Abstract - Group Policy - “Management of Whistleblowing Reports”

cdp

Contents

1. Glossary

- **ANAC:** Italian National Anti-Corruption Authority, an authority with the power to handle external whistleblowing reports and to apply sanctions.
- **Law:** Legislative Decree No. 24 of 10 March 2023 implementing 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 EU law and laying down provisions regarding the protection of persons who report violations of national regulatory provisions, the so-called "Whistleblowing Decree".
- **Whistleblowing channels:** channels through which Reports can be made (internal, external, through public disclosure, complaints to the judicial or accounting authorities).
- ***"eWhistle"* software:** IT platform implemented by the CDP Group and used by both Personnel and Third parties to transmit the Reports.
- **Public Disclosure:** making information about violations publicly available by printed or electronic means or otherwise by means of dissemination capable of reaching a large number of people.
- **Companies of the Cassa Depositi e Prestiti Group:** the Group Companies subject to management and coordination by CDP pursuant to Articles 2497 et seq. of the Italian Civil Code falling within the scope of application of this document (also "Group Companies" defined above).
- **External Supplier for the storage of the Whistleblower's identification details**: an external party that provides the service of storage of the identification details of the Whistleblower who has made Reports using the "*eWhistle*" software.
- **Reporting Manager**[1] [2]:
  - CDP: Internal Audit Department;
  - Group Companies: Internal Audit Function of each Group Company.
- **Facilitators:** those who assist a whistleblower in the reporting process operating in the same work environment, whose assistance must be kept confidential.
- **Control functions:** Internal Audit, Compliance and Anti-Money Laundering/Risk Management.
- **Corporate Bodies:** Board of Directors, Chairman of the Board of Directors, Chief Executive Officer, General Manager (where present) and Board of Statutory Auditors.
- **231 Model**: Organisation, Management and Control Model pursuant to Legislative Decree 231/01.
- **Supervisory Body** or **SB:** the control body, in the form of a board, responsible for supervising the functioning of and compliance with the 231 Model adopted by CDP and each of the Group Companies, as well as its updating.
- **Personnel**: employees that have an employment relationship with CDP or the Group companies, as well as former employees, workers not yet employed or still on probation, persons with

[1] The Reporting Manager is the data controller for the processing of the personal data relating to the receipt and management of reports in accordance with the express provisions of Article 13 of Legislative Decree no. 24/2023

[2] It should be noted that, in companies subject to the Bank of Italy Regulation of 5 December 2019 as amended by the order dated 23 December 2022, the Manager also represents the *Head of Internal Reporting Systems for Violations*.

administrative, management, control, supervisory or representative functions, volunteers and paid and unpaid trainees[3].

- **Retaliation:** any conduct, act or omission, even if only attempted or threatened, committed as a result of the report or complaint to the judicial or accounting authorities or public disclosure and which causes or may cause the whistleblower or the person making the complaint, directly or indirectly, unjustified damage.
- **European General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679:** this regulation entered into force on 25 May 2018 and imposes a series of obligations on companies with regard to the processing of personal data by any entity operating in Europe (e.g. appointment of the Data Protection Officer, implementation of the register of processing operations, etc.).
- **Whistleblowing Report:** written or verbal communication by the Whistleblower relating to information on the violations that Whistleblower has become aware of within the work context ("Report" in the rest of the Policy) The aforementioned Reports are divided into:
    - "Substantiated reports", whose narration of the facts is sufficiently detailed to enable the competent company functions to identify useful or decisive information for the purposes of verifying the validity of the Report. These Reports can be made in:
        - good faith, ("Good Faith Reports") when made by the Whistleblower in the reasonable belief, based on specific facts, that the unlawful conduct has occurred;
        - bad faith ("Bad Faith Report") in cases where the Report is unfounded and made for the sole purpose of causing unfair harm to the person and/or company reported;
    - "Generic report": this is a report that is so generic in content that it does not enable anything to be ascertained from it;
    - "Anonymous report", i.e. Reports in which the details of the Whistleblower are not known or unambiguously identifiable;
    - "Reports on significant events" i.e. Reports on anomalies and/or fraud:
        - for which a significant quantitative and qualitative impact on the financial statements can be estimated for CDP and for the Group Companies;
        - which concern the members of the Corporate Bodies of CDP and the Group Companies, direct reports of the Chairman of the Board of Directors, the Chief Executive Officer and General Manager of CDP and of the Group Companies, where present.

