Internal Information System (SII) Policy of COMPAÑIA EUROPEA DE COSPELES, S.A (CECO S.A.)

Content

VERSION LOGGING.

This document has been approved by the joint administrators of Compañía Europea de Cospeles, S.A. on 30th of November of 2023.

Revision	Date	Comment
V. 1	November 2023	Initial Version of the SII Policy

1 OBJECT

Law 2/2023 enacted on 20 February 2023, regulating the protection of persons reporting regulatory and anti-corruption breaches (hereinafter, the "Whistleblower Protection Act"), adopts the provisions of Directive (EU) 2019/1937 of the European Parliament and of the Council, dated 23 October 2019, and obliges companies such as CECO S.A. to establish an Internal Information System (hereinafter, "SII") in accordance with its terms.

The main purpose of the implementation of an SII is to safeguard those individuals who, in the context of their employment or professional activity, identify serious or very serious violations of the law, and who report them through the specified procedures. It also seeks to promote and strengthen the culture of reporting as a means of preventing and detecting irregular behavior.

The purpose of this policy is to include the fundamental principles that guide the SII of CECO S.A., as well as other aspects contemplated in the aforementioned law. This includes the channel or method designated to receive reports related to violations, the process to be followed for the treatment of such complaints, the Head of the SII and the protection measures and guarantees established for the benefit of whistleblowers, which will only apply to complaints contemplated by law.

2 SCOPE.

I. This Policy is applicable to all individuals linked to CECO S.A. who, through the procedures established in this Policy, report:

- Acts or omissions that have the potential to constitute serious or very serious criminal or administrative offences. In all cases, this will cover all serious or very serious criminal or administrative offences that result in economic losses for the Treasury and Social Security.
- Behaviours that, through action or omission on the part of a member of CECO S.A., have a real impact on the professional relationship with CECO S.A. of the person mentioned in the communication, related to the commission of acts contrary to the rules of the Code of Conduct of CECO S.A. or to the other

provisions of the Company's internal regulatory system in a work or professional environment.

- Any act or omission that may constitute an infringement of European Union law.

Individuals linked to CECO S.A. are considered to be those who are currently partners, employees, and collaborators of the Company (including, among others, external advisors and the like).

II. This Policy is also applicable to persons who provide information about any of the actions or omissions mentioned in point (I) above in a work or professional environment, even if they are not individuals linked to CECO S.A. This includes:

- Anyone who works for CECO S.A., is under its supervision and direction, as well as its contractors, subcontractors and suppliers.
- Individuals who were previously linked to CECO S.A. and have terminated their employment or statutory relationship with the Company.
- Volunteers and interns, regardless of whether they are paid or not.
- Persons whose employment relationship has not yet begun, in situations where information on infringements has been obtained during the selection process or pre-contractual negotiation.

3 INTERNAL INFORMATION SYSTEM.

The Internal Information System (SII) of CECO S.A., referred to in this Policy, is the preferred method for notifying the actions or omissions mentioned in point 2 above. The SII is mainly composed of the Internal Whistleblowing Channel designated to receive notifications within the scope of this Policy, the Head of the SII and the process that must be followed for the management of these notifications, called "Procedure for the management and processing of communications received in the Internal Whistleblowing Channel" (SII Management Procedure).

3.1 GENERAL PRINCIPLES

The SII of CECO S.A. will be managed internally independently and is governed by the following general principles:

ACCESSIBILITY

It is ensured that all persons referred to in point 2 of this Policy are able to communicate information about the violations mentioned in that point, either in writing or verbally, and have the option to do so anonymously.

GOOD FAITH

It is essential that the whistleblower act in good faith and honestly when he or she becomes aware of serious harmful or potentially harmful facts. This principle excludes the submission of false or distorted information, as well as any information obtained illegally.

