Procedure for the Management of Communications Received at CELSA

Approved by the Board of Directors of

CELSA STEEL S.A. on 28 January 2025

INDEX

1. Definitions **3**

2. Purpose of the Procedure for the Management of Communications Received at CELSA **5**

3. Means of communication **7**

4. Scope of application **9**

5. Investigation procedure **10**

Phase I. Receipt of Communications 10

5.1.1. Reception of Complaints and Enquiries 10

5.1.2 Ex officio opening 11

Phase II. Assessment of *Complaints* 12

5.2.1 Analysis and Preliminary Report on the *Complaint* 12

5.2.2 Admission of the *Complaint* for processing or filing of the *Complaint* 13

Phase III. *Complaint* handling phase 14

Phase IV. Conclusion of the *Complaint* 16

6. The Internal Information System Log Book **18**

7. Protection of personal data **19**

7.1. Preservation of information 19

7.2. Data Protection Rights of the *Informant* 20

7.3. More information on the processing of personal data 20

8. Disciplinary regime **21**

Annex I **22**

Annex II **24**

1. Definitions

Definitions of those concepts that are frequently used in this document are listed below (quoted in *italics*):

- ***CELSA / Organisation***: for the purposes of the *Criminal Prevention Model,* it will refer to the company CELSA STEEL, S.A. and to the rest of the entities that make up the *Criminal Control Perimeter,* listed in Annex I of the *Criminal Compliance Policy*.
- ***Criminal control perimeter:*** includes the entities adhering to *CELSA*'s *Criminal Compliance Model*, listed in Annex I of the *Criminal Compliance Policy*.
- ***Board of Directors:*** *CELSA*'s governing body, to the extent that it has primary responsibility and authority for activities, governance and policies, and to which *CELSA*'s Steering *Committee* reports and is accountable.
- ***Management Committee:*** a group of members within *CELSA,* with management and control functions within the *organisation* at the highest level
- ***Audit and Control Committee****: a* permanent body made up of several members of the *Board of Directors*, of an informative and consultative nature, without executive functions, with full powers of information, advice and proposal within its scope of action, which is responsible, among other duties, for supervising *the Criminal Prevention Model*.
- ***Members of the Organisation***: members of the *Board of Directors*, members of the Steering *Committee*, employees, workers or temporary employees or employees under a collaboration agreement and all other persons under the hierarchical subordination of any of the above.
- ***Business partners:*** any legal or natural person, other than *Members of the Organisation,* with whom the *Organisation* has or plans to establish some kind of business relationship. By way of example, but not limitation, this includes installation companies, agents or commission agents, suppliers, external advisors, *joint ventures*, customers and, in general, natural or legal persons contracted by *CELSA* to deliver goods or provide services.
- ***Third party: a*** natural or legal person or body independent of the *Organisation*.
- ***Criminal Prevention Model***: an organisational and management system for the prevention of crime, whose objective is the prevention, detection and management of *criminal risks*, and whose essential basis is represented in the *Criminal Compliance Policy* and in the *Crime Prevention and Response Manual*.
- ***Ethics Committee:*** *CELSA*'s internal collegiate body with autonomous powers of initiative and control, which is entrusted, among other tasks, with the responsibility of supervising the operation and observance of the *Compliance Model criminal.* The existence of this body responds to the requirements established in Spanish criminal law (article 31 bis of the

Spanish Criminal Code) regarding the supervision of the *criminal Compliance Model*. The *Ethics Committee* also plays the role of Head of the Internal Information System.

- ***Procedure for the management of communications received by CELSA:*** document that establishes the necessary mechanisms for the early communication and management of any *infringement*, as well as the necessary procedures for the internal processing of *queries*, and the internal processing and investigation of *complaints* or any known circumstance that should be investigated.

- ***Internal Information System:*** measures adopted in accordance with Law 2/2023 for the management of communications relating to *infringements* of the regulations referred to in this text. The *Internal Information System* has a *System Manager in charge of* the management and diligent processing of the *Communications* received, in accordance with the provisions of the *Procedure for the Management of Communications Received.*

- ***Communication: a*** statement of a question regarding the scope, interpretation or compliance with the regulations applicable to *CELSA.* Depending on its content, a communication may consist of a *Consultation* or a *Complaint*.

- Query***:*** communication by which any *Member of the Organisation* requests a clarification, response or opinion on the scope, interpretation or compliance with the regulations applicable to *CELSA.*

- ***Whistleblowing***: communication regarding a possible *breach* (active or omissive behaviour) of the regulations applicable to *CELSA,* understood as the set of ethical and compliance commitments voluntarily assumed by the *Organisation*, as well as the current legislation applicable to it at any given time.