  In implementation of the applicable provisions of law, reports may be submitted through: i) the internal channel established by CDP and the Group companies; ii) the external channel (under certain conditions expressly set out by the law and described in Paragraph 7.1), by addressing the report to the ANAC; iii) public disclosure (under certain conditions expressly set out by the law and described in Paragraph 7.2); iv) by reporting a complaint to the judicial or accounting authorities.
- **Work environment:** current or past work or professional activities through which, regardless of the nature of those activities, a person acquires information about violations and in the context

[3] As specifically identified in Article 3 of Legislative Decree No. 24/2023.

of which he or she could risk retaliation in the event of a report or public disclosure or a report to the judicial or accounting authorities.

- **Information on violations:** information, including reasonable suspicions concerning violations committed or which, on the basis of concrete elements, could be committed in the organisation with which the whistleblower or the person making the complaint to the judicial or accounting authorities has a legal relationship, as well as elements concerning conduct aimed at concealing such violations.
- **Violations:** conduct, acts or omissions that result in harm to the public interest or the integrity of the public administration or private entity and which consist of:
  1) administrative, accounting, civil or criminal offences that do not fall under points 3), 4), 5), and 6);
  2) unlawful conduct, relevant pursuant to Legislative Decree No. 231 of 8 June 2001, or violations of the organisation and management models provided for therein, which do not fall under points 3, 4, 5, and 6;
  3) offences falling within the scope of application of the European Union or national acts indicated in the annex to Legislative Decree No. 24 of 10 March 2023 or of the national acts that implement the European Union acts relating to the following areas: public procurement contracts; services, products and financial markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and personal data and security of networks and information systems;
  4) acts or omissions that are detrimental to the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU) specified in the relevant secondary legislation of the European Union;
  5) acts or omissions concerning the internal market (goods, persons, services and capital) as referred to in Article 26, paragraph 2 of the TFEU, including violations of EU competition and state aid rules, as well as violations concerning the internal market related to acts in violation of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the objective or purpose of the applicable corporate tax law;
  6) acts or conduct that frustrate the purposes of the provisions of the European Union in the sectors indicated under 3), 4), 5).
- **Whistleblower:** an individual belonging to the Personnel or Third Parties who carry out internal or external reporting, public disclosures or report complaints to the judicial or accounting authorities.
- **Reported party:** the subject mentioned in the internal or external report or in the public disclosure as a person to whom the violation is attributed or as a person otherwise involved in the reported or publicly disclosed violation.
- **Third parties:** external parties having a legal relationship with CDP and the Group companies (for example, self-employed workers, freelance professionals and consultants, shareholders, suppliers, consultants, collaborators etc.)[4].

[4] As specifically identified in Article 3 of Legislative Decree No. 24/2023.

- **Whistleblowing:** instrument of Anglo-Saxon origin through which the Personnel/Third parties that have an employment or other form of relationship with an organisation – either public or private – report unlawful conduct that they have become aware of within the organisation to the appropriate bodies or individuals.
- **IT Register**: a register managed by means of computerised methods guaranteeing accessibility only to the Reporting Manager and making it possible to (i) assign a unique progressive code to the Report; (ii) record the date of receipt; (iii) separate the content of the Report from the identity of the Whistleblower; (iv) keep track of the date of archiving as well as the reasons leading to the archiving.

2. Scope of application

- Parent Company: Cassa Depositi e Prestiti S.p.A. (also referred to as “CDP”).
- Group companies: Companies subject to management and coordination by CDP S.p.A. pursuant to Articles 2497 et seq. of the Italian Civil Code[5].

This Policy has been drafted for the adoption of the regulatory provisions on Whistleblowing (Legislative Decree No. 24/2023).

The Group Companies subject to management and coordination pursuant to Articles 2497 et seq. of the Italian Civil Code ensure that the operations of the unlisted second-tier subsidiaries under their management and coordination are in line with the provisions of these Group regulations, in compliance with the principle of proportionality and taking into account the decision-making autonomy of the Corporate Bodies of those companies, in particular of the Supervised Entities, as well as the specific sectoral legislation applying to the latter.

