

## DATA PROTECTION POLICY FOR THE INTERNAL INFORMATION SYSTEM

Pursuant to the provisions of the EU's General Data Protection Regulation (GDPR) 2016/679, of 27 April; of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD); and of Law 2/2023, of 20 February, Regulating the Protection of Persons Reporting Regulatory Violations and the Fight against Corruption (Whistleblower Protection Act), as well as with the provisions of other applicable data protection legislation, below we explain how we process the personal data provided through the Internal Information System.

The Internal Information System includes the necessary measures to guarantee and ensure the confidentiality of the identity and protection of the whistleblower and any third party mentioned in the communication, preventing unauthorised parties from accessing the information.

### 1. DATA CONTROLLER

The data controller is Cobega, S.A. (hereinafter, 'Cobega') with its registered office at Esplugues de Llobregat (Barcelona), Avinguda dels Països Catalans, 32; and tax identification number A-08080632.

The personal data provided will be processed by Cobega. In the event that the information provided involves any of the companies comprising Cobega, we may communicate your data to said entity in order to carry out the appropriate procedures in relation to the complaint. Discover the entities that form part of Cobega here: <https://www.cobega.com/>

### 2. PURPOSES

Depending on the processing carried out, personal data may be processed for the following purposes:

Purpose	<i>Description of the purpose and basis of legitimacy</i>
<b>Resolve queries</b>	<p>We will process the data to respond to queries made in relation to the operation and management of the Internal Information System and/or Compliance Model.</p> <p><b>Basis of legitimacy:</b> legitimate interest</p>
<b>Receiving and handling of complaints</b>	<p>We will process the data for the purpose of receiving complaints, deciding whether or not to initiate an investigation of complaints received, also with the aim of carrying out the corresponding investigation of the reported facts, protecting the whistleblower from retaliation, if necessary, taking appropriate corrective action, and, where appropriate, initiating legal action against the respondents and/or third parties.</p> <p>In the event that the complaint is reported verbally (by telephone, voice message or face-to-face meeting), we would like to inform you that we are obliged to document the complaint in one of the following ways, as you choose:</p> <p>a) by recording the conversation in a secure, durable and accessible format, or</p> <p>b) through a complete and exact transcription of the conversation carried out by the responsible staff.</p> <p>If the conversation is transcribed, you will have the opportunity to verify, rectify and accept the transcript of the conversation with your signature.</p>

	<b>Basis of legitimacy:</b> legal obligation (obliged private sector parties) / public interest (non-obliged private sector parties)
<b>Accrediting the proper functioning of the Internal Information System and the Compliance Model, and preserving any proof for Cobega's defence.</b>	<p>We can preserve data to accredit the proper functioning of our Internal Information System and the Compliance Model, and/or keep any proof for Cobega's defence.</p> <p><b>Basis of legitimacy:</b> legitimate interest and legal obligation</p>

### 3. TYPE OF PERSONAL DATA THAT MAY BE PROCESSED

Whether you provide your personal data directly to us or to a third party, we will process the following personal data:

Type of interested party	Data category
<b>Enquirer</b>	Identification data of the enquirer, contact data, employment data, financial data and other data associated with the enquiry, evidence.
<b>Named whistleblower</b>	Identification data, contact data, details of the facts considered relevant, evidence and voice.
<b>Anonymous whistleblower</b> <i>(The whistleblower can provide the following data or none of it)</i>	Pseudonym, contact details, evidence, voice.
<b>Confidential whistleblower</b> <i>(The informant does not want Cobega to know their identity. In this case, the identification data provided will only be managed by the Ethics Channel's external manager)</i>	Identification data, contact data, data associated with the reported conduct, evidence, voice.
<b>Respondent</b>	Identification data, data associated with the reported conduct, evidence.
<b>Witness</b>	Identification data, contact data, data associated with the reported conduct, evidence.
<b>Third parties</b>	Identification data, contact data, data associated with the reported conduct, evidence.

While the communication you sent is being handled, you may be asked to clarify the information communicated or to provide additional information.

### 4. BASIS OF LEGITIMACY

We will process your data in accordance with one or more of the following bases of legitimacy set out above:

Basis of legitimacy	Description
---------------------	-------------

Execution of a contract	We will process your data if required to do so for the execution of a contract, in order to fulfil the obligations set out in said contract.
Legal obligation	We may also process your personal data because we are required to do so by law.
Public interest	We may also have to process your data to perform a task carried out in the public interest or in exercising the public authority vested in us.
Legitimate interest	We may process your data when necessary for the fulfilment of overriding legitimate interests that we have as Data Controller.  For more information about the assessment of legitimate interest in each case, please contact the Data Protection Officer.