- ***Infringements:*** any behaviour, whether by action or omission, that violates the rules applicable to the *Organisation.* This includes, but is not limited to, the following:
  - Infringement of European legislation;
  - Criminal, serious administrative or very serious infringements;
  - Infringements in labour matters relating to health and safety at work, established in the Spanish legal system, and
  - Non-compliance with internal regulations, including but not limited to the *Code of Ethical Conduct*

  The infringements must be within the *organisation* or involve *CELSA*.
  An Infringement, depending on its seriousness, may range from a mere formal breach of a requirement of an internal rule to the commission of acts constituting a criminal offence potentially attributable to the *Organisation*

- ***Informant***: a natural or legal person who anonymously or by name files a *Complaint*. The figure of the *informant* includes:

- *Members of the Organisation*: includes employees whose employment relationship is in force, has ended or has not yet begun, shareholders and members of the *Board of Directors*, paid and unpaid volunteers and trainees.
- *Business partners*, as well as any person working under their supervision and direction. Subjects or legal persons external to the *Organisation*, with whom the Organisation has or plans to establish a business relationship, as well as any person working under their supervision and direction.
- *Third parties* and other individuals, e.g. trade unions.
- Any person, natural or legal, with a present or future fit in the above contexts.

- ***Affected persons*****:** this figure includes, among others, the following:
  - Witnesses, or other persons involved in the *Inquiry or Complaint*.
  - Researchers.
  - Family members, trade union representatives, and other persons supporting the *Informant*.
  - Those from which information is obtained that led to the filing of a *Complaint*.
- ***Reported***: natural or legal person(s) linked to the reported *Infringements*, as perpetrators, participants or even accessories. They may be identified in the *Communication* or be specified throughout the process of its management.
- ***Retaliation*****:** any action or omission, whether attempted, threatened or actual, direct or indirect, which may result in harm or disadvantage to the *Whistleblower* or other *Affected Persons*, in the employment or professional sphere, solely because of their status in relation to the *Whistleblowing* or because they have performed a public disclosure.
- ***Independent Whistleblower Protection Authority (IPA): an*** independent administrative authority, as a public law entity at state level, which will act in the fulfilment of its main function of protecting *whistleblowers.* Its other functions include the management of its own external channel, the processing of sanctioning procedures and the imposition of sanctions, among others.
- ***Log-book:*** system through which the evidence of the information received and of the internal investigations to which they have given rise shall be kept, guaranteeing, in all cases, the requirements of confidentiality.

2. Purpose of the Procedure for the Management of Communications Received at CELSA

This *Procedure for the Management of Communications Received in CELSA,* approved by the *Board of Directors,* develops the content of *CELSA's Internal Information System Policy,* underlining the *Organisation*'s firm will to maintain a conduct that respects both the rules and ethical standards, and promoting an environment of zero tolerance towards possible *Infractions*.

Through this *Procedure*, *CELSA* determines the necessary mechanisms to communicate and manage any *Infringement* in an early manner and establishes the necessary mechanisms to carry out the internal processing of the *Communications* received.

3. Communication channels

Different internal channels are made available to *Members of the Organisation*, *Business Partners* and *Third Parties* so that they can submit any type of *Communication* related to possible *Infractions*.

In particular, the following channels of **written** communication exist:

- The *Ethics Channel* will be available at the following link: https://celsa.integrityline.com/, accessible from the *Organisation's* employee portal and on CELSA's corporate website
- By Email: comite.etico@gcelsa.com
- By post to the following address, for the attention of the *Ethics Committee*:
  C/Ferralla, 12, Pol.Ind. San Vicente,
  08755 Castellbisbal (Barcelona) Spain

It will also be possible to perform a **verbal** *Communication* (in case of *Complaints* or *Enquiries* made by *Members of the Organisation*) through the following means:

- By telephone:
  Spain +34 910477636.
  France +33187212291.
  Poland +48221523361.

  The Reporting Party must enter the Access PIN code 9097, corresponding to CELSA, after initiating the call, and may choose to communicate in the official language of the place from which the communication is performed, in English, or in Spanish.
- By means of a face-to-face meeting with the *Compliance Manager* or any other member of the *Ethics Committee*, within seven (7) days of the request. This communication will be previously informed and will be transcribed and the informant will be informed of the processing of his/her data in accordance with the legislation in force.
- Line manager or a member of *CELSA's management,* who should forward the information to the *Ethics Committee*.

Verbal communications, including those performed through face-to-face meetings, by telephone or by voice messaging system, shall be documented with the consent of the informant, and the informant shall be informed of the processing of his or her data in accordance with the provisions on personal data protection.