DILIGENCE, SPEED AND EFFICIENCY

All necessary actions will be taken to verify and clarify the facts reported with the utmost diligence, speed and efficiency, considering the complexity of the facts. The aim is for CECO S.A. to be the first to be aware of possible irregularities, respecting at all times the provisions of the SII Management Procedure.

INTEGRATION

The Internal Whistleblowing Channel established at CECO S.A. is fully integrated into the SII.

SECURITY, CONFIDENTIALITY AND COMPLIANCE WITH DATA PROTECTION REGULATIONS

The CECO S.A. SII has been designed and established in a secure manner to guarantee the confidentiality of the identity of the informant and any third party mentioned in the communication. Likewise, the rights to privacy, honor, defense and presumption of innocence of the people involved in the investigation process that arises as a result of a communication made through the SII are protected, complying with data protection regulations. The disclosure of the identity of the informant, if known, and that of third parties mentioned in the communication shall only be carried out before judicial authorities, the Public Prosecutor's Office or the competent Administrative Authority as part of a criminal, disciplinary or punitive investigation, after notification to the informant or the affected party, provided that this does not prejudice the ongoing investigation.

PROPORTIONALITY, OBJECTIVITY AND RESPECT FOR THE GUARANTEES OF THOSE INVOLVED

Actions within the SII will be carried out in a proportional and objective manner, fully respecting current legislation and the rights of all parties involved. All the protections established in the SII Management Procedure are guaranteed for the persons involved, and retaliation against whistleblowers is expressly prohibited. The persons affected by the communication have the right to be informed of the facts attributed to them and to be heard at any time. Once informed, they may request access to the information and documentation in the file resulting from the communication, with due precautions to protect the identity of the informant.

ADVERTISING

Clear and easily accessible information is provided on the Internal Whistleblowing Channel of CECO S.A. so that informants can make use of it. All this information can be found in this Policy and is available on the website of CECO S.A. at the following address: https://ceco-sa.com/. In addition, information on the existence of the SII and the Internal Whistleblowing Channel will be included in the Company's training programs.

3.2 INTERNAL WHISTLEBLOWING CHANNEL.

Within the Internal Information System (SII) of CECO S.A., the Company's Internal Whistleblowing Channel is integrated, which is considered the preferred channel for reporting the conduct described in section 2 of this Policy.

Complaints related to sexual or gender-based harassment by employees of CECO S.A., in accordance with the guidelines of the Protocol for the Prevention of Sexual and Gender-Based Harassment in the Workplace included in the Company's Equality Plan, will also be included in the aforementioned Internal Complaints Channel (and, consequently, in the SII of CECO S.A.). However, the Company's employees have the option to file complaints of sexual or gender-based harassment directly through the Internal Whistleblowing Channel, in the same manner as any other whistleblower referred to in section 2 of this Policy.

The aforementioned Internal Whistleblowing Channel offers the following possibilities:

(a) To permit the submission of complaints in writing or orally, or in both forms, in accordance with the conditions set out in the Whistleblower Protection Act.

b) Enable the reporting person, when making the report, to indicate an address, e-mail address or safe place to receive notifications.

(c) To facilitate the submission and subsequent processing of anonymous complaints.

(d) Provide clear and accessible information to whistleblowers on the external channels available to inform the competent authorities and institutions.

e) Receive any other communication or information that is not within the scope defined in section 2 of this Policy. However, these communications and their senders will not be subject to the application or protection afforded by this Policy.

Appropriate measures will be taken to ensure the confidentiality of communications sent through non-designated channels or to personnel who are not authorized to process them, and these communications will be required to be forwarded immediately to the Head of the SII.

3.3 SII PROCEDURE

The SII Procedure establishes the rules for the management and processing of communications received through the Internal Complaints Channel, which is integrated into the Internal Information System of CECO S.A.

Complaints related to sexual harassment or gender-based harassment, filed by employees of CECO S.A. in accordance with the guidelines of the Protocol for the Prevention of Sexual and Gender-Based Harassment at Work, included in the Equality Plan of CECO S.A., will be handled as stipulated in the Protocol itself.

