

WI-0772 (Rev. 1) Whistleblower

1. Definitions

Capitalized terms and abbreviations used in this Local Policy shall have the meaning set out below or, if not explained in this Local Policy, can be found in **SOP-0178 Abbreviations and definitions**.

- Act 2/2023: Spanish Act 2/2023, of February 20, on the protection of persons who report legal breaches and fight against corruption that implements the Directive in Spain.
- CMS Spain: Canon Medical Systems, S.A.
- Directive: Directive (EU) 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.
- Reports: Complaints, disclosures, notices and/or any information furnished by an Informant related to a Wrongdoing.
- Employees: Any person who has an employment relationship with CMS Spain, either through an indefinite term employment agreement or any other type of agreement that implies a subordination relationship as well as all shareholders, and members of the administrative, management or supervisory bodies of CMS Spain (e.g. members of the Board of Directors), including non-executive members.
- External Reporting Channels: The reporting channels incorporated by the EU authorities or the Spanish authorities, as mentioned in **Attachment 2**.
- Informant: Employee or Third Party who submits a Report in relation to a Wrongdoing as described in this Local Policy.
- Local Channel Manager: Member of the Local System Manager designated by the Local System Manager to manage the Local Reporting System and to process investigation files.
- Local Channel Substitute Manager: The other member of the Local System Manager designated by the Local System Manager to substitute the Local Channel Manager in the management of the Local Reporting System when the Local Channel Manager is sick, on leave, on vacation, or for any other reason, he/she cannot temporarily take charge of the Local Reporting System.
- Local Reporting System: Internal reporting system made available for Employees and Third Parties by CMS Spain on a local basis.
- Local System Manager: Body in charge of the management of the Local Reporting System. The Local System Manager is composed by the two permanent members of the Compliance Committee of CMS Spain.
- Privacy and Data Protection Regulations: The provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), and the local regulations applicable to CMS Spain in force from time to time.
- Public Disclosure: Making information on Wrongdoings available to the public.
- Wrongdoings: As specified in section Input of this Local Policy.
- Retaliation: Any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the people who suffer them at a particular disadvantage with respect to others in the labor or professional context, solely because of their condition of Informant, or for having made a public disclosure (such as, for example, the suspension of the employment contract, the dismissal or termination of the employment or statutory

relationship, damages, including those of a reputational nature, inclusion in blacklists, etc.).

- Third Party: includes self-employed individuals, as well as any individual working for subcontractors (e.g. maintenance third party companies), suppliers (e.g. services or goods providers) or intermediaries (e.g. distributors and vendors), ex-employees of CMS Spain and candidates during the recruiting processes or other pre-contractual negotiations, where the information was obtained in the course of that application, and volunteers and paid or unpaid trainees.

2. Purpose

It is increasingly important that companies not only assume obligations of ethical behavior but also have a system whereby their own employees and other third parties with whom they work can report when behavior contrary to that ethical commitment has occurred. With this purpose, the European Union approved the Directive which, together with the obligation to have a whistleblowing channel, also establishes the rights that must be recognized for individuals who report during the entire process of managing and investigating said reports.

In line with this obligation to have speak up tools, the CMS Group has approved a Common Policy to ensure that all employees of CMS Group can expose serious concerns under the protections provided by the Directive and its national transposed laws. As per such Common Policy, in jurisdictions where local laws or regulations set stricter rules than those set out in such Common Policy, the stricter rules must prevail.

Spain has approved Law 2/2023 that implements the Directive in a more strict way and this makes it necessary to approve this Local Policy that replaces for CMS Spain the Common Policy of CMS Group. Therefore, Employees and Third Parties of CMS Spain must submit any Report related to CMS Spain through the Local Reporting System locally implemented by CMS Spain and regulated under this Local Policy.

3. Scope

This Local Policy applies to Employees and Third Parties of CMS Spain.

CMS Spain encourages their Employees and Third Parties to promptly report suspected Wrongdoings which may affect CMS Spain, and provides a safe mechanism to report them with the aim to strengthen its compliance and information culture

4. Input

All the below Wrongdoings must be reported through the Local Reporting System:

- Any act or omission that may constitute a violation of the European Union law¹.
- Any act or omission that may constitute a criminal offence.
- Any act or omission that may constitute a serious or very serious administrative infringement.

The Internal Reporting System is not intended to be used for reporting other breaches of **POL-0005 Canon - Code of Conduct (COC) and/or Canon - Standards of Conduct (SOC)** or internal regulations. For reporting such breaches,

¹ Among others, (A) breaches falling within the scope of the Union acts that concern the following areas: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and security of network and information systems; (B) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures; (C) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

Employees and Third Parties may contact the HQ Director Regulatory Affairs & Quality Assurance (compliance.EU@eu.medical.canon) by following the procedure included in the Common Policy.

