GENERAL WHISTLEBLOWING MANAGEMENT PROCEDURE

pursuant to 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 Union law and laying down provisions on the protection of persons who report breaches of national laws.

Issue date 15.07.2023

Contents

PREAMBLE

On 30 March 2023, **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 Union law and laying down provisions on the protection of persons who report breaches of national laws"* entered into force.

The new rules are designed to create a tool to counter and prevent corruption, maladministration and, more generally, breaches of the law, in the public and private sectors.

In order to ensure the effectiveness of this legality safeguard and incentivise its use, the Italian and European legislators have therefore decided to strengthen the protection against any possible retaliation of persons reporting concerns or (where the conditions are met) making public disclosures, and to extend such protection to any parties involved in the report (e.g. the reporting person's facilitator, family member, confidant, coworker or person referred to). The legal framework also requires the establishment of mechanisms to ensure persons are able to report securely any unlawful conduct of which they become aware.

The main innovations contained in the new legal framework, which no longer distinguishes between the public and private sectors, are summarised below:

- the widening of the material scope (types of reportable offences);
- the widening of the personal scope (list of persons eligible for protection);
- rules covering three different reporting channels: internal (in entities with a dedicated person or office or through an external entity with specific expertise); external (managed by ANAC – the Italian Anti-Corruption Authority and subordinate to the internal channel); public disclosure (where the conditions are met, through the press or social media);
- the establishment of different ways of reporting breaches, in writing or orally, and always with adequate guarantees in terms of security measures put in place to protect the confidentiality of communications.
- the detailed regulation of confidentiality obligations;
- the requirement for a prior data protection impact assessment and the Entity's obligation to take all the technical (e.g. encryption) and organisational measures (e.g. information on data processing, authorisation and staff training, data processing agreements with suppliers, etc.) imposed by the data protection legislation in force, both national (Legislative Decree 196/2003) and European (Regulation (EU) 2016/679 – General Data Protection Regulation – "GDPR"), in order to regulate the processing of personal data received, managed and communicated by or to third parties;

- the broadening of the types of conducts classified as "retaliation" and the strengthening of the related protection measures, offered by both ANAC and the judicial authority, and additional guidance on the reporting person's liability and on exclusions from liability;
- the introduction of special support measures for reporting persons and the involvement for this purpose of third sector entities that have appropriate expertise and provide their services free of charge;
- the revision of the rules on the penalties that can be imposed by ANAC and the introduction by private entities of penalties into their disciplinary system adopted pursuant to Legislative Decree no. 231/2001.

In the light of the above preamble, **F.lli De Cecco di Filippo Fara S. Martino Spa** (hereinafter, the "Company"), to effectively implement the legislation in question, having consulted with the workers' representatives or trade unions, has set up an "internal reporting channel" – via an IT platform that includes a voicemail box, or alternatively, where so requested by the reporting person, via a physical meeting – designed so as to ensure confidentiality and protection for the reporting person (and for any other persons involved). The Company has entrusted said internal reporting channel to an adequately instructed and trained Whistleblowing Report Management Body (hereinafter, the "Report Management Body"), which is autonomous and independent.

1. PURPOSE

This "General Whistleblowing Management Procedure" (hereinafter, the "Procedure") is designed to regulate the process of receiving, analysing and managing the reports by reporting persons (as identified below) of unlawful and suspicious conduct, irregularities, acts or facts that may constitute a breach of national and European laws or of the principles and rules of conduct contained in the Code of Ethics and in the 231 Model adopted by the Company.

2. REGULATORY FRAMEWORK

External rules

- ✓ Legislative Decree no. 24 of 10 March 2023 – Implementation of 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 and laying down provisions on the protection of persons who report breaches of national laws.
- ✓ Legislative Decree no. 196 of 30 June 2003 – Personal Data Protection Code – as amended and/or supplemented;
- ✓ 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;
- ✓ Legislative Decree no. 231/01 "on the administrative liability of legal entities, companies and associations, including those without legal personality, pursuant to Article 11 of Law no. 300 of 29 September 2000" of 08/06/2011 as subsequently updated, where applicable.
- ✓ "Guidelines on the protection of persons who report breaches of Union law and the protection of persons who report breaches of national law – Procedures for the submission and handling of external reports", issued by ANAC pursuant to Article 10 of Legislative Decree no. 24/23 by resolution no. 311 of 12 July 2023.

Internal rules

- ✓ Organisational Model 231
- ✓ Code of Ethics
- ✓ Data Protection Organisational Model

3. MATERIAL SCOPE: WHAT CAN BE REPORTED?

A report may be made where the reporting person has a reasonable and legitimate suspicion or awareness – both based on precise and concordant factual elements – of conduct, in breach of national or European Union law, which harms the public interest or the integrity of the Company, of which they have become aware in the "work-related context". The expression "work-related context" is to be understood in a broad sense. Therefore, the existence of a qualified relationship between the reporting person and the Company concerning present or even past work or professional activities is deemed sufficient. Thus, information acquired in connection with and/or because of the performance of work duties, albeit fortuitously, may also be reported.

Conduct aimed at concealing breaches (e.g. concealing or destroying evidence of a breach) may also be reported.

The report may also relate to breaches not yet committed, which the Reporting person reasonably believes could be committed on the basis of certain tangible elements. These elements may be irregularities or anomalies (symptomatic indicators) that the reporting person believes may result in one of the breaches covered by the Decree.