In the event that the facts indicated in the complaint indicate indications of criminal conduct, the Public Prosecutor's Office or the European Public Prosecutor's Office, as appropriate, will be informed.

3.4 EXTERNAL INFORMATION CHANNELS.

Without prejudice to the priority channel offered by the Internal Whistleblowing Channel, those who wish to report also have the option of using the channels enabled by the government authorities for this purpose (called "External Channels"), either directly or through the internal channels mentioned above.

Whistleblowers have the following external channels for reporting breaches of European Union rules and interests:

European Anti-Fraud Office (OLAF):

OLAF has an external channel for reporting fraud or other serious irregularities with potential negative repercussions on EU public funds (revenue, expenditure or assets of the EU institutions).

Complaints can be made anonymously through the following means:

Online, through the Fraud Reporting System:

https://fns.olaf.europa.eu/main_es.htm

By mail:

European Commission
European Anti-Fraud Office (OLAF)
1049 Brussels Bélgica.

European Public Prosecutor's Office (EPPO):

The European Public Prosecutor's Office (EPPO) is an independent body of the European Union responsible for investigating crimes against the EU's financial interests and prosecuting and prosecuting them, in particular with regard to fraud, corruption, money laundering and cross-border VAT fraud. Complaints may be made:

Online, via the "Report a Crime" service:

https://www.eppo.europa.eu/es/form/eppo-report-a-crime

The European Public Prosecutor's Office does not receive anonymous complaints, so reporting breaches through this channel requires prior identification of the whistleblower.

External channels enabled at the national level:

At the national level, whistleblowers will have access to the external channel set up for this purpose by the Independent Authority for the Protection of Whistleblowers, A.A.I. At present, both this entity and the channel are pending incorporation.

However, the following channel currently exists at the national level.

National Anti-Fraud Coordination Service (SNCA)

The SNCA is the body responsible for coordinating actions to protect the European Union's financial interests against fraud, in collaboration with the European Anti-Fraud Office (OLAF). Through the whistleblowing channel set up, information can be reported about fraud or irregularities affecting European funds.

Complaints can be made online, through the Infofraud service:

https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/Paginas/denan.aspx

The SNCA form does not allow anonymous reports, so the communication of violations through this channel requires the prior identification of the informant.

In addition, the SNCA has set up an email address through which doubts and questions can be raised:

consultasantifraude@igae.hacienda.gob.es

On the other hand, the Law on the Protection of Whistleblowers allows any natural person to report the commission of actions or omissions that fall within the scope of application of said law to the **Independent Authority for the Protection of Whistleblowers** or to the corresponding regional authorities and bodies.

4 RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM.

The person responsible for the management of the Internal Information System (SII) of CECO S.A., appointed by the management of the organization, holds the position of Compliance Officer of the company, a one-person position that assumes the responsibility of supervising the Internal Information System of CECO S.A.

The designation of the person responsible for the SII will be notified to the Independent Authority for the Protection of Whistleblowers or, where appropriate, to the competent authorities and bodies of the Autonomous Communities, within their respective competences.

The person in charge of the SII of CECO S.A. will carry out diligently and, in the absence of conflict of interest, the resolution of the procedures initiated as a result of the information received through the designated Internal Whistleblowing Channel, guaranteeing the correct application of the SII Procedure. In situations of conflict of interest, the administrative body will appoint the person in charge of such resolution, who will be subject to the same responsibilities and principles that govern the person in charge of the Internal Whistleblowing Channel.

The person in charge of the SII will keep a detailed record of the information received, in a document called a Record Book, and of the resulting investigation files, ensuring the confidentiality of the information at all times.

In order to carry out his/her duties effectively, the Head of the SII has the necessary material and human resources. These functions are exercised independently and autonomously with respect to other bodies of CECO S.A., following the principles of neutrality, honesty and objectivity towards all parties involved.