Regardless of the means of communication used, the *Reporting Person* will receive a six-digit code (Case ID) that must be retained in order to access the communication channel through the *Ethics Channel*.

The official channel for receiving information on the status of the *Report* or contacting the *Whistleblower* will be the *Ethics Channel*.

CELSA encourages all *Members of the Organisation* or subjects who suspect or know of *CELSA-related Breaches* to use these internal channels to make their *Communications* to *CELSA*.

Any *Consultation* or *Complaint* shall be handled by the *Ethics Committee* under the terms developed in the *Internal Information System Policy* and in this *Procedure.*

Furthermore, the *Organisation* informs any potential *Whistleblower* that it also has external channels of information available to the competent authorities and, where appropriate, to the institutions, bodies, organs or agencies of the European Union, such as, inter alia:

- In antitrust matters: Complaint of prohibited conduct | CNMC
- In the area of tax offences: Tax Agency: Complaints
- In case it is related to subsidies or fraud involving European funds: Anti-fraud mailbox - Complaints channel of the Recovery and Resilience Mechanism - Recovery, Transformation and Resilience Plan Government of Spain (planderecuperacion.gob.es).
- National Anti-Fraud Coordination Service: IGAE:Servicio Nacional de Coordinación Antifraud (hacienda.gob.es
- Oficina Antifrau de Catalunya: Complaints to the Anti-Fraud Office of Catalonia
- As well as any other competent local authority where CELSA operates.

CELSA also informs potential *whistleblowers* of the existence of a public body called the *Independent Whistleblower Protection Authority*, to which they can also turn.

Most convenient, however, is the use of the internal channels mentioned above as the preferred channel of communication.

Persons who report a *Complaint* must collaborate with the *Ethics Committee* in the analysis and investigation phase when required to do so. Likewise, they must maintain due confidentiality regarding the collaboration provided and the facts brought to *CELSA*'s attention. This obligation is also assumed by *CELSA*.

Annex I of this *Procedure* provides some examples of possible scenarios that can be reported.

4. Scope of application

Like *CELSA*'s *Internal Information System Policy,* this *Procedure* is mandatory for the *Organisation*. Therefore, this *Procedure* is applicable to the members of the *Board of Directors*, the *Audit and Control Committee*, the Steering *Committee* and all professionals who make up *CELSA,* regardless of the companies to which they belong, the place of residence or the place where their activities are carried out.

This Procedure is also applicable, insofar as it applies to them, to *CELSA*'s contractors, subcontractors and suppliers, as well as to those persons linked by a statutory framework, voluntary work, internship, training period or who have obtained the information in the context of a selection process or pre-contractual negotiation or an employment relationship that has already ended.

It also binds those persons who, even if they are not *Members of the Organisation,* are aware of the existence of any Infringement in their professional relationship with *CELSA*

5. Investigation procedure

This section determines the procedures and rules of action to be followed with regard to *Queries and Complaints* received through *CELSA*'s communication channels.

During all the phases described above, the *Ethics Committee* will ensure that the rights of all those involved in the *Consultation* or *Complaint* are respected, as set out in *CELSA*'s *Internal Information System Policy*.

Phase I. Receipt of Communications

5.1.1. Receipt of Complaints and Enquiries

The *Ethics Committee*, as the body responsible for the management of the *Internal Information System*, shall receive the *Communications* and shall issue, by the same means of receipt, an acknowledgement of receipt within a maximum period of seven (7) days, informing the Whistleblower *of* the information relating to the collection and processing of his or her personal data.

In cases in which the *Infringements* are not reported through the channels provided for this purpose by *CELSA*, but through other internal channels, the parties receiving the information are obliged to forward the information received immediately to the members of the *Ethics Committee* and, if immediate communication is not possible, within a maximum period of two calendar days. In any case, the seven-day period for acknowledgement of receipt of the report received must be respected, as well as the appropriate communication of the collection and processing of the whistleblower's personal data

The *Ethics Committee* shall proceed, regardless of the means by which the *Communication* has come to its knowledge, to enter its details in the *Internal Information System logbook* and assign it a file number.

After issuing the corresponding acknowledgement, the *Compliance Manager* shall verify the minimum content of the *Communication*:

- Minimum content in case of *Consultations:*
    - Date on which the *Consultation* is issued.
    - Name and contact details of the *Informant* submitting the *Query*, provided that the Query is not to be performed anonymously. In order to facilitate a response to the *Query*, it is advisable to include in the *Query* the identity of the *Informant* and the secure means of communication by which he/she wishes to be contacted, which will be actively protected, so that it remains confidential.
    - A clear and detailed statement of the matter requiring clarification or response and the reason why such clarification, response or judgement is sought.

