COMMUNICATIONS MANAGEMENT PROCEDURE SPEAKUP

Versión 1, English

November 10, 2023

Table of Contents

1. AIM OF THIS PROCEDURE

Capgemini España, S.L. (hereinafter, "**Capgemini**" or the "**Company**") has implemented an Internal Information System (hereinafter, the "**System**") with the aim to defend its corporate values and protect its ethic culture.

Also, in accordance with Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law, and Spanish Law 2/2023, of 20 February on the protection of persons who report regulatory offences and the fight against corruption, which transposes it into the Spanish law, Capgemini's System is set up as the preferred channel to inform about ethic concerns regarding potential irregularities or non-compliances.

The System is mainly formed by the following:

- The Speak Up Policy of Capgemini Group (the "**Policy**").
- This Procedure regarding the management of communications (the "**Procedure**"), which develops the referred Policy at a local level.
- The SpeakUp tool, used by Capgemini Group as a system for the receipt of reports. It is operated by Convercent, an independent services supplier, and allows communications to be submitted both by phone or through the webpage. Both modalities guarantee confidentiality of the information and offer the possibility to submit anonymous communications.
- The Responsible of Capgemini's System is the one in charge of its management and the handling of the investigation files.

This Procedure establishes **(i)** the guidelines to follow when submitting a communication about ethic concerns regarding potential irregularities or non-compliances and/or non-compliances related to the matters included in section 2.2. below, as well as **(ii)** the procedure to be followed by Capgemini when receiving and managing the communications submitted through the System.

2. SCOPE OF APPLICATION

2.1 SUBJETIVE SCOPE OF APPLICATION

This Procedure applies to Capgemini and therefore to all people professionally linked to the Company.

To this end, by way for example but not limited to, **this Procedure shall be applicable to the whistleblowers** who maintain or have maintained an employment or professional relationship with Capgemini, the shareholders, members of the Company's administrative, management or supervisory body, including non-executive members, any person working for or under the supervision and direction of contractors, subcontractors and suppliers, volunteers, trainees, whether or not they receive remuneration, as well as those whose employment relationship has not yet commenced, where information about breaches has been obtained during the recruitment process or pre-contractual negotiation. All of the above, on terms that are compatible with their relationship with Capgemini.

The different **protection measures** foreseen along this Procedure will be applied to all whistleblowers, related third parties, and persons affected by the communication. Within this context:

- Whistleblower means any person who communicates an ethical concern regarding potential irregularities and/or non-compliances related to section 2.2 below, including all above-mentioned persons.
- Related third parties means all Capgemini members assisting the Whistleblower during the process, as well as all people related to the Whistleblower who may suffer reprisals, legal representatives of the workers assisting the Whistleblower, colleagues, or family members. It includes also legal entities for which the Whistleblower may work o with whom he or she maintains an employment relationship or in which he or she holds a significant participation.
- Person affected by the communication means any person to which an action or omission which constitutes and infringement of Capgemini's System in accordance with the Policy is attributed in the context of a communication.

2.2 MATERIAL SCOPE OF APPLICATION

This Procedure is applicable in relation to requests for advice and guidance or communication of reports that may arise regarding actions or omissions constituting violations occurring in an employment or professional context relating exclusively to the following areas:

- European Union's Law Infractions related to, among other, the following areas: public procurement, financial sector, prevention of money laundering or terrorist financing, product safety and compliance, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and animal welfare, public health, consumer protection, protection of privacy and personal data, and security of networks and information systems, Union financial interests and internal market[1].

[1] Includes offences covered by: (i) the Annex to EU Directive 2019/1937, in particular Part I, B, on financial services, products and markets and the prevention of money laundering and terrorist financing; (ii) Article 325 of the Treaty on the Functioning of the European Union (TFEU) concerning the fight against fraud; or, (iii) affecting the internal market as set out in Article 26 of the TFEU.

- Serious or very serious criminal or administrative offences, including those involving financial loss to the Treasury and Social Security.
- Occupational health and safety offences under labour law.
- Violations of Cagpemini's Code of Business Conduct and any other policies or procedures implemented.

This System is not enabled for filing grievances or raising human resources concerns, such as performance review, compensation, career development and other human resources related issues. Local grievance communication channels should be used for these matters.