Whistleblowing reports must be made in good faith, in a spirit of responsibility, be in the common interest, and concern the types of breaches for which the whistleblowing system has been implemented.

✓ WHAT CAN BE REPORTED?

The report may concern two types of breaches, as summarised below[2]:

Breaches of national legislation	**Breaches of EU legislation**
1. Administrative offences 2. Torts/delicts 3. Criminal offences (regardless of their relevance for the purposes of Legislative Decree 231/2001); 4. Accounting offences 5. Where a Model 231 is adopted: Unlawful conduct relevant under Legislative Decree no. 231 of 8 June 2001 (predicate offences such as, by way of example: Misappropriation of funds, fraud to the detriment of the State, a public body or the European Union for the purpose of obtaining public funds, computer fraud to the detriment of the State or a public body and fraud in public procurement), or breaches of the Organisation and Management Model adopted pursuant to Legislative Decree 231/01 or the Company's Code of Ethics.	1. Unlawful conduct falling within the scope of European Union acts in the following areas: public procurement; 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. 2. Acts or omissions harming the financial interests of the Union (e.g. fraud, corruption and any other illegal activity related to Union expenditure). 3. Acts or omissions affecting the proper functioning of the internal market (e.g. breaches of competition and State aid rules). 4. Acts or conduct undermining the object or purpose of the provisions of EU law (e.g. acts that undermine the principle of free competition).

[2] Given the wide scope of cases covered and the complex referral technique envisaged by the legislator, we provide the link to the Official Gazette of the Italian Republic for consultation of the full text of Article 1 of Legislative Decree 24/23 and its Annex.

X WHAT CANNOT BE REPORTED

- Information that is manifestly **unfounded**, information that is already totally **in the public domain**, and information acquired only on the basis of unreliable allegations ("**rumours**" or "hearsay").
- Disputes, claims or demands linked to a **personal interest of** the reporting person or of the person lodging a complaint with the judicial or accounting authorities, which relate exclusively to their individual private or public employment relationship, or to their private or public employment relationship with hierarchical superiors. The following types of reports are therefore excluded from this policy: reports on **labour disputes** and **pre-litigation phases**, discrimination between coworkers, **interpersonal conflicts** between the reporting person and another worker or with hierarchical superiors, reports concerning data processing carried out in the context of the individual employment relationship in the absence of harm to the public interest or to the integrity of the public administration or private entity;
- Breaches already mandatorily regulated by the EU or national acts listed in Part II of the Annex to the Decree or by the national acts implementing EU acts listed in Part II of the Annex to Directive (EU) 2019/1937, even if not listed in Part II of the Annex to the Decree (for instance, reports of breaches governed by Legislative Decree no. 385 of 1 September 1993 "Consolidated Law on Banking and Credit" or by Legislative Decree no. 58 of 24 February 1998 – Consolidated Law on Financial Intermediation are excluded);
- National security breaches, as well as procurement breaches relating to defence or national security aspects, unless such aspects are covered by the relevant secondary law of the European Union.

4. CONTENT OF WHISTLEBLOWING REPORTS

Reports should be as detailed as possible, including all the elements that may be useful for the whistleblowing Report Management Body to carry out the necessary checks and enquiries to assess their grounds. To this end, reporting persons must provide at least the following elements:

- the time and place in which the reported event occurred;
- a description of the fact with an indication of the known circumstances (how, when and where);
- personal details or other elements enabling the identification of the person to whom the reported facts are attributed (the "person concerned");
- unless the whistleblowing report is anonymous, the identification details of the reporting person, including their position or function within the Company;
- the reporting person's good faith and lack of any private interests in making the report;
- any information or evidence (by attaching the relevant documents) that may corroborate the allegations, including the mention of any other persons who may substantiate the reported facts;
- If the report is not anonymous, the reporting person's identification details (name, surname, job title, etc.). As will be further discussed, these data are protected by specific technical and organisational data security measures to ensure the absolute confidentiality of the reporting person's identity.

If the report is not sufficiently detailed, the Whistleblowing Report Management Body may request **additional information** from the reporting person via the Whistleblowing Portal or even in person, if the reporting person has requested a physical meeting.

Anonymous reports are allowed if they are sufficiently detailed; they shall be handled in the same way as reports by "named" persons. In the case of an anonymous report, retaliation protection measures will only be applicable if the reporting person is subsequently identified.

Reports should not contain excessive personal data, but only the data necessary to show that the complaint is justified. Thus, as a rule, no specific data[3] or personal data revealing health or judicial proceedings should be provided. If the reports contain the aforementioned categories of personal data, concerning the reporting person or third parties, and such data are not necessary for the aforementioned purposes, the Company shall destroy them or, if this is not possible, redact them, except in cases authorised by law or by a measure of the Italian Data Protection Authority.

If the report does not fall within the scope of this procedure, which is based on the material scope described above, the Report Management Body will forward it to the competent corporate area/function and/or to the competent authorities, as specified below (see paragraph 6). In any case, such reports are considered "protected". This means that the Report Management Body shall not disclose the identity or personal data of anyone who has submitted such a report without first obtaining their express consent – unless disclosure is required by law, law enforcement investigations or subsequent court proceedings.

In all the above-mentioned cases of data disclosure, the Controller shall ensure that appropriate measures are always taken to avoid the unnecessary circulation of information, so as to ensure appropriate confidentiality in light of the particular purposes of the data processing in question.