3. Introduction

3.1 Scope and content of the Report

For the purposes of this Policy, Reporting covers information, including reasonable suspicions, concerning violations committed or which, on the basis of concrete elements, could be committed in the organisation with which the whistleblower has a legal relationship, as well as elements concerning conduct aimed at concealing such violations.

Reports must contain at least the following elements - which are considered prerequisites for the admissibility of the report:

- details of the Whistleblower if he/she decides to send the Report specifying his/her identity;
- description of the facts, details or other elements enabling identification of the Reported Party;
- the circumstances of the time and place in which the events occurred, if known;

[5] See General principles on exercising management and coordination activities

- type of unlawful conduct;
- other persons with knowledge of the same facts;
- any other information that may provide useful feedback for the reconstruction and subsequent verification of the facts reported, including any documents to be attached to the Report that may provide elements of substantiation of the facts reported.

The protections provided for by this Policy do not apply, inter alia, to the following cases:

- Generic reports, or those based on mere suspicions or rumours;
- Reports made exclusively for the personal purposes of the Whistleblower that do not in any case concern aspects of interest to CDP/Group Companies;
- Reports made in bad faith or containing information that the Whistleblower knows to be false.

The following are not treated as Reports for the purposes of this document:

- deficiencies found as a result of errors not attributable to the violations, as defined in the Glossary: (i) detected and documented by the corporate functions within the first-level internal controls; and (ii) identified by the second- and third-level control functions for which improvement actions have been established to strengthen the Internal Control System and reporting to the control functions is envisaged;
- communications concerning circumstances/facts already known and the subject of pending litigation between the CDP Group and third parties and overseen by the relevant legal and/or organisational units of the company. These communications will be sent to the corporate functions responsible for receiving and managing them on the basis of the relevant regulations.

4. Management of Internal Reports

Internal Whistleblowing reports are managed through the following main phases:

1. **Receipt, investigation and verification of the Report:**
   a) receipt and preliminary analysis of the admissibility of the report sent by the Whistleblower (primarily for the purposes of its qualification as a Report pursuant to the Law);
   b) assignment of internal reference record to the report - by means of an IT Register - and timely issuance to the Whistleblower of the acknowledgement of receipt/acceptance, within 7 days of receipt;
   c) analysis of the relevance of the report pursuant to the 231 Model and, in the event of a positive assessment, involvement of the Supervisory Body by means of appropriate reporting at all stages of the management of the whistleblowing report;
   d) conduct of the inquiry/investigation and feedback to the whistleblower within 3 months;
2. **Archiving of the Report;**
3. **Reporting.**

4.1 Receipt, investigation and verification of the Report

To receive the reports, CDP and the Group Companies use the following internal channels[6]:

- IT platform
- email address
- ordinary mail: addressed to the Internal Audit Department for CDP and to the Internal Audit Function for each Group company.

Annex 1 provides specific references for the internal channels.

Reports may also be made verbally via telephone lines or voice messaging systems or, at the request of the whistleblower, through a face-to-face meeting.

These channels ensure the confidentiality of the identity of the Whistleblower, the Reported Party, the Facilitator, the person in any case mentioned in the report, as well as the content of the report and the related documentation.

In the case of Whistleblowing Reports by ordinary mail, in order to ensure confidentiality, it is necessary for the Whistleblower to specify on the envelope the "CONFIDENTIAL" nature of the letter and the wording "Whistleblowing".

Any Reports received through channels other than those mentioned above and/or not addressed to the Reporting Managers must be sent, within 7 days of receipt, by the structure that received the report to the Reporting Managers who, with the support of the competent structures, will carry out the necessary verifications, simultaneously notifying the whistleblower that it has been sent.

Within 7 days after the Report is received by the Reporting Manager, the latter shall send the Whistleblower a notice of receipt of the Report[7].

Upon receipt of a Report, the Reporting Manager carries out a preliminary analysis necessary to assess the existence of the necessary requirements required for the admissibility of the Report (see paragraph "3.2 Scope and content of the Report"), followed by the commencement of the investigation.

Where the report pertains to areas concerning the 231 Model, it shall be managed with the involvement of the Supervisory Body by means of appropriate reporting at all stages; in all other cases, the Internal Audit Department shall conduct the investigation process independently, providing the Supervisory Body with subsequent and aggregate reporting, where necessary.