3. PRINCIPLES OF ACTION

In line with the provisions of the Policy, the principles of action that should always govern the System, as well as the use of the System by Whistleblowers and persons involved in the process, are as follows:

- **Confidentiality**: all members of Capgemini who, as part of their duties may be involved in the process, must maintain confidentiality regarding the communication raised, as well as the identity of the Whistleblower, if known, the Person(s) affected by the communication, and the facts and documentation that are the subject of the communication.

  In relation to confidentiality, it should be noted that SpeakUp allows communications to be submitted anonymously.

  To this end, the corresponding mentions to this effect will be made in all communications and actions carried out or documents generated in the investigation. Likewise, all communications made during the procedure, as well as the rest of the documentation that forms part of it, shall refer to a coded file number and the persons involved shall be assigned a correlative numerical reference, omitting in all cases any identification of the persons involved.

  Notwithstanding the foregoing, files may be disclosed to third parties for the purposes of judicial and administrative proceedings in accordance with the Capgemini Privacy Policy.

- **Good Faith**: communications must be made in good faith, meaning acting with an honest belief and intent.

  The System may not be used for any unlawful, personal or bona fide purpose and Capgemini will not tolerate any false or misleading information. The Whistleblower shall only report information that, to the best of his or her knowledge, is accurate at the time it is provided.

- **Cooperation**: all members of Capgemini have an obligation to cooperate with the Responsible of the System or the team designated to investigate the communication if requested to do so.

  In turn, the Whistleblower will provide any evidence that was lawfully obtained at the time of the initial disclosure.

- **Prohibition of Retaliation**: Capgemini undertakes not to retaliate in any way against those who report in good faith an alleged irregularity/non-compliance, or against those who assist Whistleblowers or who participate or cooperate in good faith in the clarification of the reported facts.

  Retaliation shall be understood to be any act or omission prohibited by law or which, directly or indirectly, entails unfavourable treatment that places the person who suffers it at a particular disadvantage in the employment or professional context solely because of their status as a Whistleblower or their collaboration in the handling of information.

  By way of example, the following may be considered as retaliation:

  - Suspension of employment contract, dismissal or termination of employment or non-renewal - unless in the regular exercise of managerial authority under employment law.
  - Damages, including reputational damage, financial loss, coercion, intimidation, harassment or ostracism.
  - Negative references with regard to professional work.

- Blacklisting or dissemination of information in an industry that hinders access to or promotion in the workplace.
- Denial or cancellation of leave or training.

In addition, any retaliation by a Capgemini employee will be grounds for disciplinary action, including termination of employment under applicable law.

If you witness or experience any retaliation, it is important that you report it immediately: you can contact us through the "*message*" functionality of the SpeakUp portal or by writing to us at ethics@capgemini.com.

4. INTERNAL AND EXTERNAL CHANNELS

Capgemini has a system that allows all its employees, as well as any third parties with whom it has a relationship and who are listed in section 2.1. of this Procedure, to report any irregularity to the Company, as defined in section 2.2. above.

Specifically, Whistleblowers may send their communications through the Capgemini Group SpeakUp, if they wish to do so **anonymously**, the internal reporting channels being as follows:

- Communication through the SpeakUp software tool: https://app.convercent.com/es-es/Anonymous/IssueIntake/LandingPage/21bd0129-fee2-e611-80d9-000d3ab1117e
- Communication via the local SpeakUp phone number available on the SpeakUp portal: 900839109

Without prejudice to the foregoing, the Whistleblower may make the communication by means of a face-to-face meeting, which must be held within a maximum period of seven (7) days, following a written request for the same.

In the event that a communication is received by any means other than the SpeakUpthe information must be immediately forwarded to the Responsible of the System, so that it can be processed in accordance with this Procedure. Likewise, the recipient of the communication must keep it confidential.

Likewise, the persons to whom the Policy applies **may report to the Independent Informant Protection Authority or to the competent regional authorities** or bodies and, where appropriate, to the institutions, bodies and agencies of the European Union, the commission of any actions or omissions that may involve a breach or irregularity included in the scope of application of this Procedure, either directly or following communication through Capgemini's internal channels.

5. RESPONSIBLE OF THE SYSTEM

The Board of Directors of Capgemini shall appoint, remove or dismiss the person holding the position of Responsible of the System.

The Independent Informant Protection Authority shall be notified within ten (10) working days of the appointment or removal of the individually designated natural person, specifying, in the case of removal, the reasons for such removal.

