



Genoa, January 25, 2026

COMMUNICATION TO ALL STAFF

Updated Whistleblowing Policy pursuant to Legislative Decree no. 24/2023

PRELIMINARY REMARKS

This **COMMUNICATION**:

- outlines to all staff the regulatory changes introduced by Legislative Decree no. 24/2023 on whistleblowing;
- is made available to all addressees on Company's website and posted on notice boards in easily accessible areas.

1. LEGISLATIVE DECREE NO. 24/2023 (NEW WHISTLEBLOWING POLICY)

The **Legislative Decree no. 24/2023** (hereinafter also referred to as "the Decree"), implementing EU Directive (EU) 1937/2019, and in force as of March 30, 2023):

- consolidates into a single legislative instrument **the rules on reporting channels and the protections afforded to those who report breaches** of national or European Union law that harm the Company's interest or integrity and of which they have become aware in the course of their work-related activities;
- requires public bodies and companies to establish reporting channels (**Whistleblowing**);
- contains provisions on the protection of persons who report breaches of national law.

1.1 Date of application of the new policy

In accordance with the time limits set by the Decree for companies with more than 249 employees and adopting an Organisation and Management Model pursuant to Legislative Decree no. 231/2001 (administrative liability of legal entities), the Company applies the provisions of the new policy as of **July 15, 2023**.

1.2 Subject matter of reports

Reports may concern conduct, acts, omissions and information in respect of which the reporting person has well-founded suspicions supported by specific evidence, which may constitute:

- actual or potential breaches of EU law, national law or Company regulations;
- information on breaches that may be committed;
- conduct aimed at concealing such breaches;
- conduct that violates the ethical principles and standards to which the Company voluntarily adheres;
- negligence, whether or not amounting to a criminal offence, that directly affects strategic national or EU interests (e.g. privacy, environment, tax offences).

In particular, reports should be made of conduct, acts or omissions relating to:

- administrative, accounting, civil or criminal offences;



- unlawful conduct relevant under Legislative Decree no. 231/2001 or breaches of Company's **Organisation and Management Model**;
- breaches falling within the scope of EU or national law relating to the following areas: prevention of money laundering and terrorist financing; transport safety; environmental protection; privacy and personal data protection; security of networks and information systems;
- acts or omissions that harm the financial interests of the European Union;
- acts or omissions relating to the internal market;
- conduct or practices that undermine the object or purpose of EU law provisions.

The following are excluded from the scope of the new policy: disputes, claims or requests connected with reporting person's personal interest, as well as accounting matters that concern exclusively their employment relationship with the Company.

Anonymous reports are accepted only where they are sufficiently detailed and capable of bringing to light specific facts and circumstances. They will be considered only where they do not appear irrelevant, manifestly unfounded or lacking sufficient detail.

1.3 How to submit reports

Reports can be transmitted:

- a) in writing, including by electronic means;
- b) orally, via telephone lines or voice messaging systems;
- c) by means of a face-to-face meeting, at the *reporting person's* request, to be held within a reasonable timeframe.

1.4 Subjects entitled to make reports

Reports of wrongdoing and breaches may be made by anyone who, in any capacity, performs work or services for the Company, whether or not for remuneration, and who, at their workplace, witnesses or becomes directly aware of wrongdoing or irregularities and intends to report them in the interest of, and to safeguard, the integrity of the Company.

Such persons may include:

- employees;
- self-employed workers and collaborators;
- suppliers of goods or services;
- self-employed professionals and consultants;
- volunteers and trainees, including unpaid;
- individuals whose employment relationship has not yet commenced, during the probationary period, and after the termination of the employment relationship, provided that the information was obtained during that relationship or during the recruitment/selection process;
- shareholders and persons performing administrative, management, control, supervisory or representative functions, including where such functions are exercised on a *de facto* basis;
- trade union representatives, provided they act in a personal capacity and not as representatives of a trade union/employee category;
- 'facilitators', i.e. persons who assist the reporting person during the reporting process;
- persons linked to the reporting person by a stable relationship of affection or kinship;



- colleagues working within the same Department/work-related context as the reporting person.

1.5 Reporting channels

Legislative Decree no. 24/2023 provides for three reporting channels:

1. **Internal channel** (within the work-related context);
2. **External channel** (ANAC - National Anti-Corruption Authority);
3. **Public disclosure** (through the press, electronic means (e.g. the Internet, social media channels) and other means of dissemination capable of reaching a large number of persons).

1.6 Retention times for reports

Internal and external reports, and the related documentation, are retained for the time necessary to handle the report and, in any event, for no longer than 5 years from the date on which the final outcome of the reporting procedure is communicated, in compliance with the confidentiality obligations laid down in EU and national legislation on the protection of personal data.