- Minimum content in case of Reports*:*
  - Date on which the Report is issued*.*
  - As clear and detailed a statement of the facts as possible.
  - Identification of the possible perpetrator, as well as other possible participants and persons who may have knowledge of the event in question.
  - Name and contact details of the *Whistleblower,* as long as this is not to be performed anonymously. In order to facilitate the investigation of the reported facts, it is advisable to include in the *Report* the identity of the *Reporting Person* and the secure means of communication by which he/she wishes to be contacted*,* which will be actively protected, so that it will be confidential.
  - The time at which the *Breach of* the rules applicable to the *Organisation* was committed or continues to be committed at the time the *Complaint* is being made*.*
  - Any other information and/or documentation that the Whistleblower can provide for the understanding of the event in question.

Upon receipt of the Report or Query, the *Ethics Committee* shall act according to the content of the *Communication*:

- In the case of a Query, the *Ethics Committee* shall respond as soon as possible to all the points raised by the same means by which the Query was communicated to it.
- On the other hand, if the content of the Query leads to the possibility that a *Member of the Organisation* has committed or may perform an *Infringement*, such *Communication* shall be treated as a Report.
- Where there is a *Communication*, but its content is insufficient, incomplete, or does not provide the necessary detail, then a *Notification* shall be sent to the *Reporting Party*, where the option to contact the Reporting Party is available, requesting the necessary additional information.

In the hypothetical case that any member of the *Ethics Committee* is involved in the reported facts, he/she must voluntarily withdraw, and the other members of the *Ethics Committee* will continue with the management of the *Communication.*

5.1.2 Opening ex officio

In addition, the *Ethics Committee* may also initiate this procedure ex officio when there are indications of a possible *infringement,* by any other means expressly regulated by the *Organisation*, such as, among others:

- During the performance of its members' duties.
- During the review of *CELSA's Crime Prevention Model.*

- During the course of or as a result of an audit exercise.
- During or after performing monitoring processes in different areas or processes.
- Through public or private statements or communications by any *Member of the Organisation* (in the media, in the context of formal or informal meetings, in the context of discussions, etc.).
- By oral or informal communications.

The *Ethics Committee* shall collect and document all evidence on which the suspicions are based, in order to be able to proceed with the contextualisation of the facts and their preliminary analysis. It shall therefore prepare or collect the following information:

- Clear and detailed statement of the facts.
- Identification of the possible perpetrator(s) of the event(s), as well as other possible participants and persons who may have knowledge of the event in question.
- Time of commission, or indicate the persistence of commission of the *Offence.*
- Any other information and/or documentation that may contribute to the understanding of the event in question.

Under the aforementioned conditions, it will be considered a *Complaint* and the channels foreseen in will be followed in this *Procedure*.

Phase II. Evaluation of *Complaints*

5.2.1 Analysis and Preliminary Report on the *Complaint*

Once the *Complaint* or *Consultation* has been received or the procedure has been initiated ex officio, the *Ethics Committee* shall perform a preliminary analysis of the plausibility of the *Complaint*, taking into account the following four aspects:

- Contrast the objective and subjective data of the information received.
    - Objective data: all those concrete elements provided by the *Informant* such as: facts, dates, names, amounts, places, etc.
    - Subjective data: all those ideas, hypotheses, opinions, assessments, rumours, etc. In other words, the information provided in the presentation of the facts of the *Complaint*.
- Analysis of the source of information and *communication*. Attention will be paid to:
    - The credibility of the source of information, understood as the guarantee offered by the source of information (*Informant*) in terms of its capacity to obtain the data provided in the *Complaint* (e.g. job position) as well as other communications received, related to the *Complainant* and *Informant*.

- The accuracy of the information contained in the *Complaint*, taking into account the degree of specificity of the data provided.

- Analysis of the information. The *Ethics Committee* shall study the information provided in the *Complaint* with regard to these aspects:
  - Contextualisation of the data provided in the *Complaint*.
  - Analysis of the information known in *CELSA* that can support or be compared with the data provided in the Report.
  - Consider information that may enrich the data provided in the *Complaint* or provide new insights into them.

- Integration. The *Ethics Committee* will establish, as a result of the information acquired and the analysis of the information, the hypothesis that it considers most likely and those that, although unlikely, represent relevant risks for *CELSA*, in addition to other possible hypotheses that may give coherence to the information known so far.