The person in charge will carry out his/her functions independently and autonomously from any Capgemini body and may not receive instructions of any kind in the exercise of his/her functions and must have the personal and material means necessary to carry them out.

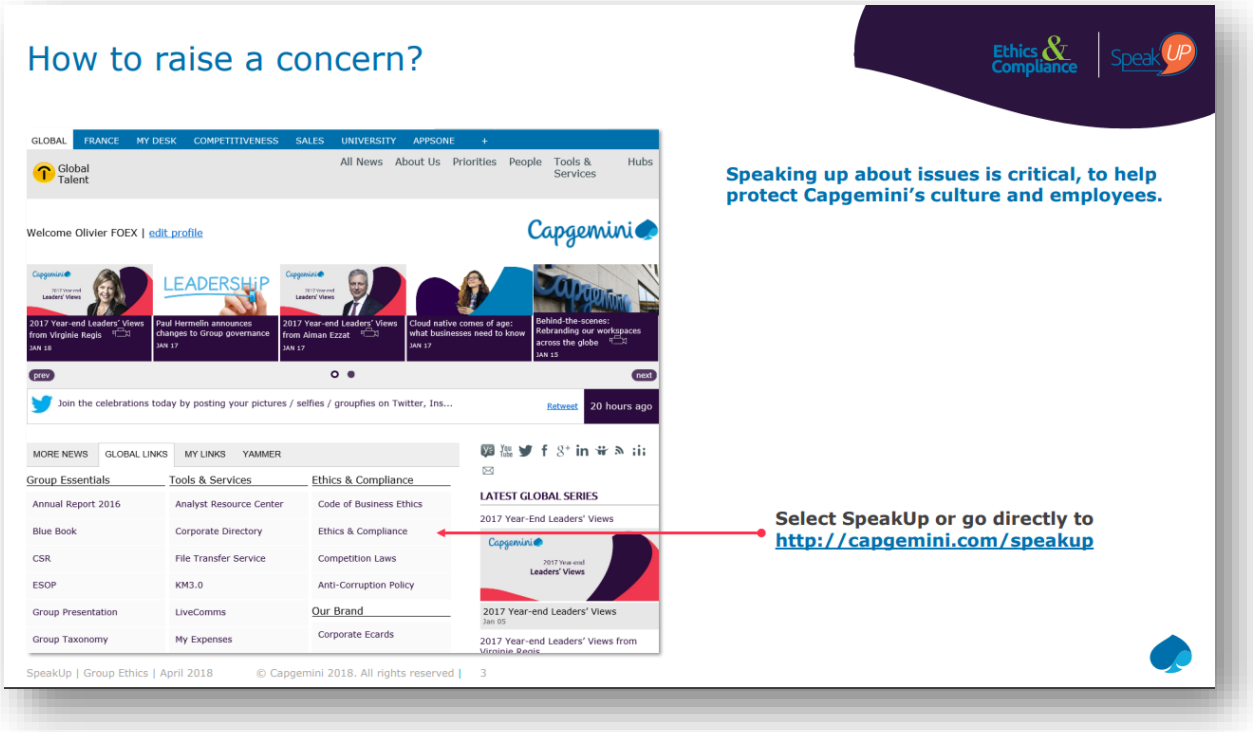
The Responsible of the System will be in charge of the management of the System and the processing of investigation files. These functions include:

- Promote and continuously supervise the implementation and efficiency of the Policy.
- Grant access to the Policy, the Procedure and the SpeakUp tool to all members of Capgemini and interested third parties.
- Implement the procedures to manage communications received through the SpeakUp.
- To know, instruct and issue the reports corresponding to the investigations arising from the communications received through Speak Up.
- Report to the Board of Directors of Capgemini on the most relevant results of the SpeakUp activity as part of its reporting duties.
- Collaborate with and represent the Company in the event of a request from the judicial authorities, the Public Prosecutor's Office, the State Security Forces and Corps, the Independent Informant Protection Authority or any other authorities with jurisdiction in the matter.

