WHISTLEBLOWING MANAGEMENT SYSTEM
DATA PROTECTION POLICY

In accordance with the provisions of Regulation (EU) 2016/679, of 27 April, on the Protection of Natural Persons with regard to the Processing of their Personal Data (GDPR); in Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD); and in 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 the rest of the applicable data protection legislation, as follows, we explain how we process personal data provided through our internal reporting system (the "**Whistleblowing Management System**" or "**WMS**").

The Whistleblowing Management System has the necessary measures in place to guarantee and ensure the confidentiality of the identity and protection of the whistleblower and any third party mentioned in the communication, preventing unauthorised persons from accessing the information.

1. DATA CONTROLLER

Your personal data will be processed by:

Information	Details of the Data Controller
Company	COMSA Corporación de Infraestructuras, S.L. (hereinafter, "**COMSA CORPORACIÓN**")
Tax ID No.	B08937724
Postal address	Calle Viriato, 47, 08014, Barcelona
Contact details of the Data Protection Officer (DPO)	lopd@comsa.com

The personal data you provide us with will be processed by COMSA CORPORACIÓN. In the event that the information provided concerns any of the companies that form part of COMSA CORPORACIÓN, we may communicate your details to this entity in order to carry out the appropriate procedures in relation to the report.

2. PURPOSES

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

Purpose	Description of the purpose and basis of legitimacy
Resolving queries	We will process the data to respond to enquiries made in relation to the operation and management of the Whistleblowing Management System and/or the Compliance Model. **Basis of legitimacy**: legitimate interest.
Receipt and processing of reports	We will process the data for the purpose of receiving reports, deciding whether or not to initiate an investigation of the reports received, also for the purpose of conducting an investigation of the reported facts, protecting the whistleblower from

	retaliation, taking, if necessary, appropriate corrective measures and, if necessary, initiating legal action against the reported persons and/or third parties. In case the communication of the report is made verbally, we inform you that we are obliged to document the report in one of the following ways, at your choice: a) by a recording of the conversation in a secure, durable and accessible format; or b) through a complete and accurate transcript of the conversation made by the staff responsible for dealing with it. In case of transcription of the conversation, you will have the opportunity to check, rectify and accept by signature the transcription of the conversation. **Basis of legitimacy**: legal obligation (obliged private sector entities) / public interest (non-obliged private sector entities).
To prove the proper functioning of the Whistleblowing Management System and the Compliance Model and to preserve evidence for COMSA CORPORACIÓN's defence.	We may keep your data in order to prove the proper functioning of our Whistleblowing Management System, our Compliance Model and/or to keep evidence for the defence of COMSA CORPORACIÓN. **Basis of legitimacy**: legitimate interest and legal obligation.

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:

Types of data subjects	Data categories
Consultant	Identification data of the consultant, contact details, employment data, financial data and other data associated with the query, evidence.
Named whistleblower	Identification data, contact details, details of the facts considered relevant, evidence and voice.
Anonymous whistleblower *(The whistleblower can provide the following data or none of them)*	Pseudonym, contact details, evidence, voice.
Reported person	Identification data, data associated with the conduct reported, evidence.
Witness	Identification data, contact details, data associated with the reported conduct, evidence.
Third parties	Identification data, contact details, data associated with the reported conduct, evidence.

During the course of the handling of the communication sent by you, 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 this is necessary for the performance of a contract, in order to fulfil the obligations set out in the 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 for the performance of a task carried out in the public interest or in the exercise of public authority vested in us.
Legitimate interest	We may process your data where it is necessary for the fulfilment of overriding legitimate interests that we have as Data Controller. For more information about the weighting of legitimate interest in each case, please contact the DPO.

5. DATA COMMUNICATION

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

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

Likewise, they may be communicated to the Law enforcement agencies, 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.

Where 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 the 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 DATA TRANSFERS

If COMSA CORPORACIÓN has international suppliers or forms part of a group of companies, it is possible that your personal data may be processed outside the European Union or the European Economic Area.

In this case, COMSA CORPORACIÓN will ensure that such data processing is always protected with the appropriate 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 in line with the requirements of the European Data Protection Regulation.

7. DURATION OF PROCESSING

- **Queries**

In the case of queries, personal data will be kept for the time necessary to resolve the doubt or question raised and to provide the data subject with a reply. Once the corresponding retention period has expired, the data may be duly blocked and retained in order to prove compliance with COMSA CORPORACIÓN's Compliance Model and, where appropriate, to comply with legal obligations. Once this period has expired, the data will be definitively deleted.

- **Reports**

Personal data will be kept in the whistleblowing channel of the Whistleblowing Management System only for the time necessary to decide whether to initiate an investigation into the reported facts and, in any case, for a maximum period of three (3) months from the date of sending the acknowledgement of receipt or, if we have not acknowledged receipt, for a maximum period of three (3) months from the seventh day following the date of sending the report.

If, three (3) months after receipt of the report, no investigation has been initiated, the data will be deleted from the Whistleblowing Management System, unless they are kept as evidence of the proper functioning of the system, in which case they will be anonymised, without the obligation to block them provided for in the LOPDGDD being applicable.

In the case of reports admitted for processing, they shall be kept in the Whistleblowing Management System for the duration of the investigation and, in general, for a maximum period of ten (10) years. However, we may extend the maximum retention period in the following cases:

1. To prove the effective operation of our Compliance Model, in accordance with the provisions of article 31 bis of the Spanish Criminal Code, taking into account the statute of limitations for offences in accordance with the provisions of the Spanish Criminal Code.

2. When the reported act constitutes a crime or administrative offence, during the statute of limitations period for crimes established in the Spanish Criminal Code and, in the case of administrative sanctions, according to the period established in the laws applicable to each case.

After expiry of the retention period, they shall be definitively destroyed.

We also inform you that we will delete personal data immediately in certain cases, without any obligation to block the data:

- If it is established that the information provided or part of it is not truthful, unless the lack of truthfulness constitutes a criminal offence, in which case the data shall be kept for the time necessary for the duration of the legal proceedings.
- If personal data have been communicated that are not necessary for the purpose of knowledge and investigation of the actions or omissions within the scope of this Whistleblowing Channel, including special categories of data. In the latter case, they shall be deleted immediately, without registration and processing.

8. EXERCISE OF RIGHTS

The data subject may at any time exercise his/her data protection rights (including withdrawal of consent) of access, rectification, erasure, objection, portability and restriction free of charge by writing to lopd@comsa.com and including the reference "**Data protection rights**".

If we have doubts about your identity, i.e. that it is you who is exercising the corresponding data protection right, we may ask you for a copy of your ID card or equivalent document proving your identity and, once we have verified your identity, we will execute your request to exercise your rights.

However, in the event that the person under investigation exercises the right to object to the processing of his or her personal data, it shall be presumed that, in the absence of proof to the contrary, there are compelling legitimate grounds to continue the processing of his or her personal data.

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

Additionally, you may file a complaint with the Spanish Data Protection Agency (www.aepd.es) if you feel that we have not properly addressed your rights.

9. ADDITIONAL INFORMATION

For more information on how to exercise your data protection rights, please refer to our Website Privacy Policy, which can be found at https://www.comsa.com/en/legal-texts/website-privacy-policy/.

Last updated: 12 June 2023.