As provided for in Paragraph 4.2, if the Reports concern the Supervisory Body as a whole, they are handled directly by the Internal Audit structure, excluding the Body itself.

The Reporting Manager shall:

- record the Reports received in a confidential IT register;
- assign a unique progressive code to the Reports;
- record the date of receipt;

[6] These channels were established after consulting with the trade unions referred to in Article 51 of Legislative Decree No. 81/2015

[7] Acknowledgement of receipt cannot be issued if the Whistleblower files an anonymous report or has not provided the necessary identification details.

- separate the content of the Report from the identity of the Whistleblower in order to ensure their anonymity;
- maintain dialogue with the Whistleblower and, if necessary, request supplements;
- make the content of the Report available only to the parties that manage the investigation.

The time limit for commencement of the investigation is 15 working days from receipt of the Report.

In order to follow up diligently on the Report received, the Reporting Manager ensures the performance of the appropriate and necessary verifications on the verifiable reported facts, ensuring that these are carried out on time and in compliance with the principles of confidentiality, objectivity, professional competence and diligence, with the support, where necessary, of the applicable specialist functions.

Specifically, the Reporting Manager shall:

- initiate verifications, informing (as appropriate) the corporate functions competent for the subject of the matters covered by the Report (for example, for the acquisition of documentation), and/or external consultants for specific and specialised investigation needs;
- ensure, where possible, any dialogue with the Whistleblower, through the exchange of messages, documents and supplementary information;
- complete the checks, keeping a trace of the reasons in cases of archiving of the Report; see paragraph “Archiving of Reports” of this document for more details;
- report the results of the assessments carried out in accordance with Paragraph 5.3 Reporting.

The Reporting Manager shall:

- agree, with the manager of the department involved in the verification, any action plan necessary to improve the Internal Control System, also ensuring that its implementation is monitored;
- inform, in the event of Reports relating to relevant events, the Corporate Bodies, through the respective Chairmen of the Board of Directors and the Chairmen of the Board of Statutory Auditors, if they are not involved in the events that are the subject of the Report.
- agree, with the competent company functions, on any action to be taken to protect the interests of the Company (for example, legal action, disciplinary sanctions, suspension/deletion of suppliers from the list, etc.);
- submit the results of the in-depth analyses for assessment by the Board of Directors, the Board of Statutory Auditors and the competent company functions (to the extent permitted by Law), to enable the adoption of the most appropriate disciplinary measures or other actions, in compliance with the provisions of the Law and the relevant company regulations and in accordance with the provisions set out in greater detail in Paragraph 8, “Disciplinary measures and other actions” of this document, to which reference is made.

The Reporting Manager provides feedback on the report, giving an account of any measures taken or intended to be taken, within 3 months from the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within 3 months from the expiry of the seven-day period following the submission of the report.

If the Reported Party believes that the Whistleblower has submitted the Report only for the purposes of slander and/or defamation (i.e. “Bad Faith Report”), they may file a complaint against persons not known to him/her. Where the Judicial Authority deems it necessary to take action against the Whistleblower, it may request the Company to provide the identity of the Whistleblower. CDP and the Group Companies, by accepting this request, provide the details - where these can be found - to the Judicial Authority. If the Report has been transmitted through the IT platform, CDP and the CDP Group Companies, by accepting this request, obtain information from the External Supplier for the storage of the Whistleblower’s identification details. In this case, when the whistleblower's criminal liability for offences of defamation or slander, or in any case for the same offences committed with the complaint to the judicial or accounting authorities, or their civil liability, for the same reason, in cases of wilful misconduct or gross negligence, is established, even by a first-instance judgment, the disciplinary sanction deemed appropriate shall be applied against the whistleblower.

The aforementioned Supplier may provide such data only after having received a request from the Company duly signed by its legal representative in which it:

- communicates the identity ticket (unique code generated by the system following the request for identity of a Whistleblower) of the Report;
- states the reasons why it is necessary to receive the identification details of the Whistleblower;
- certifies the satisfaction of all the requirements established by the regulations that permit access to the identification details of the Whistleblower;
- requests to receive the communication of the identification details of the Whistleblower associated with the Report.