5. SUBMISSION OF COMMUNICATIONS AND FOLLOW UP BY THE WHISTLEBLOWER

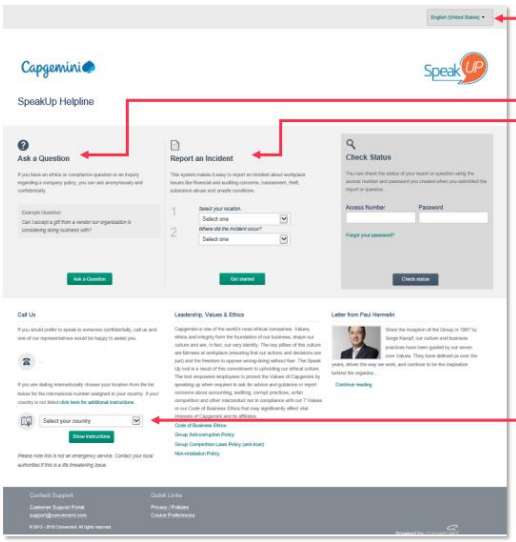
5.1 SUBMISSION OF COMMUNICATIONS

Internally, Capgemini members will be able to raise their communications through SpeakUp, which can be accessed on the Company's internal network:



In turn, third parties related to the Company can communicate their communications through the SpeakUp portal accessible on the Capgemini website:

SpeakUp helpline (web and phone)



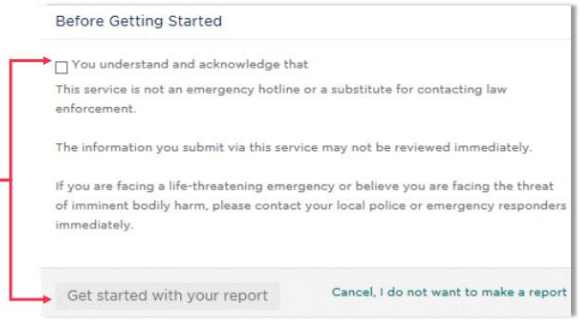
Select your language.

Web: select Ask a question
or Report an incident, and select the location.

Phone: select your country to get the toll-free number.

Accept the Data Protection and Privacy Notice

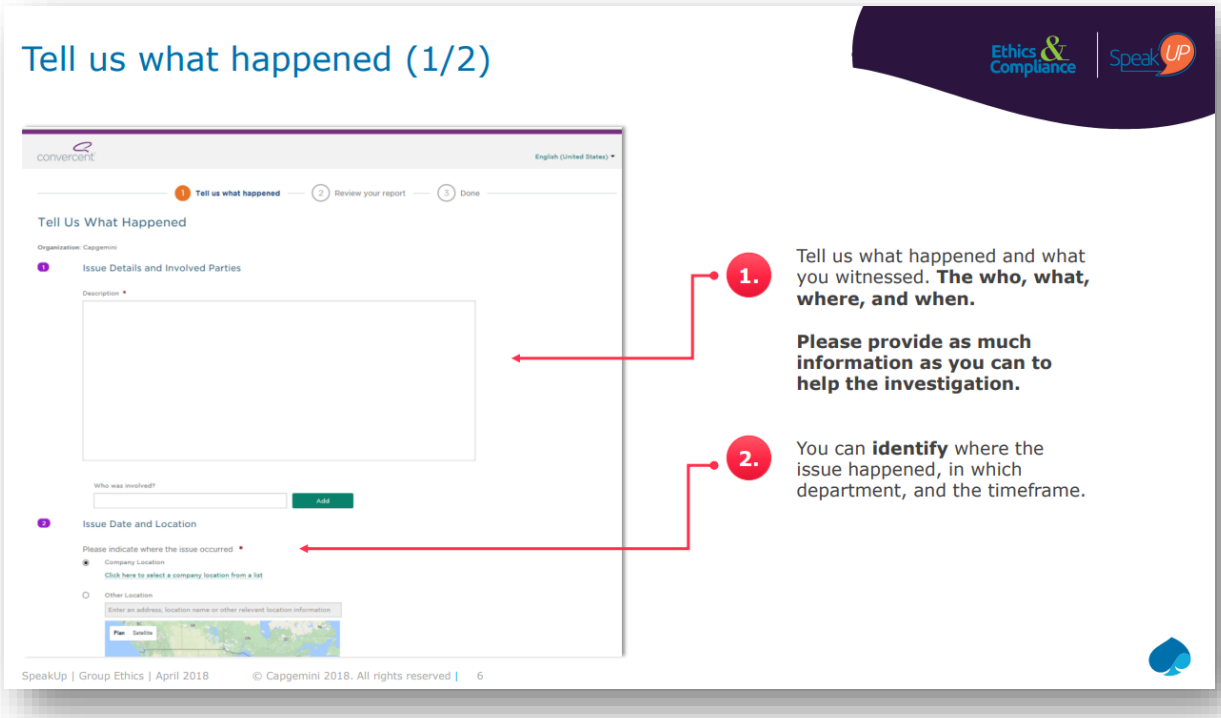
If you agree to the Data Protection and Privacy Notice, check the box and click on Get started.