5. PERSONAL SCOPE: WHO CAN REPORT?

Persons operating within the Company's work-related context are entitled to report. They include

- employees;
- self-employed workers;
- collaborators, freelancers and consultants;
- interns and trainees, paid and unpaid;
- shareholders and persons with administrative, management, supervisory or representative functions, even if such functions are exercised on a *de facto* basis.

Reporting can be done:

- when the legal relationship is ongoing;
- during the probationary period, if the information was acquired during the selection process or in other pre-contract stages;
- when the legal relationship has not yet begun, if information on breaches was acquired during the selection process or at other pre-contract stages;
- after the termination of the legal relationship, if the information on breaches was acquired before such termination (retirees).

[3] Information revealing racial or ethnic origin, sexual orientation, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or religious, philosophical, political or trade union organisations.

6. RECIPIENT OF REPORTS

The Report Management Body is Mr Nicola Lotti La Barba D'Alessandro.

Such Body, in its capacity as Recipient of the Report:

- is autonomous and independent;
- shall guarantee a fair and impartial assessment of the report received;
- shall respect the confidentiality obligation, in particular on the identity of the reporting person, the reported person and other persons involved (facilitator, family members, co-workers, witnesses, etc.);
- shall handle the report (shall assess admissibility and carry out the initial assessment of the reported facts or conduct);
- shall manage contacts with the reporting person (issuing notices of receipt and closure of the report and exchanging information);
- shall inform the reporting person of the outcome of the investigation (giving feedback about the actions envisaged or taken as follow-up to the report and the reasons for the choice made).
- The Report Management Body shall duly publicise this procedure and the other channels (external channel, public disclosure, reporting) provided for by Legislative Decree 24/2023, with particular regard to the requirements for access to the competent persons and procedures.

If the report is submitted to a **party other than** the Report Management Body appointed by the administration or company, within seven days of receiving the report, the initial recipient shall forward it to the competent body, simultaneously notifying the reporting person of such transmission.

If the reporting person believes that the Report Management Body has a conflict of interest, they may submit their report to Martina Colombara, stating the reason for the conflict.

7. REPORTING CHANNELS AND ASSISTANCE

Any person who has a reasonable suspicion that one of the breaches under paragraph 3 has been committed, may make a written or oral report using the following internal channels:

- Through the **Whistleblowing Portal**, as specified below.
- By means of a **physical meeting** with the Report Management Body, arranged in such a way (e.g. choice of venue and time of the meeting) as to ensure the confidentiality of the reporting person in accordance with the relevant legislation.

Should the reporting person need assistance, they may contact the Whistleblowing Contact Person, who is the Corporate Social Responsibility and Sustainable Development Manager, Giovina Di Cecco, at the following email address – ginadicecco@gmail.com.

The above person has been trained on the functioning of the reporting channels and on this procedure, and will be able to assist the reporting person while maintaining absolute confidentiality on the assistance provided.

Please note that the above e-mail address is **NOT** an alternative reporting channel. Thus, to ensure the confidentiality and security of information, the e-mail to the Whistleblowing Contact Person should **NOT** include details of the report (factual circumstances, name of the reported person and/or witnesses, etc.) **but should only request assistance, agreeing on the terms.**

Alternatively, the reporting person may contact a trusted person, who, acting as a "Facilitator" within the meaning

of the relevant legislation, shall be entitled to the same protection as the reporting person (see paragraph 9 below).

7.1 THE WHISTLEBLOWING PORTAL

The Whistleblowing Portal can be accessed at the following dedicated web address:

https://digitalroom.bdo.it/dececco

The platform allows anyone (employees and collaborators, suppliers and any other person as defined in paragraph 5) to report breaches through a guided online procedure, guaranteeing the confidentiality of the reporting person's identity or, where chosen, total anonymity. Indeed, the system allows reporting persons to make reports without having to register or provide their personal details. If the reporting person chooses to give their personal details, confidentiality is guaranteed.

The platform allows confidential interaction with the reporting person, with no possibility for the receiver or other parties to trace the origin of the report.

Specifically, no log-in is required to access the Whistleblowing Portal, thereby preventing the identification of reporting persons who wish to remain anonymous. This means that the Company's IT systems are unable to identify the portal access point (IP address) even when access is made from a computer connected to the Company's network.

Reports transmitted via the Whistleblowing Portal are received exclusively by members of the whistleblowing Report Management Body. Indeed, the reporting person's identity can be associated with the report only by the Report Management Body.

The data contained in the reports will be processed using organisation and processing logic that guarantees the security, integrity and confidentiality of the data in compliance with the organisational, physical and logical measures laid down in the legislation in force.

In particular, the transmission of data provided by the reporting person using the platform is managed with the HTTPS protocol. Encryption techniques are also utilised to ensure the confidentiality of the information transmitted.

After accessing the Portal, the reporting person can choose whether to use the voicemail box or fill in a questionnaire consisting of open-ended questions allowing them to provide the elements of the report (facts, temporal context, etc.).

The Portal will ask the reporting person whether they wish to disclose their identity. In any case, the reporting person may also provide their personal details at a later stage, including through the messaging system provided by the Portal. The voicemail box, on the other hand, has voice-disguising features for the same purpose.

When the report is submitted, the Portal will issue the reporting person with a unique identification code (ticket). This number, known only to the reporting person, cannot be recovered if lost. The reporting person can use the report ID code to access their report via the Portal in order to monitor the progress in processing the report, enter further information to substantiate the report, provide personal details, and answer any further questions.