5.2.2 Admission of the Report for processing or closure of the report

The *Ethics Committee* shall document the reasons for admitting or closing a Report, which shall contain the following points:

- Descriptive information on the Report, its date of receipt.
- Data provided in the *Complaint*, discriminating between objective and subjective data.
- Assessment of the plausibility of the facts contained in the *Complaint* and the reliability of the *Informant*.
- Analysis of the information and documentation submitted with the *Complaint*.
- Exceptional measures taken prior to the decision on whether or not to admit the *complaint.*
- In the event that the Report is derived from the response to a previous Query, the content of the Query and the response provided shall be included in the report.
- Decision on whether the *complaint* is admissible, stating, if appropriate, the action to be taken, including the need to perform an investigation.

The *Ethics Committee* will proceed to inform the Whistleblower of the relevance or otherwise, and consequently admit or shelve the reported facts.

In addition, the details of the *Complainant* and of the *Members of the Organisation* and *Third Parties* shall be kept in the *information logbook* only for the time necessary to decide whether to initiate an investigation into the alleged facts.

Phase III. *Complaint* handling phase

Once the Report has been admitted for processing, the *Whistleblower* (and, where appropriate, the other Affected *persons*) has been notified of this circumstance and the corresponding file has been opened, the investigation shall be conducted by the *Ethics Committee* in accordance with criteria of impartiality, speciality and knowledge of the matter.

The investigation shall be aimed at obtaining sufficient elements to enable the resolution of the case and the drafting of the corresponding Investigation Report and conclusions. This investigation, except in duly justified exceptions accepted by the *Ethics Committee,* shall last for a maximum of three (3) months from receipt of the *Communication* or, if no acknowledgement of receipt was sent to the *Informant*, three (3) months from the expiry of the period of seven days after the *Communication* was made, except in cases of particular complexity, which may be extended for an additional three (3) months.

Throughout the research, a channel of communication shall be maintained with the *Informant,* if applicable, through the preferred means designated by the Informant, and the *Ethics Committee* may request additional information from the Informant in order to ensure the success of the research.

However, the *Ethics Committee* may request advice from an external expert *Third Party* or have the support of another *Member of the Organisation* that can provide expert opinion in the investigation of a *Complaint*, if it so deems appropriate and there is no conflict of interest. In any case, said external *Third Party* - natural person or entity - shall maintain constant communication with the *Ethics Committee* regarding the actions carried out, guaranteeing in all cases the strictest confidentiality and limitation of access to the information.

Likewise, for the specific performance of the different functions attributed to the *Ethics Committee*, it may be assisted - by requesting help or the specific assistance of one or more functions - from the different areas that make up *CELSA*, depending on the specific circumstances of the case, which may make it advisable to do so.

The *Respondent* shall then be informed of the processing of his or her personal data within a reasonable period of time after the personal data have been obtained, and at the latest within one (1) month. If the personal data are to be used for communication with the *Respondent*, the Respondent shall be informed of the processing at the latest at the time of the first communication with the Respondent.

The information to be provided to the *Respondent* should include, as a minimum, the following points:

- The identity and contact details of the controller.
- The rights of access, rectification, erasure and portability of your data, of restriction and objection to their processing, as well as your right to file it with a supervisory authority and to take legal action, insofar as applicable.

- The origin or source of the data.
- The category of data.
- The facts of which he is accused.
- The person(s) within *CELSA* who could have access to the information during the investigation of the file.

In addition to the information relating to the protection of personal data, a summary of the facts for which the investigation is being carried out shall also be provided to the Whistleblower so that he/she may provide the allegations he/she deems appropriate and provide the evidence he/she deems appropriate to accredit his/her position regarding the facts that are the object of the investigation, and the record of the communication of the facts to the Whistleblower as well as all the evidence he/she provides to the procedure shall be recorded in the *Internal Information System*'s *Register Book.*

In the event that the research work has already begun, the *Ethics Committee* shall ratify the appropriateness of the research, or determine what is appropriate.

CELSA must at all times guarantee the confidentiality of the *informant* and the absence of *retaliation* in the event of good faith *complaints*. Therefore, the information provided to the *Reporter* in the exercise of his/her right of access will exclude the identity of the *Reporter* or those circumstances that make him/her identifiable to the *Reporter.*

The *Ethics Committee* shall be responsible for verifying the truthfulness and accuracy of the facts and information contained in the Report and, in particular, of the conduct reported, in order to verify the existence of a *breach* the regulations applicable to the *Organisation*. To this end, the *Ethics Committee* shall have the power to perform any investigative measures it deems necessary, respecting the rights of those affected and documenting its actions in the *Internal Information System Log Book*.