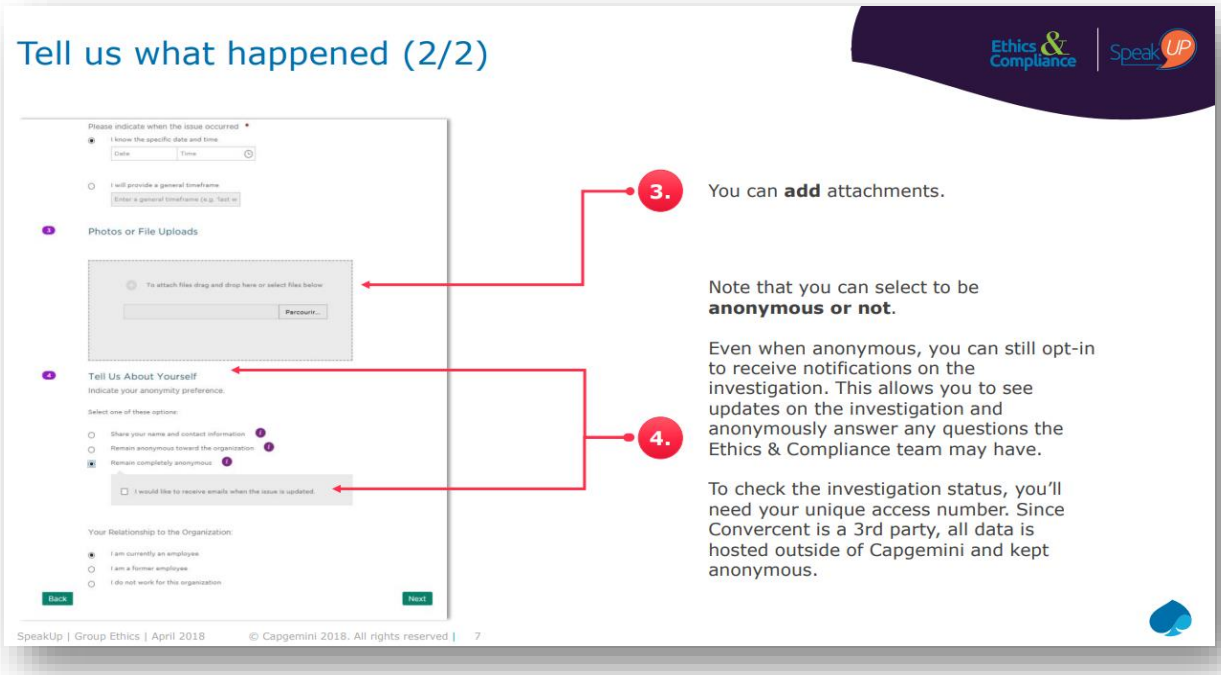


The Notice can be accessed here **http://www.capgemini.com/resources/speakup-data-protection-and-privacy-notice**

The same Notice has to be agreed to when giving a call.

If you do not consent to the processing of your personal data as described in the Notice, Capgemini will be unable to accept any information through this system. In this case, you may use one of the other internal reporting channels to report the suspected misconduct, such as reporting to your manager or to a representative of the HR, Ethics, or Legal Departments.





Verbal communications made by telephone or through a face-to-face meeting must be documented by a recording of the same in a secure, durable and accessible format or through an accurate and complete transcript of the conversation. This is without prejudice to his or her rights under data protection law, and the Whistleblower shall be given the opportunity to verify, rectify and agree to the transcript of the conversation by signing it.