7.2 PHYSICAL MEETING

If the reporting person prefers to meet in person with the Report Management Body, they may request the latter to arrange a meeting, which may take place in person or via remote communication systems, in either case guaranteeing the confidentiality imposed by law.

In that case, the Report Management Body shall schedule the meeting within a reasonable time.

At the time of the meeting – after providing the privacy policy and/or information on where to find the full text of the policy – to ensure the traceability of the oral report and the same level of protection as for written reports, the Report Management Body shall record on the IT platform the report and the progress of the initial assessment.

8. REPORT MANAGEMENT

8.1. MANAGEMENT PROCEDURE

Reports received by the Report Management Body are subject to the following assessment procedure.

Reports that are too vague to be assessed with a reasonable prospect of tangible results will not be examined further, and the procedure will be immediately closed.

The reports and their supporting documents will undergo an initial assessment by the Report Management Body, to verify the presence of sufficient data and information to assess the abstract merits of the report, as a basis for further investigation.

Following this assessment, if the Report Management Body finds that the reported fact is not relevant under Legislative Decree no. 24/23, but may be relevant to the Company for other purposes, it shall promptly forward the report to the competent body/organisation, informing the reporting person thereof.

If, on the other hand, the Report Management Body considers that the report appears to be reasonably well-founded/reliable, it will carry out an in-depth investigation into the reported facts, to ascertain whether they are well-founded. In carrying out this initial assessment – with regard to specific aspects covered by the report and where deemed necessary – the Report Management Body may avail itself of the support of other corporate functions to the extent of its competence, and may request further information and/or documentation from the reporting person through the Portal or even in person, always taking care to preserve the confidentiality of the reporting person's identity.

If the initial assessment finds that the details provided are insufficient or the reported facts are unfounded, the report will be closed, providing reasons. In such a case, the Report Management Body will inform the reporting person of the conclusion and results of the assessment carried out.

If, instead, the initial assessment finds sufficient elements to consider the report well-founded, a more in-depth investigation will be launched.

In this case, the Report Management Body shall:

- launch in-depth analyses with the help, if deemed appropriate, of the Company's competent structures;
- on completing the in-depth investigation, submit the results for assessment to the competent internal bodies or external bodies/institutions, each according to its competences, depending on the subject of the report, so that the most appropriate measures can be taken. It is not for the Report Management Body to ascertain individual responsibilities, whatever their nature, nor to carry out lawfulness or substantive checks on the acts and measures adopted by the reported body/administration.
- terminate the initial assessment at any time if, in the course of such assessment, it is established that the report is unfounded.

The described activities need not be carried out sequentially.

In any case, at the end of the initial assessment phase, the Report Management Body shall inform the reporting

person of the outcome of the assessment, giving feedback about the action envisaged or taken as follow-up to the report and the grounds for the choice made, provided that such information does not affect the internal enquiry or investigation or harm the rights of the person concerned (e.g. notice of closure of the procedure, referral to the competent authority for further investigation, launch of an internal enquiry, etc.).

In the spirit of prioritising the reporting person's will, the reporting person may at any time **withdraw their complaint** by sending a communication to that effect through the channel originally chosen for filing the complaint. In that case, any investigations already started will be closed.

8.2. TIMEFRAME

In managing the internal reporting channel, the Report Management Body shall:

- issue an acknowledgement of receipt to the reporting person within 7 days of the date of receipt of the report;
- provide prompt feedback to any requests submitted by the reporting person through the reporting channels (messaging system deployed on the platform);
- provide feedback on the report within three months from the date of notice of receipt or, in the absence of such notice, from the expiry of the seven-day period from the submission of the report.

9. THE SYSTEM OF PROTECTION

The protection system under Legislative Decree no. 24/2023 comprises the following types of protection:

1. protection of the confidentiality of the reporting person, the facilitator, the person concerned and the persons referred to in the report;
2. protection against any retaliatory measures taken by the entity by reason of the report, public disclosure or complaint made and the conditions for its application[4];
3. limitations on liability in connection with the disclosure and dissemination of certain categories of information apply under certain conditions[5];

[4] The legislation has established a very broad notion of retaliation that includes:
"any conduct, act or omission, even if only attempted or threatened, prompted by internal reporting, reporting to the judicial or accounting authorities or public disclosure and which causes or may cause, directly or indirectly, unjustified detriment to the reporting person". In order for retaliation to occur and, consequently, for the person to benefit from protection, there must be a close link between the reporting or disclosure and the adverse treatment/act/omission suffered, directly or indirectly, by the author of the report, complaint or public disclosure. No protection against retaliation is provided when the reporting person has been found guilty, even by a court of first instance, of the criminal offences of defamation or slander or, in any case, of the same offences committed by reporting to the judicial or accounting authorities or has incurred civil liability for the same offences in cases of wilful misconduct or gross negligence, even by a court of first instance. The management of retaliation reports is the responsibility of ANAC, which is in charge of ascertaining whether the retaliation is consequent to the report, complaint or public disclosure made.

[5] These limitations apply under certain conditions, without which criminal, civil and administrative liability would be incurred.
The exemption, however, operates only where two conditions are SIMULTANEOUSLY fulfilled:
1. The first is that at the time of disclosure or dissemination there are reasonable grounds to believe that the information is necessary to reveal the breach. The person must therefore reasonably believe, not on the basis of mere inferences, that the information must be disclosed because it is indispensable in order to reveal the breach, excluding any superfluous information, and not for other, different reasons (e.g. gossip, revenge, personal gain or scandal-mongering purposes);
2. The second condition, on the other hand, is that the report, public disclosure or complaint be made in compliance with the conditions laid down in Legislative Decree no. 24/2023 in order to benefit from the protection granted to whistleblowers (reasonable grounds to

4. the provision of support by third-sector entities included in a special list published by ANAC[6].