5 PROTECTION MEASURES AND GUARANTEES.

5.1 SCOPE.

The protection provisions and guarantees described in this section shall be mandatory for CECO S.A. in the event that the Whistleblower Protection Law is applicable. Informants must act in good faith and must follow the principles of truthfulness and proportionality in their communications, limiting themselves to referring only to facts related to CECO S.A. Submission of false or malicious communications or information could result in penalties.

Persons who report or disclose violations within the scope of this Policy are entitled to the safeguards set forth in this Policy, provided that they comply with the following conditions:

a) Have reasonable grounds to believe that the information provided is truthful at the time of communication or disclosure, even if they are unable to provide conclusive evidence, and that such information is within the scope of this Policy.

b) The communication or disclosure has been made in accordance with the requirements set forth in this Policy.

This protection extends to any natural person who, within the organization in which the reporting person works, assists or is related to the reporting process, whether as a representative of the workers, colleagues or family members, and to any legal entity for which the reporting person works or with which he or she has some type of employment relationship or significant influence.

The protection measures contemplated in this Policy do not exclude those established in the specific regulations that may be applicable and do not prevent the application of the rules related to the criminal process, including the corresponding investigations.

Persons who report or disclose:

a) Information contained in communications that have been rejected by any Internal Whistleblowing Channel or for any of the following reasons:

• When the facts reported lack credibility.

• When the facts reported do not constitute legal violations within the scope of this Policy.

• When the communication is clearly unfounded or there are reasonable indications that it was obtained in a criminal manner.

• Where the communication does not provide new and significant information on infringements compared to a previous communication that has already been the subject of relevant proceedings, unless new legal or factual circumstances arise that justify different treatment.

b) Information related to interpersonal disputes or affecting exclusively the reporter and the persons mentioned in the communication or disclosure.

(c) Information that is already publicly available or based on mere hearsay.

d) Information related to violations in procurement procedures involving classified information or information that has been declared secret or reserved, or those that require special security measures according to the legislation in force or when required by the protection of interests essential to the security of the State.

e) Data concerning violations in the management of contracting processes that involve classified information or that have been designated as secret or confidential, as well as those procedures that require particular security measures according to current legislation.

5.2 NO RETALIATION.

In accordance with the Whistleblower Protection Act, acts that constitute retaliation, including threats of retaliation and attempts at retaliation against individuals who submit a communication in accordance with this Policy, are explicitly prohibited.

Retaliation is defined as any act or omission that is prohibited by law, or that, directly or indirectly, results in unfavorable treatment that places the persons who suffer it at a particular disadvantage in the work or professional context because of their status as informants.

By way of example, the following are considered retaliation:

• Suspension of the employment contract, dismissal or termination of the employment or statutory relationship; the application of disciplinary sanctions of any kind; demotion or denial of promotion, as well as any substantial modification of working conditions; and the non-conversion of a temporary employment contract into an indefinite one, if the person who submitted the communication had legitimate expectations to that effect.

• Damages, including reputational damages, or financial loss, coercion, intimidation, harassment or ostracism.

• Negative evaluation or unfavorable references in relation to work or professional performance.

• Blacklisting or the dissemination of information in a specific sectoral area, which makes it difficult or impossible for the person to access employment or the contracting of works or services.

• Denial or revocation of licenses or permits.

• Denial of training opportunities.

5.3 SUPPORT AND PROTECTION MEASURES

The Whistleblower Protection Act also provides for a series of support and safeguard measures for those whistleblowers who report the actions or omissions indicated in Article 2 and described in Section 2 of this Policy. These measures, which may be provided by the Independent Whistleblower Protection Authority or another competent entity, without prejudice to the specific support and assistance measures that CECO S.A. may implement, are detailed as follows:

SUPPORT MEASURES

Individuals who report or disclose violations covered by this Policy through the procedures set forth in this Policy will have access to the following support measures:

(a) Obtaining complete, independent and free information and advice on available procedures and remedies, protection against retaliation and the rights of the person concerned.

b) Effective assistance by the competent authorities vis-à-vis any relevant entity involved in its protection against retaliation, including certification of its right to protection under the Whistleblower Protection Act.