5. Local Reporting System Safeguards

5.1. Non-Retaliation

CMS Spain will protect Informants against any Retaliation for reporting or disclosing a Wrongdoing in good faith, even if the Report turn out to be unfounded. Lack of good faith exists when the Informant knows or has reasonable reasons to believe that the disclosure is not true.

This protection also extends to: (i) the legal representatives of the employees in the exercise of their functions of advice and support to the Informant; (ii) any natural person who, within the company in which the Informant works, has assisted the Informant to report or disclose the Wrongdoing; (iii) any individuals who are connected with the Informant and who could suffer Retaliation, such as colleagues or relatives of the Informant; and (iv) legal entities that the Informant owns, works for, or is otherwise connected with in a work-related context or in which the Informant has a significant shareholding (v) any Employee who participate or collaborate in the investigation process.

CMS Spain will take disciplinary action up to and including dismissal (in accordance with local labor laws) against anyone who threatens or engages in Retaliation or harassment of any Informant or person who is considering reporting a Wrongdoing.

Malicious or dishonest Reports by an Informant shall be subject to disciplinary actions under CMS Group policies or applicable local regulation. In addition, under Act 2/2023 it is a very serious offence to lodge a Report knowing it to be false.

5.2. Confidentiality and Privacy

Any Report received will be treated with appropriate confidentiality and complying with current Privacy and Data Protection Regulations.

if a Report is sent through non-established reporting channels or to members of the personnel not responsible for its processing, such Report will be treated as confidential and the relevant recipient will immediately forward it to the Local Channel Manager and delete it. The relevant recipient will be obliged to keep strict confidentiality about the Report and its content. Failure to comply with this obligation may lead to disciplinary actions.

When a good faith Report is made, even if the facts subsequently prove to be incorrect or do not give rise to any action, the identity of the Informant, the information contained in the Report and the identity of all persons referred to in the Report, shall not be communicated nor disclosed, except if needed to comply with a legal obligation, to anyone other than those people in charge of the reception and process of the Reports or the investigation or those supporting in the investigation on a need to know basis. These persons shall be subject to a specific duty of confidentiality.

The Informant's identity may only be communicated to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, sanctioning or disciplinary investigation. This information shall be communicated to the Informant before disclosing his/her identity, unless such information could jeopardize the investigation or the judicial proceedings.

5.3. Anonymity

The Local Reporting System allow for the submission and subsequent processing of anonymous Reports.

As a general rule, Informant are strongly encouraged to disclose his/her identity rather than proceed with an anonymous Reports. It is more difficult to follow up on a Report and to conduct a thorough and complete investigation if it is impossible or difficult to contact the source for further information.

5.4. Rights of the persons concerned

Reports will be managed with respect for the presumption of innocence and the honor of the persons concerned. Additionally, the person concerned should be informed of the acts or omissions attributed to him or her under the relevant Report, and be heard at any time. Such communication shall take place at such time and in such manner as is deemed appropriate to ensure the proper conduct of the investigation.

6. **Procedure to manage the Reports submitted through the Local Reporting System**

6.1. Local System Manager, the Local Channel Manager and the Local Channel Substitute Manager

In accordance with Act 2/2023, Employees and Third Parties may report Wrongdoings through the Local Reporting System managed by the Local System Manager.

CMS Spain has appointed the two permanent members of the Compliance Committee as the Local System Manager. Currently, the two permanent members of the Compliance Committee are the following:

- The Tech & Operation Manager of CMS Spain: Miguel Ángel González Cibia
- The CFO of CMS Spain: Víctor Mateo López

The Local System Manager has appointed the **Tech & Operation Manager as the Local Channel Manager** and the **CFO as the Local Channel Substitute Manager**, who will substitute the Local Channel Manager in case he is absent due to vacation, sick leave etc.

The Local Reporting System is managed directly from Spain.

6.2. Means for the Submission of Reports through the Local Reporting System

In order for the Reports to be effectively received and duly administered through the Local Reporting System, the Reports shall be submitted by the Informant by sending an email to compliance.IB@eu.medical.canon which is available 24 hours a day, 365 days of the year.

In case the person concerned is the Local Channel Manager, the Report can be filed through the Local Channel Substitute Manager at his direct email address: victor.mateo@eu.medical.canon. Likewise, if the Report refers to the Local Channel Substitute Manager, the Report can be filed through the Local Channel Manager at his direct email address: miguelangel.gonzalez@eu.medical.canon.

At the Informant's request, the Report may also be submitted by means of a face-to-face meeting within a maximum of 7 calendar days. If the Report is filed during a face-to-face meeting, prior agreement with the Informant: (i) the conversation shall be recorded on a durable and retrievable medium or (ii) an accurate written record of the conversation shall be made. The Informant shall have the opportunity to verify, rectify and approve the transcript of the conversation or the minutes (as applicable) by signing them (electronically, if applicable).