At all stages of the investigation of the reported facts, CDP and the Group Companies ensure that the Whistleblower is protected against any retaliatory action that he/she may suffer and/or adopted as a result of the Report made. Accordingly, if the Whistleblower, after the acknowledgement of the Report, believes that he/she has been subject to retaliatory conduct, he/she may submit a new a new – non-anonymous – Report concerning the retaliation suffered, providing advance authorisation to the Reporting Manager to access his/her personal data so that the necessary measures can be adopted to restore the situation and/or to remedy the negative consequences associated with the discrimination, as well as to initiate all the measures that will be deemed necessary, possibly even disciplinary measures.

4.2 Archiving of the Report

The Reporting Manager archives the report if:

- the subject matter does not fall within the scope of the Reports addressed within this document;
- as a result of the checks carried out, no elements have emerged that would suggest that the alleged wrongdoing has actually occurred;
- description of the facts is manifestly unfounded and/or in bad faith and/or of such a generic nature that it cannot be verified;
- the communications concern circumstances/facts already known and the subject of pending litigation between the CDP/Group Companies and Third Parties, overseen by the relevant legal and/or organisational units of the company;

- the Whistleblower has failed to provide the clarifications/explanations requested and/or necessary for the conclusion of the investigation.

The Reporting Manager archives the report and updates the IT register, keeping track of the reasons leading to the archiving.

5. Other reporting channels

5.1 External reporting channel - ANAC

The Whistleblower may file an external report to the ANAC if, at the time of its submission, one of the following conditions applies:

- within the work environment, no mandatory activation of the internal reporting channel is envisaged or, even if this channel is mandatory, it is not active or, even if it has been activated, it does not comply with the provisions of the law;
- the Whistleblower has already filed an internal report and it has not been followed up;
- the Whistleblower has reasonable grounds to believe that, if he or she were to file a report through the internal channel, the report would not be effectively followed up or the report itself might lead to the risk of retaliation;
- the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious threat to the public interest

ANAC[8] has further clarified that priority is given to the use of the internal channel, and only in the event of one of the aforementioned conditions, it is possible to make an external report.

External reports may also be filed in written form via the IT platform or verbally via telephone lines or voice messaging systems, or, at the request of the whistleblower, by means of a face-to-face meeting set within a reasonable period of time.

An external report submitted to a subject other than the ANAC is transmitted to the latter within seven days from the date of receipt, with simultaneous notification of transmission to the whistleblower.

Upon receipt of the report, the ANAC notifies the whistleblower of the receipt of the external report within seven days from the date of its receipt, unless explicitly requested otherwise by the whistleblower or unless the ANAC considers that the notice would compromise the protection of the confidentiality of the whistleblower's identity. Furthermore, the Authority must[9] (i) maintain dialogue with the whistleblower and request supplements from the latter, if necessary; (ii) diligently follow up on the reports received; (iii) carry out the necessary investigation to follow up on the report, also by means of hearings and acquisition of documents; (iv) give feedback to the whistleblower within three months or, if there are justified and substantiated reasons, six months from the date of acknowledgement of receipt of the external report or, in the absence of said notice, from the expiry of the seven days from its receipt; (v) notify the Whistleblower of the final outcome, which may also

[8] https://www.anticorruzione.it/-/whistleblowing e document ANAC “La disciplina del whistleblowing: novità introdotte dal D.Lgs. n.24/2023 attuativo della Direttiva Europea n.1937/2019” – Dott.ssa Giulia Cossu.
[9] ANAC may refrain from following up on reports of minor violations and proceed to archiving them.

consist in it being archived or sent to the competent authorities or in a recommendation or in an administrative monetary sanction[10]against the person held responsible.

5.2 Public Disclosure

The Whistleblower may also resort to public disclosure if:

- they have delivered the report through the internal and/or external channel and no response was received within the time limit as provided by law;
- they have well-founded reasons to believe that the violation may constitute an imminent or obvious threat to the public interest;
- they have reasonable grounds to believe that the external report may entail a risk of retaliation or may not be followed up effectively due to the specific circumstances of the specific case (for example, there is a risk that evidence will be concealed or destroyed, or a well-founded fear that the recipient of the report may be colluding with the perpetrator of the violation or is involved in the violation).