Among other measures, it shall have the power to perform interviews with the *Whistleblower*, the *Reported Person* and those *Third Parties* involved in the facts contained in the *Report* or who may have knowledge of them. Interviews shall be performed, whenever possible, in the presence of a witness (line manager, teammate or any other person deemed appropriate), allowing the *Reporting Person* to verify, rectify and accept the minutes of the meetings by signing them, and in the event that they are recorded, the interviewees shall be informed in advance of the transcription of the session. The *Informant* shall be given the opportunity to verify, rectify or accept by signature the transcript of the conversation.

Some possible investigative steps that could be taken are included in **Annex II** of this document.

Minutes will be taken of all the research sessions and interviews performed during the course of the research at the end of each meeting or later if the circumstances of the case so require, and it is recommended that they be signed by all those attending the corresponding session, in any

case allowing the *informant* to verify, rectify or accept the transcription of the conversation by signing it.

Phase IV. Conclusion of the *Complaint*

At the end of the previous Phase, the *Ethics Committee* shall draw up an Investigation Report and conclusions, which shall contain, as a minimum, the following points:

- Descriptive information on the *Complaint*, including its Unique *Complaint* Identification Number and its date of receipt.
- Data provided in the *Complaint,* discriminating between objective and subjective data.
- Assessment of the content of the *Complaint* and the reliability of the *Informant*, following the investigation performed.
- Analysis of the information and integration of this with expression of the most likely and highest risk hypotheses.
- Results of the investigation, where required.
- Measures proposed, if any, or already performed, in the event that the *Ethics Committee* has deemed them necessary or desirable for reasons of urgency.
- Proposal for action.

This report will be addressed to:

- To the *Board of Directors*, through the *Audit and Control Committee* in cases *of reports* about events that may generate liability for *CELSA*. The Audit *and Control Committee* may add any observations it deems appropriate, and may include an additional proposal for actions to be performed. The members of the *Board of Directors* may perform the observations they deem appropriate, ratify their content in a collegiate manner when they deem it appropriate and adopt the actions it deems necessary.
- To the Steering *Committee,* in cases of reports about facts related to serious or very serious administrative infringements, infringements in matters of safety at work and any other infringement of the legal system applicable to *CELSA* and the rest of the internal regulations of the *Organisation*.

In accordance with the report submitted by the *Ethics Committee*, the appropriate measures will be adopted, in accordance with the type of matter, including those of the sanctioning regime provided for in current labour and contractual regulations.

Together with the Investigation Report and conclusions, the *Ethics Committee* may make available to the *Audit and Compliance Committee*, the *Board of Directors* and the *Management Committee, the* express request of the members with a legitimate interest therein, the remaining documentation contained in the *Complaint*, such as: minutes, analysed documentation or other documented information of relevance for decision-making. In such cases, measures shall be

adopted to guarantee the confidentiality of the information, where necessary, by anonymising personal data or other circumstances that allow the identity of the *informant* to be known.

Where an *Infringement* has been concluded, the *Board of Directors* or the *Management Committee* shall:

- Take appropriate measures to resolve the *infringement* and continuously monitor the effectiveness of these measures.
- Administer appropriate sanctions (disciplinary or contractual), which are legitimate and proportionate to the facts reported.
- Refer matters to the relevant authorities, where appropriate, and monitor the outcome of decisions taken.

The *Audit and Control Committee* and/or the *Management Committee, as appropriate,* shall inform the *Ethics Committee* of the agreed actions, so that they are duly documented and recorded in the *Internal Reporting System logbook*. Among others, they shall order disciplinary measures that are legitimate and proportionate to the facts reported, and in the event of affecting *Members of the Organisation*, they shall consider the expert judgement of the Chief People Officer for their appropriate execution within the applicable labour framework.

The *Ethics Committee* will communicate in a documented and accredited manner, the completion of the investigation to the *Whistleblower* and the *Reporter*, indicating whether or not there has been a *breach of* the regulations applicable to *CELSA.* Alternatively, and if the circumstances so recommend, the means used to inform could be hand-delivery, on the premises *of the Organisation*, by a member of the *Ethics Committee*, with acknowledgement of receipt

The documentary evidence of the communication shall be recorded in the *Register Book*, and the file shall be blocked to prevent further processing. However, if it emerges from the investigation of the file that the *Whistleblower* acted solely with the intention of harming the *Reporter* or a *Third Party* due to personal interests, the *Ethics Committee* must assess the possibility that the *Whistleblower*'s actions may constitute a breach of any of the rights of the *Reported Party*. In such a case, and provided that it is necessary for the *Reporter* to be able to exercise his or her rights of effective protection before the courts.