When making the Report, the Informant may provide a physical address, an email address or a safe place to receive notifications.

Reports may be made anonymously, although this may limit CMS Spain's ability to process and investigate them.

6.3. Reception of the Reports

All Reports made through the Local Reporting System for Spain will be received by the Local Channel Manager.

If a Report is sent locally to an Employee other than the Local Channel Manager, the recipient shall immediately transfer the Report to the Local Channel Manager and the recipient will keep strict confidentiality of the Report.

When a Report is received, the Local Channel Manager will provide written acknowledgment of receipt of the Report to the Informant within 7 calendar days of the receipt of the Report.

If the Report does not meet the requirements set out under this policy and therefore is not admissible, the Informant will be informed of the reasons underlying this inadmissibility.

The persons referred to in the Report will be informed of the Report at such time and in such manner as is deemed appropriate to ensure the proper conduct of the investigation .

6.4. Investigation of the Reports

The Local Channel Manager will make a preliminary assessment of the Report and decide on the next course of action.

The way in which a Report is handled will depend on its nature and severity but CMS Spain will always seek to ensure that it is managed according to the Safeguards included in this policy and by the most appropriate individual or team.

The Local Channel Manager will carry out the investigation of the Report, with such internal team as he/she deems necessary, or assisted by external counsels, if he/she considers that this is the most appropriate way to investigate the Report and always in compliance with local legal requirements.

The term to give response to the investigation will not exceed 3 months from the acknowledgement of receipt of the Report or, if no acknowledgment was sent, 3 months from the expiration of a 7 calendar day period after the Report was made, except in cases of particular complexity requiring an extension of the term, in which case the term may be extended for a maximum of 3 additional months.

Every Employee who, without being involved in the reported events, has information regarding the subject matter of a Report, shall collaborate during the corresponding investigation per request of the investigation team, duly and timely furnishing the information he/she has knowledge of. Failure to collaborate may result in disciplinary action.

During the investigations, and once the same are concluded, the confidentiality of the information contained in the Reports shall be protected according to the applicable laws.

6.5. Resolution

Once the investigation is concluded, if the reported Wrongdoing is shown to be justified, then the relevant actions will be adopted according to the CMS Group' policies and procedures and applicable local law.

The Local Channel Manager shall carefully assess the need to bring reported Wrongdoings to the attention of the relevant Public Prosecutor's Office or to the European Public Prosecutor's Office on a case-by-case basis.

6.6. Register-book

The Local Channel Manager shall keep a Register of all Reports received through the Local Reporting System and of the internal investigations to which they give rise, guaranteeing, in all cases, their confidentiality.

This Book-Register shall not be public and only at the reasoned request of the competent judicial authority, by means of an order, and within the framework of a judicial proceeding and under the protection of the latter, may access all or part of its contents.

6.7. Data Protection

The information related to data protection is included in **Attachment 1** hereto.

6.8. Other Reporting Channels

6.8.1. External Reporting Channels

While CMS Spain expects that Employees and Third Parties will feel comfortable reporting their concerns through the Local Reporting System, they may also decide to report the Wrongdoings externally to competent external authorities as those mentioned, as examples, in **Attachment 2**.

6.8.2. Public Disclosure

A Public Disclosure of a Wrongdoing may only be made by Employees or Third Parties in any of the following situations:

- If they have first submitted the Report through the Local Reporting System and any of the External Reporting Channels, or directly through any of the External Reporting Channels, without appropriate action having been taken on the matter within the prescribed time limits.
- If they have reasonable grounds to believe that either the Wrongdoing may constitute an imminent or manifest danger to the public interest, in particular where there is an emergency situation, or there is a risk of irreversible damage, including a danger to the physical integrity of a person; or, in case of communication through an External Reporting Channel, there is a risk of Retaliation or there is little likelihood of effective handling of the Report due to the particular circumstances of the case, such as concealment or destruction of evidence, collusion of an authority with the perpetrator of the Wrongdoing, or that the authority is involved in the Wrongdoing.

Attachment 1. Data Protection

Canon Medical Systems S.A. is responsible for the processing of personal data managed through the Local Reporting System. The processing of the data by other persons, or even their communication to third parties, shall be lawful when it is necessary for the processing of the sanctioning or criminal proceedings that may be applicable, as the case may be.

The sole purposes of this data processing are (i) to assess the Reports received through the Local Reporting System, (ii) to carry out the necessary internal investigations, and (iii) to record the operation and effectiveness of the Local Reporting System.