These protection measures are granted, in addition to the reporting person, to the following persons:

- ✓ the **facilitator** (a natural person who assists the reporting person in the reporting process, operating within the same work-related context and whose assistance must remain confidential). By way of example, the facilitator could be a colleague belonging to a different office than the one to which the reporting person belongs, who assists the reporting person in the reporting process on a confidential basis, i.e. without disclosing the information acquired. The facilitator may be a colleague who is also a trade union officer, provided he/she assists the reporting person in a personal capacity, and not as a trade union officer;
- ✓ **persons in the same work-related context as the** reporting person, the person making a complaint or the person who has made a public disclosure and who are linked to them by a stable emotional or family relationship up to the fourth degree;
- ✓ **colleagues** of the reporting or publicly disclosing person, who work in the same work-related context as the reporting person and who have a habitual and current relationship with that person.
- ✓ **legal entities** that the reporting persons own, work for or are otherwise connected with in a work-related context.

Full or partial waivers and settlements relating to the rights and protections granted by the Decree shall not be valid, unless they are made in the protected fora referred to in Article 2113(4) of the Civil Code.

9.1 PROTECTION OF CONFIDENTIALITY

The Company guarantees the confidentiality of the Reporting person's identity[7] from the time it receives the report, in compliance with the provisions of the law. To this end, the personal identification data of the reporting person are not directly visible in the report and are stored in such a way as to be visible only to the whistleblowing Report Management Body. The Company has put in place all the safeguards and technical and organisational measures provided by law in order to protect the confidentiality of the reporting person's identity, so that it is not disclosed to third parties without the reporting person's express consent, except in the case of malicious or defamatory reports. These measures include the redaction of personal data, especially those relating to the reporting person, but also of other persons whose identity, under Legislative Decree 24/2023, must remain confidential (the facilitator, the person concerned, the other persons referred to in the report), if, for investigative reasons, other persons also need to be made aware of the content of the report and/or of the documents annexed thereto.

No direct or indirect retaliation or discrimination is allowed against a person who has made a report in **good faith**, regardless of whether or not the report turns out to be well-founded.

Penalties are provided for those who breach the protection and confidentiality measures in place for reporting persons.

On the other hand, the protection of the reporting person **is not** guaranteed in the event of reports made with

believe that the information on the breach is true and concerns one of the reportable breaches under Legislative Decree no. 24/2023; internal and external reports, public disclosures made in the manner and under the conditions set out in Chapter II of the Decree).

[6] To further strengthen the protection of reporting persons, the law provides that ANAC may enter into agreements with third-sector entities that will provide support to the reporting person (assistance and advice free of charge). These entities will be included in a special list published by ANAC on its official website.

[7] The protection afforded by the Decree, in accordance with the principles of data protection legislation, includes the prohibition to disclose, without the reporting person's express consent, the identity of the reporting person and any other information from which that identity may be directly or indirectly inferred, to persons other than those authorised to receive or follow up on the reports.

malice or **gross negligence** or which prove to be false, unfounded, defamatory or otherwise made with the sole purpose of harming the Company, the person concerned or other persons referred to in the report. Penalties are provided against the reporting person, if identifiable, in the event of reports made with malicious intent or gross negligence or which prove to be false, unfounded, defamatory or otherwise made with the sole purpose of harming the Company, the person concerned or other persons referred to in the report.

The Company may also take appropriate legal action.

In the event of **disciplinary proceedings**, the identity of the reporting person may not be disclosed where the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it. The reporting person's identity may only be disclosed where:

- the charge is based, in whole or in part, on the report itself and knowledge of the identity of the reporting person is absolutely essential for the accused's defence; and
- the reporting person gives their consent.

In such a case, the Company shall inform the reporting person in writing in advance of the reasons for disclosing their identity.

10. PROTECTION OF THE PERSON CONCERNED

The Company ensures adequate protection for the persons directly or indirectly targeted by the report.

The report is not sufficient to initiate any disciplinary proceedings against the person concerned.

Therefore, no disciplinary penalties may be issued against the person concerned on the basis of the allegations made by the reporting person, without obtaining objective evidence and investigating the reported facts.

This could possibly be done using other evidence found and investigated on the basis of the report.

If proceedings are launched against the person concerned after the assessment and analysis of the report, and if such proceedings are based in whole or in part on the report, the person concerned may be contacted and given the opportunity to provide any necessary clarification.

11. PROTECTION OF PERSONAL DATA AND RECORD-KEEPING

The personal data of the reporting person and of other persons entitled to protection (e.g. facilitator, persons referred to, persons concerned, etc.) and the information contained in the reports and any documents annexed thereto, as well as any data acquired during the initial assessment by the Report Management Body, are processed in accordance with the Personal Data Protection Policy adopted by the Company, in observance of the principles of fairness, lawfulness, transparency and protection of the confidentiality and rights of all the persons concerned (the reporting person, the person concerned and any connected third parties), and in compliance with the obligations imposed by the data protection legislation in force.

The Company, as Data Controller, has carried out a prior Impact Assessment of its whistleblowing management system, which can be consulted upon request to the Report Management Body.