6. The Internal Information System Log Book

The *Internal Information System logbook* is a secure record of all *Enquiries* and *Complaints* received, as well as any decision and/or action taken in relation thereto. It is the tool to be used by the *Ethics Committee* to order, document and safeguard the documentation generated in the process of managing the *Communications* received through the *Internal Information System.*

When the *Ethics Committee* receives a *Communication*, it shall register it with a unique identification number so that it can be easily located by all those involved in the procedure. In this regard, the *Register* is equipped with the necessary technical and organisational security measures to ensure the highest possible level of confidentiality. In addition, the *Ethics Committee* shall keep a record of the *Notifications* sent through the communication channels implemented by *CELSA*.

The platform enabled by the *Organisation* for the management of the Internal Reporting System shall be the preferred means of communication for performing communications and notifications with the *Reporting Party,* unless the latter has designated another secure means of notification. It shall also be the means for performing *Communications* to other *Relevant Interested Persons* concerned in the process of managing and investigating *the Whistleblowing.*

In order to record and store in the *Log-book* the information relating to the *Communications* received, *the Organisation* shall have logical locations with restricted access and classified by year and file number. It will also allow the management of the *Communications* reported by *Members of the Organisation*, *Business Partners* and *Third Parties* from the initial reception phase, until the resolution and archiving of the *Complaint*.

The *Register Book* will be organised in locations according to the type of *Communications* received.

When a *Communication* is received*,* through the *Internal Information System* or any other communication channel enabled for this purpose by *CELSA,* the *Ethics Committee* will assign a File number and create a File Folder in the *Register Book*, which will include the documentation generated in relation to each *Communication.* Those containing data relating to notifications under investigation or awaiting resolution shall be considered live records.

Custody of and access to the *Register* is the responsibility of the *Ethics Committee*. Likewise, the personal data shall be incorporated with restricted and confidential access, the ownership of which belongs to the *Organisation*, for the purpose of adequately managing the *Internal Information System, and* shall record, as a minimum, the personal data relating to the *Communications* received, as well as the investigations performed. The data shall be kept only for the essential time and, in no case, for a period of more than ten (10) years.

7. Protection of personal data

The *Organisation* shall process the data received through the *Internal Information System in* accordance with current data protection regulations and its policies and procedures in this regard, including, but not limited to, its Privacy Policy.

CELSA is committed to maintaining strict privacy protection, data security and data retention, in accordance with applicable regulations and *CELSA'*s Privacy and *Compliance* policies and procedures. These rules will also apply with respect to all personal data related to reports performed in accordance with this *Policy*.

The processing of personal data is based on the legitimate interest of *CELSA*, as well as the consent of the *Informant,* if applicable, the purpose of managing and resolving any *Inquiry* or *Complaint*, as well as to analyse the criticality of the reported facts, perform, if necessary, an investigation into possible *Infringements*, adopt the necessary interim measures and, if necessary, initiate the corresponding internal or legal actions. The use of the information obtained in this way for purposes other than those motivating the implementation of the system is neither permitted nor envisaged.

In order to comply with these purposes, certain personal data and information must be collected, either directly through the *Informant*, through the person/s determined by the *Organisation* or through authorised *Third Parties* specifically contracted for this purpose, who will guarantee the highest level of confidentiality and technical security.

All *Members of the Organisation* are obliged to provide true, accurate, truthful and lawful information, and are solely responsible for any false or inaccurate statements they provide, as well as for the internal, administrative and/or legal consequences that may apply.

The *Organisation* shall ensure in all cases that the different communication channels of the *Internal Information System* constitute a secure medium, equipped with the measures required by the regulations on Personal Data Protection and information security.

7.1. Retention of information

CELSA shall process, manage and keep the information and personal data contained in the *Complaints*, investigations, reports and other documentation in accordance with the time periods established in the current legislation on personal data protection and other applicable regulations, i.e. the information from the *Informants* may be kept for no more than three (3) months from its entry in the *Internal Information System*, except for those data essential to decide whether to initiate an investigation into the reported facts, which may be kept for a longer period of time. Once this period of investigation has expired, the data shall be deleted from the *Internal Information System*.

With the exception of the above, when the purpose is to leave evidence of *CELSA*'s *Criminal Prevention Model*, the retention period will be that determined for that purpose, and in particular

that of the demonstration of compliance with labour legislation, as described below.

This information will also be under the custody of the *Ethics Committee* and will be deleted, blocked or anonymised at the end of the legal deadlines and in accordance with the Privacy Policies specified in the information entry channels.

CELSA will keep a record of all *Complaints* received. These records and the personal data they contain will be kept confidential. The records will be kept for no longer than is necessary and in any event for as long as is necessary to comply with any applicable legal requirements from time to time.