(c) Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with Community legislation.

(d) Financial support and psychological support, in exceptional circumstances, if determined by the Independent Whistleblower Protection Authority after assessing the circumstances arising from the submission of the communication.

Protection of the Whistleblower in accordance with the Whistleblower Protection Act.

PROTECTIVE MEASURES

In accordance with the provisions of the Law on the Protection of Whistleblowers, the following protection measures are established:

(a) The whistleblower shall not be held liable for the disclosure of information as long as he or she has reasonable grounds to believe that such disclosure was necessary to expose a breach as defined in the Whistleblower Protection Act. This measure will not exempt from criminal liability. This principle applies even to communications made by workers' representatives, despite being subject to legal obligations of confidentiality or non-disclosure of confidential information, without prejudice to the specific protection regulations established by labour law.

(b) The informant shall not be liable for the acquisition of or access to the information communicated, provided that such acquisition or access does not constitute an offence. Any other liability that may arise from actions or omissions unrelated to communication or that are not necessary to disclose a breach under this Policy shall be governed by applicable law.

(c) In legal proceedings dealing with harm suffered by whistleblowers, once the whistleblower has reasonably demonstrated that he or she has made a communication and suffered harm, it shall be presumed that the harm occurred in retaliation for reporting. In such cases, it will be up to the person who took the prejudicial measure to prove that the action was based on duly justified grounds and was not related to the communication.

(d) In legal proceedings, including those relating to defamation, copyright infringement, breach of secrets, violation of data protection regulations, disclosure of trade secrets, or claims for compensation based on labor or statutory laws, whistleblowers and persons legally protected by the Whistleblower Protection Act shall not be held liable for communications covered by such law. Such persons have the right to allege, as a defence in such legal proceedings, that they made the communication whenever they have reasonable grounds to believe that such communication was necessary to expose an infringement in accordance with the aforementioned law.

(e) During the processing of the file, the persons affected by the communication shall have the right to the presumption of innocence and the rights of defence. Restricted access to the file will be allowed, and the confidentiality of identity and data of the procedure will be maintained.

6 INFORMATION LOGBOOK

The SII will keep a record of the information received and the resulting internal investigations, guaranteeing due confidentiality and complying with personal data protection regulations. This register will contain the following information about the communications:

- **Date of receipt**
- **Identification code**
- **Actions taken**
- **Measures taken**
- **Closing Date**

This register shall not be available to the public and its contents may only be accessed in whole or in part upon justified request by the competent judicial authority, in the context of and under the supervision of a judicial proceeding.

7 PROTECTION OF PERSONAL DATA

CECO S.A. will be responsible for the processing of personal data derived from the use of the internal information system and the management of internal investigations (hereinafter, the "Personal Data"), in accordance with this policy and the provisions of the regulations on the protection of personal data.

If they wish, interested parties can contact the Request Manager for the exercise of rights at the email address protecciondatos@ceco-sa.com.

Categories of Personal Data and Origin of Data

The Personal Data processed within the scope of the Internal Whistleblowing Channel will include identification, contact, economic, professional and employment information, as well as data related to the facts that are the subject of the communication. In exceptional circumstances, and when necessary in the context and according to the nature of the investigation, data of special categories may also be processed, such as information on criminal or administrative offences, data on health, sexual orientation or life, ethnic or racial origin, and any other data derived from the use of the Internal Complaints Channel.

The personal data processed in this area will be provided directly by the data subjects or, where appropriate, by the informants. In addition, they may be provided by workers and third parties who are requested to provide information in the context of the Internal Whistleblowing Channel during the investigation, if it is carried out, and will always be related to the facts investigated.

About the Processing of Personal Data (Purposes, Legal Bases and Retention Periods)

(i) Purposes of the processing and legal basis of the Internal Whistleblowing Channel.

