Privacy Policy of the Internal Information System

Introduction:

The purpose of this Privacy Policy of the Internal Information System of the FUNDACIÓN MARIA CRISTINA MASAVEU PETERSON (FMCMP or Foundation) is to inform about the processing of personal data that, where applicable, will be carried out for the management and processing of communications or information that may be submitted through its information channel.
For correct configuration and design of the channel, FMCMP, complies with the following regulations regarding the whistleblower protection and data protection:

- Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against the corruption.
- Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, on the protection of persons with regard to the processing of personal data and the free circulation of this data.
- Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.

Who is responsible for the treatment?

FUNDACIÓN MARÍA CRISTINA MASAVEU PETERSON
Address: c/Alcalá Galiano, 6 – 28010 Madrid. E-mail: rgpd@fmcmp.com
Phone: 91 576 47 37

For what purpose is it carried out?

The personal data collected through the information channel are processed for the exclusive purpose of processing communications or information received, send the informant the pertinent communications about the status of processing or its results, unless you have objected to it; and, if appropriate, carry out all actions aimed at verifying the verisimilitude of the facts reported. to determine its archive, the adoption of pertinent measures or its transfer to the competent authority in each case.

What categories of data are you referring to?

Name and surname, address, email or safe place for communications purposes that is provided by the informant in the case in which you have not decided to make the communication anonymously.
Identity and contact data of the people to whom the information received refers, as well as that relating to the facts that are reported. are revealed in order to determine whether they constitute an infringement. The information must have been obtained in a context work or professional.

Identification and contact data of legal representatives or support people and related to informants when necessary to effects of implementing protective measures.

Is there an obligation to provide the data and what are the consequences of not doing so?

Communications may be made anonymously and will also be processed.
Likewise, if you have provided your contact information, you can object to receiving communications related to the processing of the process.

What groups are data processed?

Likewise, if you have provided your contact information, you can object to receiving communications related to the processing of the process.

- Law 2/2023, of February 20, regulating the protection of people who report regulatory infractions and the fight against the corruption.
- The self-employed.
- Members of Board of Trustees, participants and persons belonging to the administrative, management or supervisory body of the company, including non-executive members.
- Any person who works for or under the supervision and direction of contractors, subcontractors and suppliers.
- Those people who have maintained an employment or statutory relationship.
- In cases where information about violations has been obtained during the selection or pre-contractual negotiation process, those people whose employment relationship has not yet begun.

Additionally, and whenever necessary, data will be processed for the purpose of establishing protective measures for:

- Legal representatives of employees in the exercise of their advisory and support functions for the whistleblower.
- Individuals who, within the framework of the Foundation, assist the whistleblower in the process.
- Individuals who are related to the whistleblower and who may suffer reprisals, such as colleagues or family members of the whistleblower.

Why is it possible to carry out this data processing?

The Foundation carries out the treatment in compliance with a mission performed in the public interest, namely the prevention of violations of current regulations and the ethical code it has adopted and within which it carries out its activity.

To whom can your data be communicated?

In no case will the identity of the informant be communicated to the affected subjects nor will they be given access to the communication.

If necessary or required, the data will be communicated to those third parties to whom FMCMP is legally obliged to provide them, such as competent authorities, Judges and Courts.

FMCMP is obliged to send the information to the Public Prosecutor's Office immediately when the facts could be indicatively constitutive of a crime, or to the European Public Prosecutor's Office in the event that the facts affect the financial interests of the European Union.

The Independent Whistleblower Protection Authority, A.A.I. or the competent body, if applicable, at the autonomous level may require documentation, data or any information related to the procedures being processed, including data on personal character.

The identity of the informant may only be communicated to the judicial authority, the Public Prosecutor's Office or the administrative authority. competent in the framework of a criminal, disciplinary or sanctioning investigation. This circumstance will be transferred to the informant before revealing your identity, unless such information could compromise the investigation or judicial procedure.

Why is it possible to carry out this data processing?

The Independent Whistleblower Protection Authority, A.A.I. or the competent body, if applicable, at the autonomous level may require documentation, data or any information related to the procedures being processed, including data on personal character.

How long is your data kept?

They will be deleted immediately:

- All personal data that may have been communicated and that refer to conduct that is not included in the scope of law enforcement. If the information received contains personal data included within the special categories of data, it will be immediately deleted, without proceeding to its registration and processing.
- Information provided or part of it in the case in which it is proven that it is not true, from the moment it is obtained proof of said circumstance, unless said lack of veracity may constitute a criminal offense, in which case will keep the information for the necessary time during which the judicial procedure is processed.

The data that are subject to processing are kept in the information system only for the necessary time. to decide on the appropriateness of initiating an investigation into the reported events.

Communications that have not been processed are kept anonymously.

In the event that the start of the pertinent investigation is agreed, said data will be processed for the entire duration of the investigation.

A record of information is maintained at the disposal of the competent judicial authorities in accordance with the requirements and limits established in the Law. In no case are the data kept for a period greater than ten years.

What rights do you have?

You may request the exercise of these rights by contacting FMCMP through account rgpd@fmcmp.com

Right	**Content**
Access	To consult your data, obtaining confirmation as to whether or not it is being processed.
Rectification	To modify those that are incomplete or inaccurate.
Suppression	To request that they be deleted when they are not necessary, established by law, withdraw your consent or object to the treatment, among other reasons.
Opposition	To request that they not be processed for reasons based on your personal circumstances, in which case once analyzed These reasons will no longer be treated. In the case of the person to whom the communication refers, it is presumed that there are compelling reasons that legitimize the processing of your personal data.
Limitation of treatment	So that the treatment is blocked while it is assessed whether the attention of other rights is appropriate, when you oppose your deletion, or whether they are preserved, even if the person responsible does not need to process them, for the exercise or defense of their claims.
Unless subject to automated individual decisions	In order not to be subject to a decision based solely on the processing of your data, including profiling, that produces legal effects on you or significantly affects you in a similar way.

You can also file a claim with the Spanish Data Protection Agency (AEPD) if you consider that the processing of your data does not comply with the law.

You have the possibility of using external information channels before the competent authorities and, where appropriate, before the institutions, bodies or agencies of the European Union referred to in article 7 of the Law.

The affected person has the right to be informed of the actions or omissions attributed to him or her and to be heard at any time.

Whoever submits a communication or makes a public disclosure has the right not to have his or her identity revealed to third parties.

Confidentiality

The system is designed to guarantee the confidentiality of the identity of the informant and any third party mentioned in communication, as well as the actions that are carried out in the management and processing of the same, preventing the access of unauthorized personnel. Confidentiality is also guaranteed when the communication is sent through another channel or to non-staff members. responsible for your treatment, who will immediately send the communication to the person responsible for the system designated by FMCMP. Our staff has received training in this regard.

Proportionality and data minimization

No personal data is collected whose relevance is not evident to process specific information or, if collected by accident, they will be deleted without undue delay. No data is obtained that would allow the identification of the informant if he or she had chosen to make the communication anonymously.

Limiting access to data

Internally Compliance Officer can access the data from the Ethics Channel.
Other people may participate in the treatment when necessary for the adoption of corrective measures in the treatment. entity or the processing of sanctioning or criminal procedures that, where appropriate, may apply:

- When it is appropriate to adopt disciplinary measures against a worker, the person responsible for human resources or body competent for this purpose.
- Those in charge of treatment who are eventually designated to collaborate in the investigation, professionals who will act at all times subject to a duty of secrecy, confidentiality and confidentiality.