In particular, *CELSA* will keep the Whistleblower's personal data for the time necessary to decide whether to initiate an investigation into the facts or conduct reported and, once decided, it will be deleted, and may be processed outside the system to investigate the facts for the time necessary to make a decision. Once the investigation of the communication has been completed and the appropriate actions have been taken, as the case may be, the data of those Reports that have been processed will be duly blocked in order to comply with the legal obligations that may apply in each case.

In the event that it is decided not to follow up on the *complaint* filed, the information may be retained in anonymised form.

7.2. Data protection rights of the *Informant*

As an *Informant*, the reporting person may exercise, at any time and under the terms provided for by the applicable regulations, access to the personal data concerning him/her. If this person believes that the data is incorrect or incomplete, he/she may request its rectification in accordance with the applicable legislation. He or she may request that the data be deleted if they are no longer required, except where there is a legal obligation to retain them. You may also request that the processing of your personal data be restricted, object to the processing, or request the portability of your data, and you have the right to withdraw your consent. You will be informed at the time of filing the *Complaint* how you can exercise all these rights.

If you consider it appropriate, you can also file it with the competent data protection authority.

7.3. Further information on the processing of personal data

Individuals may obtain further information about the processing of their personal data and the contact details of the entity's possible representative for this purpose, as well as of the Data Protection Officer or other privacy officer.

8. Disciplinary regime

In accordance with the provisions of *CELSA's Internal Information System Policy* and this document, all *CELSA Members*, regardless of their organisational group and functional location, have an obligation to comply with the principles and procedures set out in these texts, as well as an obligation to report any contravention thereof.

Consequently, when the *Ethics Committee* becomes aware of a breach of the provisions of these texts, it shall propose, as appropriate, to the *Board of Directors*, through the *Audit and Control Committee,* and to the *Management Committee*, disciplinary measures in the employment sphere (for *Members of the Organisation*) or in the contractual sphere (in commercial relations with *Business Partners*) that it deems proportionate to the risk or damage caused.

The Steering *Committee* is responsible for taking the relevant decisions with regard to facts related to serious or very serious administrative offences, occupational safety offences and any other contravention of *CELSA*'s internal regulations or the applicable legal system that does not have criminal implications.

The *Board of Directors* is responsible for taking the relevant decisions regarding those events that may give rise to criminal liability for *CELSA*, once informed by the *Ethics Committee* through the *Audit and Control Committee*

These measures will not only apply to the individuals whose conduct has caused the risk or damage, but also to the *Members of the Organisation* who have not followed the procedures established by *CELSA* for prevention and response, a circumstance that is in itself considered a *breach* of the values and ethical principles to which *CELSA* is committed.

The measures adopted from a legal perspective will always be respectful of the applicable regulations, without losing forcefulness or proportionality with the seriousness of the facts from which they arise, informing the Workers' Legal Representatives if appropriate.

In the event that there are unequivocal indications that the actions of any *Member of the Organisation* could constitute a criminal offence, this circumstance shall be reported to the competent Public Authorities for their knowledge and prosecution. Such notification shall be accompanied by the evidence and/or indications that may have been gathered in this respect.

Annex I

Examples of possible behaviours to communicate

Some assumptions that could be communicated through CELSA's *Internal Information System* are described below

- Reporting an event that may constitute a money laundering and terrorist financing offence.
- Avoid bribery and corruption.
- Working in a safe and healthy environment.
- Avoid conflicts of interest in any action related to professional development.
- Avoid discrimination, as well as sexual and non-sexual harassment.
- Prevent internal fraud.
- Protect fair competition and international trade rules.
- Responsible use of company assets.
- Protect fiscal integrity, business integrity and integrity of financial records.
- Creating an inclusive and respectful workplace.
- Protect *CELSA* information, the dissemination of which may affect the interests of the Group or the legitimate rights of third parties.
- Protect *CELSA* from cyber-attacks.
- Respect urban and land-use planning regulations.
- Protect human rights.
- Respect global and local laws and customs, limiting relations with public administrations to a professional environment.

Annex II

Some possible investigative steps in the investigation of the *Complaints*

The **investigative steps** that may be taken include:

1. **Interview with the *informant*** to expand on the information contained in the complaint.
2. **Witness statements**.
3. **Requesting external assistance** from suitably qualified and experienced professionals.
4. **Obtaining documentation from the company** relevant to the clarification of the facts.
5. **Analysis of processes and procedures relevant** to the research.
6. **Adoption of surveillance measures** through detectives or computer, telematic or audiovisual means, provided that these are in accordance with the principles of appropriateness, sufficiency and strict proportionality, with respect for the fundamental rights of privacy and secrecy of workers' communications.
7. **Statement of the *Defendants***.
8. **Any other actions that the investigator deems necessary** for the proper verification of the facts and identification of those responsible.