The Company has consequently adopted appropriate technical and organisational data protection measures, which are periodically audited. Notably:

- the Company has adopted a whistleblowing management platform that guarantees appropriate technical protection measures, such as encryption, segregation of access, prohibition of tracking the

reporting person, tracking of the operations of the Report Management Body;

- The Company has put in place organisational measures such as: the authorisation, instruction and training of personnel authorised to access the personal data in question; formal agreements with suppliers acting as data processors (e.g. SaS supplier of the whistleblowing management platform); provision of the privacy policy pursuant to Article 13 GDPR to the data subjects; updating of the data processing register.

The Report Management Body keeps on file all the documentation supporting the report received. Personal data relating to reports are retained and kept for the period necessary to complete the investigation of the allegations contained in the report and for **5 years** thereafter, **starting from the date of notification of the final outcome of the report assessment procedure,** without prejudice to any proceedings arising from the management of the report (disciplinary, criminal, accounting) against the person concerned person or the reporting person (bad faith, false or defamatory statements). In that case, the documents will be retained for the duration of the proceedings and until the expiry of the time limit for appealing the relevant measure. At the end of said period, the data are either deleted or irreversibly anonymised and stored for statistical purposes only.

12. PENALTIES

Breaches of the principles laid down in this procedure shall be prosecuted promptly and immediately.

The Company reserves the right to take disciplinary action against the reporting person in the event of misuse of the whistleblowing tool, for example in the event of reports manifestly made for personal gain and/or for the sole purpose of harming the person concerned or the persons referred to in the report, and any other case of improper use or intentional exploitation of the whistleblowing tool and procedure.

Penalties will be applied on the basis of the **Workers' Statute (Law no. 300/1970)** and individual National Collective Bargaining Agreements, without prejudice to the possibility of seeking further remedies before the competent courts.

13. UPDATES TO THE POLICY

This Procedure and the Portal shall be periodically reviewed to ensure constant alignment with the relevant legislation and in the light of the experience gained.

14. AWARENESS-RAISING AND PUBLICITY

Through its whistleblowing Report Management Body, the Company runs communication and awareness-raising initiatives on this procedure and the other reporting channels provided for by Legislative Decree 24/23 (external channel, public disclosure, legal action). This is done through training initiatives disseminated via the intranet portal and the Company's official website to all potential reporting persons. The training covers the aims of the Whistleblowing system and the procedures for its proper use; the related rights and obligations; the consequences of misuse of the system; and the results generated by implementation of the system.

15. ANNEXES

The following are attached:

Annex 1: *Privacy Policy*

Annex 2: *Workflow*

ANNEX 1

PRIVACY POLICY PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679

(GDPR – GENERAL DATA PROTECTION REGULATION)

MANAGEMENT OF REPORTS (WHISTLEBLOWING)

PARTIES TO WHOM THE PRIVACY POLICY IS ADDRESSED	DEFINITION
Reporting person (or complainant/whistleblower)	A natural person who reports information on breaches acquired in the context of their work-related activities.
Person concerned (or reported)	The natural or legal person who is referred to in the report as a person to whom the breach is attributed or who is howsoever involved in the reported breach.
Facilitator	A natural person who assists a reporting person in the reporting process, operating in the same work-related context, and whose assistance must be confidential.
Third party	A natural person, other than the reporting person and the person concerned, whose personal data might be contained in the report or acquired in the course of the initial assessment.

SCOPE OF THE DATA PROCESSING

F.lli De Cecco di Filippo Fara San Martino S.p.A., with registered office in Fara S. Martino (CH), via F. De Cecco, VAT no. 00628450694 in the person of its current legal representative, in its capacity as "Controller" of the personal data processing, hereby informs you of the characteristics and methods of the processing of personal data provided during a physical meeting with the Report Management Body (or responsible body) or, in written or oral form, through the "*Whistleblowing Management Platform".* The report management process is governed by the specific procedure adopted by the Company, which can be consulted by employees on the Company's intranet and by anyone on the Company's website www.dececco.com in the "***Whistleblowing Reports***" section and at the following link https://digitalroom.bdo.it/dececco, which must be read.

The personal data provided by the reporting person and the information contained in the reports and in any documents annexed thereto, as well as any data acquired during the initial assessment by the Report Management Body, shall be processed in accordance with the principles of fairness, lawfulness, transparency and protection of the confidentiality and rights of all the persons involved (reporting person, person concerned, facilitator and any third parties as defined in the introduction), in compliance with the obligations imposed by the data protection legislation and by Legislative Decree no. 24/2023, "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 Union law and on the protection of persons who report breaches of national laws".

Since suspected breaches can also be reported anonymously on the platform provided by the Company, the reporting persons are not required to disclose their personal data. However, since any subsequent identification of the reporting person could expose them to the risk of possible retaliation by the person concerned, pursuant to Article 16 of Legislative Decree 24/2023, the reporting person who has resorted to anonymity, in the event of subsequent disclosure of their identity, shall benefit from the protection measures afforded to all reporting persons.

In any case, even in the case of anonymous reports, it cannot be ruled out that, in the course of examining the reports, the Report Management Body might receive information containing identification data, professional data, or financial data concerning the other categories of interested parties (person concerned, third parties), which shall be processed pursuant to this privacy policy.

PURPOSE AND LEGAL BASIS OF DATA PROCESSING

The personal data provided by the reporting person and acquired by the body performing the initial assessment in the course of the procedure will be processed in relation to the obligations under Legislative Decree 24/2023.