Personal Data will be processed for the purpose of processing the communication, deciding on its admission or inadmissibility, and, in case of admission, carrying out the corresponding investigation, as well as adopting the relevant corrective and disciplinary

measures. This data processing will be carried out in accordance with the legal obligations of CECO S.A. in relation to the existence and management of an information system, and in accordance with the Regulations on the Protection of Informants.

(ii) Retention of data in the Internal Whistleblowing Channel

Personal Data will only be processed within the Internal Whistleblowing Channel for the time necessary to make a decision on its admission and will not be communicated to third parties, unless it is necessary for the proper functioning of the system or to make a decision regarding the admission of a communication for processing.

In particular, when the submission of communications through the Internal Whistleblowing Channel is verbal, the informant is aware that the verbal communications will be recorded and documented by recording the conversation in a secure, durable and accessible format, or through the subsequent complete and accurate transcription of the recording of the conversation. In any case, the informant will be given the opportunity to verify, rectify and accept the transcript of the conversation by signing it.

Once the decision on admission or inadmissibility has been made, the Personal Data will be deleted from the Internal Complaints Channel and, in any case, if no decision has been made in this regard, three months after its registration. However, limited information may be retained for a longer period of time in order to provide evidence of the operation of the system.

(iii) Processing of internal investigation and subsequent data retention

In the event that the communication is admitted for processing, the Personal Data may be processed outside the Internal Whistleblowing Channel by the team responsible for the investigation, for the purpose of carrying out the corresponding internal investigation. This processing will be carried out in compliance with the legal obligations of CECO S.A. (art. 6.1.c GDPR).

Personal Data will be processed for the time necessary to carry out the investigation and comply with legal obligations. If it is found that the information provided or part of it is not true, it will be immediately deleted as soon as this circumstance becomes known, unless the lack of veracity may constitute a criminal offence, in which

case the information will be kept for the time necessary to process the legal proceedings. Once the investigation is concluded, the Personal Data will be kept for the time necessary to adopt and execute the corresponding measures and, after that, for the maximum limitation period for legal or contractual actions. Under no circumstances will the data be kept for a period exceeding ten years.

(iv) Recipients of personal data and international data transfers

Personal Data will be processed by the Head of the SII and by those persons of the CECO S.A. organization who, in accordance with the scope of their competences and functions, and with the Law on the Protection of Whistleblowers, are necessary. They will only be communicated to third parties when it is appropriate to carry out the investigation (e.g. service providers or external consultants) or for the subsequent adoption of appropriate corrective action (e.g. the head of human resources when disciplinary action against an employee is necessary).

The identity of the informant may be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or punitive investigation. Disclosures made for these purposes will be subject to safeguards set forth in applicable law. In particular, the individual shall be informed before revealing his or her identity, unless such information may jeopardise the investigation or judicial proceedings.

There are no plans to make international transfers of Personal Data outside the EU. However, given the international activity of the entity, if the facts subsequently reported or investigated have circumstances that make the international transfer of Personal Data necessary, appropriate measures will be adopted in accordance with the applicable regulations. In addition, in the event that the processing of data by any of the service providers assisting in the management of the Internal Whistleblowing or Investigation Channel involves international transfers, these will be carried out in accordance with the applicable regulations, and information may be requested on the guarantees adopted by the entity.

(v) Exercising personal data protection rights

Interested parties may contact the Request Manager for the exercise of rights through the email address protecciondatos@ceco-sa.com, to exercise their rights of

access, rectification, opposition, deletion, portability, limitation or any other right recognized by the applicable regulations in relation to the data contained in the corresponding file, in accordance with current legislation. However, in the event that the person to whom the facts are attributed or any third party exercises their right of access, the identifying data of the informant will not be communicated.

In addition, the holders of Personal Data may submit complaints or requests related to the protection of their Personal Data to the corresponding data protection authority: in Spain, the Spanish Data Protection Agency (https://www.aepd.es).