6. Disciplinary measures and other actions

If the investigations into the Reports identify unlawful or improper conduct by the Reported Party, or by the Whistleblower in the cases described above, CDP and the Group Companies evaluate whether to adopt disciplinary and/or sanctioning measures, or legal action.

7. Retention of documentation and traceability

All the organisational units involved in the activities governed by this document shall ensure, each for their respective area of responsibility, the traceability of the data and information and retain the documentation produced, in paper and/or electronic form, in order to enable the reconstruction of the various phases of the process, while guaranteeing the confidentiality and protection of the personal data of the Whistleblower and the Reported Party.

The original documentation, in printed and/or electronic form, must be kept for no more than five years from the date of the communication of the final outcome of the reporting procedure, except in cases of legal proceedings initiated/in progress.

If a recorded telephone line or other recorded voice messaging system is used for reporting, the report, subject to the consent of the whistleblower, shall be documented by the personnel in charge by means of a recording on a device suitable for storage and listening or by means of a complete

[10] Article 21 of the Law envisages the following administrative monetary sanctions: "... a) from 10,000 to 50,000 euro when it ascertains that retaliation has been committed or when it ascertains that the report has been impeded or that an attempt has been made to impede it or that the obligation of confidentiality referred to in Article 12 has been breached; b) from 10,000 to 50,000 euro when it ascertains that no reporting channels have been established, that no procedures for the filing and handling of reports have been adopted or that the adoption of such procedures does not comply with those referred to in Articles 4 and 5, as well as when it ascertains that the reports received have not been verified or analysed; c) from 500 to 2,500 euro, in the case referred to in Article 16, paragraph 3, unless the person filing the report has been convicted, even at first instance, of the offences of defamation or slander or, in any case, of the same offences committed with the report to the judicial or accounting authorities. 2. The private sector entities referred to in Article 2, paragraph 1, letter (q), number (3), in the disciplinary system adopted pursuant to *Article 6, paragraph 2, letter (e) of Decree No. 231 of 2001*, shall provide for sanctions against those found liable for the offences referred to in paragraph 1".

transcript. In the case of a transcript, the whistleblower may verify, rectify or confirm the contents of the transcript by signing the relative report.

If an unregistered telephone line or other unregistered voice messaging system is used for reporting, the report shall be documented in writing by means of a detailed record of the conversation by the personnel in charge. The whistleblower may verify, rectify and confirm the contents of the transcript by signing the relative record.

When, at the request of the person filing the whistleblowing report, the report is made verbally during a meeting with the personnel in charge, the report, subject to the consent of the whistleblower, shall be documented by the personnel in charge by means of a recording on a device suitable for storing and listening or by means of meeting minutes. The whistleblower may verify, rectify and confirm the meeting minutes with their signature.

8. Processing of data for data protection purposes

This process protects the processing of the personal data of the persons involved and/or mentioned in the Reports, in accordance with the law in force and the company's data protection procedures.

CDP and the CDP Group Companies ensure that the processing of personal data is carried out lawfully and correctly and in any case in accordance with the specific rules established by the current regulations.

Personal data which is manifestly not useful for the processing of a specific Report shall not be collected or, if accidentally collected, shall be erased without delay.

In addition, it should be noted that the confidentiality of employees of CDP and/or Group Companies making a Report is also protected in accordance with the provisions of Article 2 *undecies*, entitled "*Restriction on the rights of the data subject*", of Legislative Decree No. 101 of 10 August 2018 on "*Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)*".

In relation to the disclosure obligations provided for by Article 13 of the GDPR, please refer to the individual disclosures (for each individual Group Company) already included within the IT platform.

Annex 1 Internal channels established in Fintecna

- IT platform: accessible at https://ewhistlecdp.azurewebsites.net/ and on the official website https://www.cdp.it/sitointernet/en/whistleblowing.page
- voicemail inbox: accessible at **0642214761**
- ordinary mail: addressed Internal Audit Department for Fintecna, via Alessandria,220, 00198, Rome, specifying on the envelope the “CONFIDENTIAL” nature of the letter and the wording “**Whistleblowing**”.

A direct and confidential meeting with the Reporting Manager can also be organised by conveying the request through one of the channels mentioned above.