In particular, said data will be processed for the following purposes:

- **Managing the reports** (investigating the reported facts). The primary legal basis for the processing is the legal obligation for the Controller [under Article 6(1)(c) GDPR, or, where it is essential to provide specific data to substantiate the report, under Article 9(2)(g) GDPR], in accordance with the provisions of Leg. 24/2023, to implement an IT platform for submitting and managing whistleblowing reports. Any processing of data in subsequent court or out-of-court proceedings is based on the legitimate interest of the Controller (Article 6(1)(f) or, where the processing of special data is required, on Article 9(2)(f) GDPR).

- **Managing any disciplinary proceedings based in whole or in part on reporting**. In order to ensure the right of defence of the person concerned, the information contained in the report may be used, together with any other external evidence, in the disciplinary proceedings initiated against the person concerned. On the other hand, the identity of the reporting person, may be disclosed in the context of disciplinary proceedings – hence also to the person concerned – only if those proceedings are based exclusively on the content of the report, in order to ensure the right of defence of the person concerned and, in any case, subject to the express consent of the reporting person. The consent of the reporting person to the disclosure of their identity during disciplinary proceedings is not mandatory, but failure to give such consent means that disciplinary proceedings based solely on the reporting person's statements cannot be brought against the person concerned.

TYPE OF DATA PROCESSED

The Whistleblowing Management Platform implemented by F.lli De Cecco di Filippo Fara San Martino Spa only collects the identification data of the reporting person (if provided) and the data communicated in the reports. However, in the course of the procedure, the following personal data may be acquired:

- identification document, any other contact details given by the reporting person;

- Information (identification data[8], professional data[9], financial data[10]) on the person concerned, contained in the report or acquired during the initial assessment;
- Information (identification data, professional data, financial data) relating to third parties that may be included in the report and in any documents attached or acquired during the initial assessment.

The personal identification data of the reporting person are not directly visible in the report and are stored in such a way as to be visible only to the whistleblowing Report Management Body. The Company has put in place all the safeguards provided by law in order to protect the confidentiality of the reporting person's identity, so that it is not disclosed to third parties without the reporting person's express consent, except in the case of malicious or defamatory reports.

As set out in the Whistleblowing Procedure adopted by the Company, reports should not contain excessive data, but only the data necessary to prove the grounds for the report. As a rule, therefore, no special data[11] or personal data disclosing health or judicial status will be included. If the reports contain the aforementioned categories of personal data, concerning the reporting person or third parties, and such data are not necessary for the aforementioned purposes, the Company shall destroy them or, if this is not possible, redact them, except in cases authorised by law or by a measure of the Italian Data Protection Authority.

DATA PROCESSING METHODS

The processing will be carried out via an IT platform accessible from a link on the Company website made available in the dedicated section. The data will be processed with organisation and processing logics strictly related to the above-mentioned purposes, and in such a way as to guarantee the security, integrity and confidentiality of the data, in compliance with the organisational, physical and logical measures laid down in the legislation in force.

In particular, the transmission of data provided by the reporting person using the platform is managed with the HTTPS protocol. Encryption techniques are also utilised to ensure the confidentiality of the information transmitted.

Finally, it should be noted that the personal data identifying the reporting person are stored in such a way as to ensure their confidentiality. Indeed, the reporting person's identity can be associated with the report only by the Report Management Body.

DATA STORAGE PERIOD

Pursuant to Article 14 of Legislative Decree 24/2023, personal data relating to reports, and the related documentation shall be stored and kept for the period necessary to complete investigation of the facts set out in the report and in any event **no longer than five years from the date of the communication of the final outcome of the report assessment procedure**, in compliance with the confidentiality obligations set out in Article 12 of this Decree and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679 and Article 3(1)(e) of Legislative

[8] *E.g. name, surname, date and place of birth, address, telephone number, fax number, e-mail address.*

[9] *E.g. occupation, employer and role held.*

[10] *E.g. pay slips, bank accounts and securities portfolios.*

[11] *Information revealing racial or ethnic origin, sexual orientation, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or religious, philosophical, political or trade union organisations.*

Decree no. 51 of 2018. In the event of any proceedings arising from the handling of the report (disciplinary, criminal, accounting) against the person concerned or against the reporting person (bad faith, false or defamatory statements), the data in question will be retained for the duration of the proceedings and until the expiry of the time limit for appealing the relevant measure.

RECIPIENTS OF PERSONAL DATA

For the pursuit of the above-mentioned purposes, the information sent through the whistleblowing platform shall be managed by those Company persons who have been duly designated, trained and instructed and must manage such data to fulfil their tasks in receiving, analysing, assessing and managing reports and taking any consequent actions.

It is reiterated that only the whistleblowing Report Management Body will have access to the identification data of the reporting person, if provided.

The data that are the subject of the report, on the other hand, may also be processed by employees of F.lli De Cecco Di Filippo Fara San Martino Spa who have been authorised to do so and who shall follow the instructions given by the Controller. This data may also be processed by external consultants or suppliers designated as data processors for this purpose pursuant to Article 28 GDPR, who shall operate according to the instructions given by the Controller, in particular by putting in place appropriate security measures to ensure the confidentiality and security of the data. In particular, one such data processor is BDO, the company that provides the platform and processes the information uploaded to it by means of a filing system on servers located in Italy. It should be noted that this supplier provides the infrastructure needed to implement the IT reporting procedure, but does not access the content uploaded to it (identity of the reporting person, subject of the reports, attached documents, messages exchanged between the reporting person and the body carrying out the initial assessment, etc.).