2. INTERNAL REPORTING CHANNEL

The internal reporting channel was designed by the Company, after consulting the trade union organisations, with security measures suitable to ensure the confidentiality of the following information:

- the identity of the reporting person,
- the persons involved and, in any event, mentioned in the report,
- the content of the same and of the related documentation.

2.1 Recipients of reports submitted through Company's internal reporting channel

The recipient of reports is the person specifically appointed by the Company to collect and manage them in the most appropriate manner. At present, this role is performed by the **Supervisory Board**, in the person of **Vittorio Drovandi, lawyer**, who ensures the utmost confidentiality regarding the report, its subject matter and the identity of its author.

Reports may be submitted in any of the following ways, at the reporting person's discretion:

- a) by telephone, using the landline number **+39 010 5722272** or the mobile number **+39 338 1489476**;
- b) in writing, via internal mail or to the following address: **Carbofin SPA, Organismo di Vigilanza, Via G. D'Annunzio 2-108, 16121 Genoa**;
- c) by email to the following address, which is designed to ensure full confidentiality by allowing access only to the designated recipient: **organismo.vigilanza@carboflotta.it**;
- d) **through the dedicated electronic platform, accessible at the following web address: <https://digitalplatform.unione fiduciaria.it/whistleblowing/>**.¹ Platform's features are described

¹ The arrangements for using the platform will be explained through dedicated initiatives run by the IT Department. The report itself may also be preceded by a confidential telephone call with the person designated to receive it, with whom a subsequent face-to-face meeting may also be agreed, always in strict compliance with confidentiality requirements.



at the following link: <http://www.ufwhistleblowing.it/software/>.² The service also allows reports to be made in oral form.

- e) Via the Company's website, in the dedicated section, at the following link: <https://www.carboflotta.com/it/segnalazioni/>.

In this respect, the Supervisory Board (OdV) performs its tasks as a person authorised to process personal data, and its duties are set out in a specific document kept with Management.

2.2 Requirements for reports submitted through Company's internal reporting channel

Reports must be:

- strictly related to facts or conduct that occurred in the course of the reporting person's work activities, or in any event having a direct and unequivocal connection with their work activities;
- sufficiently detailed, i.e. containing, in addition to the elements **identifying** the unlawful act or the infringing conduct, also the elements that **enable it to be placed in time, specify the location**, indicate (where the reporting person has certain knowledge) **the persons present** or otherwise **involved** in, or aware of, the facts or conduct, and any other circumstances that may help to provide the most complete overall picture of the report;
- based on **precise and consistent factual elements**, of which the reporting person became aware by virtue of the functions performed within their work-related context.

It is reiterated that the reporting policy serves a positive purpose, in the common interest of all stakeholders, namely to prevent wrongdoing and to safeguard Company's reputation. The Company rejects any distorted interpretation that treats reports as a means of pursuing personal aims, unrelated to the purposes set out above.

The Company will apply the disciplinary measures provided for under the Internal Disciplinary System to any conduct inspired by such a misguided interpretation.

As already stated in the Preliminary Remarks, the methods, conditions and procedures for submitting reports must be:

- clear, visible and easily accessible to all potential recipients, including those who do not attend the workplace;
- published in a dedicated section on Company's website in order to ensure that all interested parties are made aware of them;
- made available to interested parties on a notice board within the workplace.

2.3 Procedural steps following an internal report:

Within 7 days of receipt, the recipient of the report must:

- issue an acknowledgement of receipt to the reporting person and, where necessary, request additional information;
- maintain contact with the reporting person and follow up the assessment of the report;
- provide the reporting person with appropriate feedback within a maximum of 90 days.

² The arrangements for using the platform will be explained through dedicated initiatives run by the IT Department. The report itself may also be preceded by a confidential telephone call with the person designated to receive it, with whom a subsequent face-to-face meeting may also be agreed, always in strict compliance with confidentiality requirements.



A report received by a person who is not competent to deal with it must be forwarded to the correct recipient within 7 days.

3. PROTECTIONS FOR THE REPORTING PERSON

Anti-discrimination and anti-retaliation protections apply where, at the time of reporting, the reporting person has reasonable grounds to believe that the information concerning the reported breaches, the publicly disclosed breaches or the breaches reported to the competent authorities is true and falls within the material scope of the Decree, and that the procedure set out in the Decree has been complied with.

The persons covered by the protections for reporting wrongdoing include anyone who, in any capacity, provides work or services for the Company, regardless of the nature of their activity and even in the absence of remuneration.

By way of example, in addition to the reporting person, this includes:

- ♦ persons who supported the reporting person during the reporting process (so-called 'facilitators'),
- ♦ other persons 'close' to the reporting person, such as colleagues and family members,
- ♦ employees or collaborators,
- ♦ employed and self-employed workers,
- ♦ self-employed professionals,
- ♦ volunteers and trainees, including unpaid,
- ♦ individuals involved in pre-contractual negotiations,
- ♦ persons during the probationary period,
- ♦ persons whose relationship with the organisation has ended (e.g. former employees, former consultants),
- ♦ shareholders,
- ♦ persons performing administrative, management, control, supervisory and representative functions.