The lawful basis for the processing of data received as a result of a Report or in the framework of a subsequent internal investigation is Article 6(1)(c) of the General Data Protection Regulation (EU) 2016/679. In other words, the processing is necessary for compliance with the legal obligation to have an internal whistleblowing channel.

Access to personal data and any other information contained in the Local Reporting System shall be limited, within the scope of its powers and functions, exclusively to:

- The Local Channel Manager, the Local Channel Substitute Manager, if applicable, and whoever manages it directly.
- The professionals (internal and external) involved in the internal investigation and, where appropriate, the public authorities to whom the result of the possible internal investigation is transferred (investigating judge, Public Prosecutor's Office or relevant administrative authority) within the framework of a criminal, disciplinary or sanctioning investigation.
- Canon Medical System S.A.'s Human Resources Manager, if other than the Local Channel Manager, only when disciplinary measures may be taken against an Employee or if the Human Resources Manager is part of the investigation team.
- The person in charge of Canon Medical System S.A.'s legal services, in the cases provided for in the previous sections, and if the adoption of legal measures in relation to the facts described in the Report is appropriate.
- The persons in charge of the processing that may be appointed.
- The Data Protection Officer.

The processing of personal data managed through the Local Reporting System includes, in any case, the following obligations:

- No personal data shall be collected or processed if they are not manifestly relevant to the processing of a specific Report or, if collected by accident, shall be deleted without undue delay.
- Any personal data contained in Reports which relate to conduct that does not fall within the Material Scope of this policy will be deleted. If the information received contains personal data falling within the special categories of data, it shall be deleted immediately, without undue delay.
- Any Report that is proven to be untrue shall be immediately deleted, unless such untruthfulness may constitute a criminal offence, in which case the Report shall be kept for the time necessary for the duration of the legal proceedings.
- All Reports which have not been followed up and which are intended to be kept shall be anonymized, without identifying any individual who is a party to the Report or file;
- Individuals within the personal scope of application of this policy shall be informed of the processing of personal data that takes place within the framework of the Local Reporting System. In addition, when personal data are obtained directly from the individuals, they shall be provided with the legally required information on the processing of such data and shall be informed that their identity shall be kept confidential in all cases.

- If the Report is made verbally and is to be recorded, the Informant shall be warned of such recording and shall be informed of the processing of his or her data in accordance with the provisions of the Privacy and Data Protection Regulations.
- The person to whom the facts related shall in no case be informed of the identity of the Informant or of the person who has made the public disclosure, even if he/she exercises his/her right of access to his/her personal data.
- The data processed may be kept in the Local Reporting System only for the time necessary to decide whether or not to initiate an investigation into the facts reported. In any case, they shall be deleted after three (3) months have elapsed from the receipt of the Report without any investigation having been initiated, unless the purpose of the storage is to leave evidence of the operation of the Local Reporting System.
- Once the three (3) month period has elapsed, the data may continue to be processed outside the Local Reporting System, for the development of the investigation of the reported facts, or when necessary for the execution of civil, criminal, labor, administrative, disciplinary or any other type of action. Once the investigation has been completed, the data shall be kept in the Register-book for a maximum period of ten (10) years, except when they should be retained for a long time in order to safeguard Canon Medical Systems, S.A. right of defense.
- Personal data subjects may exercise, in accordance with the Data Protection Regulations, their rights of access, rectification, deletion, opposition, limitation of processing and portability of their data, where applicable according to the applicable regulations, by sending an e-mail to the address data.protection@eu.medical.canon. In addition, they also have the possibility of lodging a complaint with the relevant supervisory authority. In the case of Spain, this is the Spanish Data Protection Agency (www.aepd.es).
- However, the exercise of such rights does not apply when this exercise is planned in relation to a Report related to the prevention of money laundering and terrorist financing, in which case the provisions of article 32 of Law 10/2010, of 28 April, shall apply. In addition, in the event that the person to whom the facts described in the Report refer exercises the right to object, it shall be presumed that there are compelling legitimate reasons that legitimize the processing of their personal data, unless there is evidence to the contrary.

Attachment 2. External Authorities for External Reporting Channels Purposes

European Authorities

- European Anti-Fraud Office (OLAF)
- European Public Prosecutor (EPPO)
- European Maritime Safety Agency (EMSA)
- European Aviation Safety Agency (EASA)
- European Security and Markets Authority (ESMA)
- European Medicines Agency (EMA)

Local Authorities

- The Independent Authority of Protection of the Reporting Persons²
- National Department of Anti-fraud Coordination
- Anti-fraud Office of Catalonia
- Anti-fraud Office of Andalucía
- Anti-fraud Office of the Autonomous Community of Valencia
- Prevention and Fight against Corruption on the Balear Islands
- Good Practice and Anticorruption Office of the Foral Community of Navarra

² At the time of approval of this local policy, this authority has not been appointed.