The personal data contained in the reports may also be communicated to the competent offices of F.lli De Cecco Di Filippo Fara San Martino Spa and/or of the Group's Companies to launch judicial and/or disciplinary actions connected with the report, or to the competent authorities in the event of breaches of the applicable legislation.

If the report does not fall within the competence of the whistleblowing Report Management Body on the basis of the material scope of this procedure, it shall be forwarded to the competent business area/body and/or the competent authorities. In any case, such reports are considered "protected". This means that the Report Management Body shall not disclose the identity or personal data of anyone who has submitted such a report via the whistleblowing platform without first obtaining their express consent – unless disclosure is required by law, law enforcement investigations or subsequent court proceedings.

In all the above-mentioned cases of data disclosure, the Controller shall ensure that appropriate measures are always taken to avoid the unnecessary circulation of information, so as to ensure appropriate confidentiality in light of the particular purposes of the data processing in question.

DATA DISCLOSURE

Your personal data will not be disclosed to unspecified recipients or published.

TRANSFER OF DATA ABROAD

Your personal data will not be transferred outside the EU.

Intra-group transfers are only envisaged where necessary to carry out checks (e.g. the complaint involves a partner or manager of a different group company). In such cases, equivalent confidentiality safeguards and appropriate data transmission security measures will be ensured.

RIGHTS OF DATA SUBJECTS

1. Rights of the reporting person

Within the limits of the provisions of Article 2-undecies of Legislative Decree No 196 of 30 June 2003, the reporting person can exercise the rights under Articles 15 to 22 of the GDPR:

- right of access to personal data;
- right to have their data rectified or deleted (except for the contents of the report);
- right to withdraw consent, where provided for: the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal; withdrawal of consent will prevent the reporting person from access their profile, but they will still be able to view their reports by means of their codes. However, withdrawal of consent is not allowed where processing is necessary for compliance with a legal obligation to which the controller is subject;
- the right to lodge a complaint with the Italian Personal Data Protection Authority pursuant to Article 77 GDPR or to appeal to the competent judicial authority pursuant to Article 79 GDPR, in the manner and within the limits provided for by current national legislation (Legislative Decree 196/2003).

2. Rights of the person concerned

Pursuant to Article 2-undecies of Legislative Decree 196/2003 (Italian Privacy Code), the Data Controller hereby informs the person concerned that the exercise of the rights set out above (the data subject rights set out in Articles 15 to 22 of the GDPR) and in particular the right of access, may be delayed, limited or excluded for as long as this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the person concerned, in order to safeguard the confidentiality interests of the reporting person and to avoid the risk of the investigation being undermined (e.g. tampering with evidence, concealment of information).

The above rights may not be exercised by a request to the Controller, or by a complaint pursuant to Article 77, where the exercise of those rights may adversely affect the confidentiality of the identity of the reporting person. In such cases, however, the rights of the data subject may be exercised through the Italian Data Protection Authority in the manner set out in Article 160 of Legislative Decree no. 196/2003, under which the Authority shall inform the person concerned that it has carried out all the necessary checks or that it has conducted a review, without prejudice to the right of the person concerned to seek a judicial remedy.

In all other cases, you can exercise your rights by contacting our Data Protection Officer (DPO), Lawyer Giulio Maria Garofalo, at DPO@dececco.it

COOKIES

No personal data of users are acquired by the platform.

No cookies are used to transmit personal data nature, nor are persistent cookies used to track users.

Only technical cookies are used, to the extent strictly necessary for the correct and efficient use of the platform. The use of session cookies (which are not permanently stored on the user's computer and disappear when the browser is closed) is strictly limited to transmitting session identifiers (consisting of random numbers generated by the server) necessary to enable the safe and efficient navigation of the platform.

ANNEX 2

START

Reporting person

Submits the report

The report can be made either through
1) physical meeting with the Report Management Body
2) whistleblowing portal

The reporting person may at any time withdraw the report by sending a communication through the channel used to submit the original report. In that case, any investigations already started will be closed.

Acknowledgement of receipt within 7 days of receipt of the report

Report Management Body

Preliminary analysis of reports and their supporting documents

Report Management Body

Closes the report providing grounds, informing the reporting person of the conclusion and outcome of the investigation

NO

Sufficiently detailed elements

YES

impact for the purposes of Legislative Decree 24/23?

NO

YES

Report Management Body

Launches the initial assessment phase

Provides feedback on the report within three months from the date of the notice of receipt -

MANAGEMENT OF REPORTS

Competent body

Forwarding to the function/body competent for the matter concerned, informing the reporting person

Report Management Body

In-depth investigation of the reported facts

At this stage, the Report Management Body, while keeping the identity of the reporting person confidential, may request the support of other corporate functions and further information and/or documentation from the reporting person

Closes the initial assessment at any time if it is established that the report is unfounded.

- initiates specific analyses;
- submits the results for assessment by the relevant internal bodies or external entities/institutions, each according to their competences, depending on the subject of the report, for the most appropriate action to be taken.

It is not for the Report Management Body to ascertain individual responsibilities, whatever their nature, nor to carry out lawfulness or substantive checks on the acts and measures adopted by the reported entity/administration.

Report Management Body

informs the reporting person of the outcome of the report, giving feedback about the action envisaged or taken

END