are performed between companies of the same group and binding corporate rules have been approved pursuant to art. 47 of the GDPR. In this case, said rules or the electronic address where they can be accessed shall be attached.

- Standard contractual clauses on data protection adopted by the European Commission have been signed. A copy of the signed clauses shall be attached.

- The entities that perform the data transfer are adhered to a code of conduct or certification mechanism, together with binding and demandable commitments by the controller or processor in the third-party country to apply suitable guarantees, including those on the rights of the data subjects. A copy of the code of conduct or certification or the electronic address where it is can be accessed shall be attached.

In this case, the advice of the Data Protection Officer can be requested to fulfil this obligation.

vii. **Automated individual decisions and profiling**

Profiling and the automated individual decisions of a natural person entail the processing of relevant personal data that can frequently take place in the framework of a research project.

The GDPR introduces provisions to guarantee that its use does not cause an unsubstantiated impact on the rights of persons, such as[20]:

- "specific requirements of transparency and equity;
- greater obligations of proactive responsibility;
- specific legal bases for processing;
- individual rights to reject profiling, and specifically profiling for marketing; and
- if certain conditions are met, the need to conduct a data protection impact assessment".

Article 22 of the GDPR establishes the right of any data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Example: the denial of public subsidies, cancelling a contract, imposing a fine, etc.

Thus, both concepts must be understood in a separate and joint way.

Profiling[21] is a procedure that entails an automated processing of personal data to assess personal aspects, and in particular to analyse or make predictions on persons (in other words, it entails assessing or judging a person in some way).

This term is more than simply classifying people (by age, gender or height).

For example, classifying data subjects by their age or gender for statistical reasons for the purpose of achieving a global vision of them (WITHOUT making predictions or drawing conclusions on an individual) is not profiling, as its goal is not to assess individual attributes.

Thus, this legal concept involves gathering information on a person (or group of people) and assessing their attributes or behaviour patterns in order to assign them to a certain category or group, and in particular to analyse or make predictions on, for example:

- their ability to perform a task;

---

[20] Examples given in the guidelines on automated decisions and profiling of the work group of art. 29

[21] "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. (art. 4.4 GDPR).

- their interests; or
- their likely behaviour

Automated decisions are those made by technological means without human participation.

The GDPR addresses these concepts in three possible categories:

1.- Decisions based solely on automated processing, including profiling, which produce legal effects concerning the data subject or similarly significantly affect him or her.

The key is the concept "automated decision-making", based solely on technological means with no human intervention. This case is established in article 22.1 of the GDPR, which would entail a general ban of this type of actions. However, there are exceptions[22]. If applied, there should also be measures to guarantee the rights and freedoms of the data subject.

2.- General profiling
3.- Decisions based on profiling

In both these cases, the principles of article 5 (purpose, retention, minimisation, etc.), the bases that legitimise article 6 (preferably consent, public interest), transparency (notify the data subject) and, where appropriate, an impact assessment as detailed in article 35 shall be applied among other obligations. WP29 published guidelines[22] in order to guarantee compliance with the regulation when these processing activities take place.

viii. Rights of the data subjects

People who take part in research projects can exercise their rights of access, rectification, erasure, to limit the processing and to not be the target of automated individualised decisions.

If researchers are aware of any requests to exercise said rights, they must notify this

---

22 Article 22. Automated individual decisions, including profiling.
1. All data subjects will have the right not to be targeted by a decision based solely on automated processing, including profiling, which produce legal effects concerning the data subject or similarly significantly affect him or her.
2. Section 1 will not be applicable if the decision:
a) is necessary to enter into or execute a contract between the data subject and the controller;
b) has been authorised by Union or Member State law applicable to the controller and establishes suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject, or
c) is based on the explicit consent of the data subject.
3. In the cases detailed in section 2, letters a) and c), the controller shall adopt the suitable measures to safeguard the rights and freedoms and legitimate interests of the data subject, at least the right of the controller to obtain human intervention, to express their point of view and to challenge the decision.
4. The decisions referred to in section 2 shall not be based on the special category data included in article 9, section 1, except when applying article 9, section 2, letter a) or g), and when suitable measures have been taken to safeguard the rights and freedoms and legitimate interests of the data subject.
23 Guidelines on automated individual decisions and profiling for the purposes of Regulation 2016/679

to the Data Protection Officer of the UMH as soon as possible so that said request can be decided on with them.

ix. **The data protection officer of the UMH.**

The Data Protection Officer (DPD, from its meaning in Spanish) is an advisory and independent body which, among other tasks, must supervise compliance with regulation on the issue of personal data protection, provide reports and, where appropriate, manage the queries of people who get in touch with the DPD regarding the processing of their personal data at the university.

Likewise, they are also the person in charge of notifying senior management of their legal obligations on the issue of data protection, cooperating with the supervisory authority and acting as the contact point between the latter and the entity in charge of processing the data (article 39 of the GDPR).