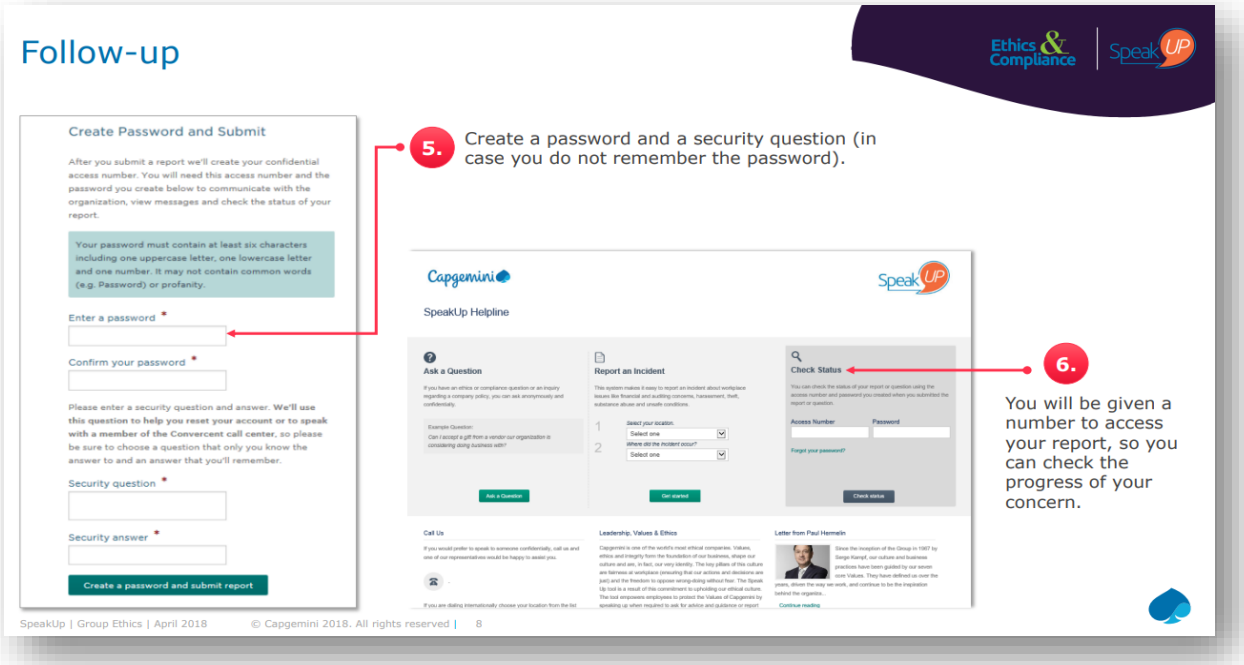
In the case of face-to-face meetings, in addition, minutes will be drawn up and signed by the attendees, to which either the aforementioned transcript or recording will be attached.

Once the communication has been raised through SpeakUp, an acknowledgement of receipt will be sent to the Whistleblower automatically and in any case within a period of no more than seven (7) calendar days.

5.2 COMMUNICATIONS' FOLLOW UP

When a submission is made, the SpeakUp tool provides the Whistleblower with login credentials (a unique reference number that only the Whistleblower will know) so that the Whistleblower can (i) track the progress of the communication and (ii) answer any questions received by the investigation team.

Even if the Whistleblower chooses to report his/her communication anonymously through the SpeakUp -using the option set up for this purpose in the tool- the Whistleblower may choose to receive notifications about his or her communication through said tool without his or her identity being known.



6. PRELIMINARY ANALYSIS AND INVESTIGATION PROCESS

Capgemini Group Ethic's Office shall engage a preliminary evaluation of the communication in order to determine the corresponding procedure and will then assign it to the Responsible of the System for its management and, if it was the case, its investigation. All along this process, Capgemini shall:

- Make sure the Person affected is informed, whenever is most convenient in order to ensure the successful completion of the investigation, of the actions or omissions attributed to him or her. Likewise, he or she will have the right to be heard at any time.

  Also, respect for the principles of confidentiality, presumption of innocence and the right to honour shall be guaranteed all along the process both with respect to the Person affected and also the rest of the parties involved in the investigation.

- If deemed necessary, the Whistleblower may be asked for additional information about the submitted communication and, if deemed appropriate, further communication with the Whistleblower may be maintained.

  Although the Responsible of the System or assigned investigation team may communicate with the Whistleblower through the use of the 'Message' function of the SpeakUp tool to request additional information about the communication, the Whistleblower cannot be identified as long as the communication has been anonymously submitted through the tool.