## 5. DATA COMMUNICATION

In general, your personal data will be kept confidential and will not be communicated to those related to the facts or to third parties.

However, your personal data may be communicated to those external service providers we have contracted to receive information from the channel and, where appropriate, to manage and carry out the necessary investigations, as well as process the data in their capacity as data processors and will, in no case, process the data for their own purposes.

Furthermore, it may be communicated to the Security Forces, Judges or Courts, as well as any other competent body in the event of being required to do so, in compliance with the legislation in force.

When there are indications that the reported facts may constitute a criminal offence, there is an obligation to immediately notify the Public Prosecutor's Office of these facts. If the alleged facts are likely to affect the financial interests of the European Union, they should be referred to the European Public Prosecutor's Office.

## 6. INTERNATIONAL TRANSFER OF DATA

In the event that Cobega has international suppliers or is part of a group of companies, your personal data may be processed outside the European Union or the European Economic Area.

In this case, Cobega will ensure that such data processing is always protected by suitable safeguards, which may include:

- EU-approved Standard Clauses: these are contracts approved by the European regulator, and which provide sufficient guarantees to ensure that the processing complies with the requirements established by the European Data Protection Regulation.
- Third-party certifications: framework agreement between the EU and a third state that establishes a standardised framework for data processing compliant with European Data Protection Regulation requirements.

## 7. DURATION OF PROCESSING

- **Inquiries**

In the case of inquiries, personal data will be kept for the time necessary to resolve the doubt or question raised and to provide the interested party with a reply. After the end of the relevant preservation period, the data may be duly blocked and preserved in order to prove compliance

with the Cobega Compliance Model and, where appropriate, to comply with legal obligations. Once this period has expired, the data will definitively be deleted.

- **Complaints**

Personal data will be kept in the Ethics Channel of the Internal Information System only for the time necessary to decide whether to initiate an investigation into the reported facts and, in any event, for a maximum period of three (3) months from the date of sending the confirmation of receipt or, if we have not confirmed receipt, for a maximum period of three (3) months from the seventh day following the date of sending the report.

If no investigation has been initiated within three (3) months of receipt of the complaint, the data shall be deleted from the Internal Information System, unless it is kept as evidence of the correct functioning of the system, in which case it shall be anonymised, and the obligation to block it, as set out in the LOPDGDD, shall not apply.

In the case of admissible complaints, they shall be preserved in the Internal Information System for the duration of the investigation and, in general, for a maximum period of ten (10) years. However, we may extend the maximum preservation period in the following cases:

1. To accredit the effective operation of our Compliance Model, in accordance with the provisions of article 31 bis of the Criminal Code, taking into account the statute of limitations for offences in accordance with the provisions of the Criminal Code.
2. When the reported act constitutes a crime or administrative offence, during the statute of limitations period for crimes established in the Penal Code and, in the case of administrative sanctions, according to the period established in the laws applicable to each case.

After the preservation period has expired, it shall be definitively destroyed.

Please also note that we will delete personal data immediately in certain cases, without any obligation to block the data:

- If the information provided is proven to be fully or partially untrue, unless the untruthfulness constitutes a criminal offence, in which case the data shall be preserved for the time necessary for the duration of the legal proceedings.
- If personal data has been communicated that is not necessary for the knowledge and investigation of the actions, or omissions within the scope of this channel, including special data categories. In the latter case, it shall be deleted immediately, without being registered and processed.

## **8. EXERCISING RIGHTS.**

The owner of the personal data may at any time exercise their data protection rights (including withdrawal of the consent granted) of access, rectification, deletion, opposition, portability and limitation at no cost by writing to [privacidad@cobega.com](mailto:privacidad@cobega.com) and including the reference 'Personal data'.

In the event that we consider it necessary, i.e. that you are the one exercising the corresponding data protection rights, we may ask you for a copy of your ID card or equivalent document proving your identity in order to execute your request to exercise your rights.

Nevertheless, if the person being investigated exercises their right of objection to the processing of their data, it will be presumed that, unless proven otherwise, there are compelling legitimate reasons that legitimize the continuation of said processing of their personal data.

If you have any questions or complaints about how we process your personal data, you can contact our Personal Data department at the contact address indicated in the '**Data Controller**' section.

A complaint may also be presented to the Spanish Data Protection Agency ([www.aepd.es](http://www.aepd.es)) if you feel that we have not properly addressed your rights.