  The Whistleblower will also be notified when the communication has been closed under SpeakUp but, for confidentiality reasons, details of the outcome of the investigation will not be provided to the him or her.

- The Person affected will have access to the file according to the applicable Law, guaranteeing the identity, confidentiality of the reported facts and other data of the investigation.

- In any event, the maximum period for responding to the investigation proceedings shall not exceed three (3) months from receipt of the communication or, if no acknowledgement of receipt was sent to the Whistleblower, three (3) months from the expiry of the seven (7) day period following the communication, except in cases of particular complexity requiring an extension of the period, in which case the period may be extended by up to a maximum of three (3) additional months.

- Capgemini may seek the advice of external experts to advise and assist it during the investigation process. Such external experts shall be subject to the same principles and obligations as provided for in this Procedure with respect to confidentiality and data protection and shall enter into appropriate agreements to that effect.

- When the facts may be indicative of a criminal offence, the Responsible of the System shall immediately forward the information to the Public Prosecutor's Office. In the event that the facts affect the financial interests of the European Union, it shall be forwarded to the European Public Prosecutor's Office.

7. SCOPE OF PROTECTION

7.1 PERSONS SUBJECT TO PROTECTION

Capgemini offers through its System protection to both the Whistleblower in good faith against any damage which it may suffer as a result of reporting possible infringements of which it has knowledge and all Related third parties. In the same way, Capgemini offers protections to those persons who have made a public disclosure about an offence falling within the scope of the System.

Also, protection shall be extended in the same terms to all Persons affected by the communication.

7.2 PROTECTION CONDITIONS

In the event that the Whistleblower submits a report through Capgemini's System or makes a public disclosure, the protection afforded by the Company is conditioned on the submission or disclosure being made in good faith in accordance with the Policy and this Procedure. Good faith is presumed to exist when there are reasonable grounds to believe that the information is true at the time of the communication or public disclosure, even if it does not provide conclusive evidence, and that the information is within the scope of the System.

Communications made by impersonating the identity of the Whistleblower or detailing facts that are known to be uncertain or involve persons who have had no connection with such facts, even if they are true, shall be considered to be communications in bad faith.

The following are expressly excluded from the protection offered by Capgemini:

(i) Information contained in communications that have been previously rejected in the System itself or by the Independent Informant Protection Authority for any of the following reasons:
- When the facts reported lack any plausibility.
- When the facts reported do not constitute an infringement of the legal system included in the scope of application of the System.
- When the communication is manifestly unfounded or there are reasonable grounds to believe that it was obtained through the commission of an offence.
- Where the communication does not contain significant new information on infringements compared to a previous communication in respect of which the relevant proceedings have been concluded unless there are new factual or legal circumstances that justify a different follow-up.

(ii) Information relating to claims of interpersonal conflicts or affecting only the Whistleblower and the persons to whom the reported communication or disclosure relates.

(iii) Information that is already fully available to the public or that constitutes mere hearsay.

(iv) Information that relates to actions or omissions not covered in paragraph 3.2 above.

In case the Whistleblower makes a public disclosure, protection offered by the Company will be subject also to the legally stablished conditions for protection.

8. RECORD KEEPING AND PERSONAL DATA PROTECTION

The Company will keep record of all documents that may serve as probatory material of the investigation process that was carried out because of the submission of a communication for as long as there is a continuing risk of a criminal offence or a legal obligation to retain such documents. In no case personal data shall be kept for more than ten (10) years.

In turn, the Responsible of the System shall keep a register of the information received and of the internal investigations to which they give rise, guaranteeing, in all cases, the requirements of confidentiality.

In any case, the processing of personal data that takes place within the scope of application of this Procedure shall be carried out in accordance with the provisions of the Privacy Notice included in the Policy.

9. TRAINING

The Board of Director, the top management, the Responsible of the System, as well as any other person who has a role, responsibility or authority within the System, or who are likely due to their position to receive reports of irregularities, such as legal or trade union representatives, must be trained on how to operate the Policy and this Procedure.

This training shall include, among other aspects, the guarantee of confidentiality that must prevail, the warning about the classification as a very serious breach of confidentiality, as well as the establishment of the obligation of the recipient to immediately forward the information received to the Responsible of the System.

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com