For all such individuals, the Company ensures protection in three forms:

- a) protection of confidentiality;
- b) protection against retaliation;
- c) protection through statutory exemptions from liability.³

Additional protective measures include:

- the nullity of any waivers and settlements relating to the rights and protections provided for by the Decree;
- a general exemption (which excludes civil and administrative liability, as well as criminal liability) in favour of the person who, pursuant to Article 16, makes a report, files a complaint or makes a public disclosure of information covered by secrecy obligations, copyright, or protected under data

³ Protection must also be ensured where the employment relationship has not yet commenced, during the probationary period, or after the termination of the employment relationship, provided that the information concerned was obtained during the employment relationship itself or during the recruitment/selection process.



protection law, provided that, at the time of the disclosure, there were reasonable grounds to believe that such disclosure was necessary in order to report the breach;

- the exclusion of any other liability for the acquisition of, or access to, information on breaches, except where the conduct constitutes a criminal offence; this does not apply to conduct that is not strictly necessary to reveal the breach or that is, in any event, not connected with the report, complaint or public disclosure.

The burden of proof is reversed: retaliation is presumed to have occurred and any damage suffered is presumed to be a consequence of the report. The person who carried out the act or conduct bears the burden of proving that the acts and conduct were motivated by reasons unrelated to the report, complaint or public disclosure.

3.1 What is meant by 'retaliation'

"Any conduct, act or omission, including where merely attempted or threatened, carried out as a result of the report, a complaint to the judicial or accounting authority, or a public disclosure, which causes or may cause, directly or indirectly, unjustified harm to the reporting person or to the person who filed the complaint."

Examples of retaliatory conduct:

- dismissal;
- suspension from work;
- demotion;
- failure to promote;
- change of duties;
- change of workplace;
- salary reduction;
- change in working hours;
- suspension of training;
- negative performance assessments;
- the imposition of disciplinary measures or other sanctions, including financial penalties;
- coercion, intimidation, harassment and ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into an open-ended contract, where the worker had a legitimate expectation of such conversion;
- failure to renew, or early termination of, a fixed-term employment contract;
- harm, including to the person's reputation, particularly on social media;
- economic or financial detriment, including loss of economic opportunities and loss of income;
- revocation of a licence or permit;
- requiring a person to undergo psychiatric or medical examinations.
- ...

The assessment and handling of reports of retaliation fall within the remit of ANAC (National Anti-Corruption Authority).

4. EXTERNAL REPORTING CHANNEL

An external report may be made only where the reporting person,



- a) in their specific work-related context:
- does not have access to an active internal reporting channel;
 - has access to an internal reporting channel, but it does not comply with the applicable legal requirements;
 - has already made an internal report, but it has not been acknowledged, or it concluded with an unfavourable final decision;
- b) has reasonable grounds to believe that, if they were to submit an internal report, it would not be followed up effectively (for example, where the head of the Office/Department is involved in the reported breach);
- c) believes that making an internal report may expose them to a risk of retaliation;
- d) has reasonable grounds to believe that the reported breach may pose an imminent or manifest danger to the public interest.

As with internal reports, external reports can be submitted:

- a) in writing, via an electronic platform;
- b) orally, via telephone lines or voice messaging systems;
- c) by means of a face-to-face meeting, at the reporting person's request, to be arranged within a reasonable timeframe.

Reports submitted through the external reporting channel must be sent to ANAC (National Anti-Corruption Authority), as the sole authority competent to assess and handle them.

4.1 Role of ANAC

ANAC has activated an 'external reporting channel' which ensures confidentiality with regard to:

- the identity of the reporting person,
- the identity of the person concerned,
- the identity of any person mentioned in the report,
- the content of the report and of the related documentation.

Confidentiality is ensured also where reports are received through a channel other than the one established for that purpose, or by a person other than the one designated.

In addition, ANAC is responsible for:

- a) imposing sanctions on organisations that fail to comply with the obligations set out in the Decree;
- b) ensuring the proper functioning of the entire reporting process for the reporting person;
- c) providing the same confidentiality safeguards as those applicable to the internal reporting channel;
- d) handling notifications of retaliation.

4.1.1 ANAC agreements with third-sector entities

In order to provide reporting persons with additional support measures, ANAC has entered into agreements with third-sector entities and makes the relevant updated list available.



The support measures, provided free of charge, consist of information, assistance and advice on reporting procedures and on the protection against retaliation offered by national law and EU law; on the rights of the person concerned; and on the procedures and conditions for accessing State-funded legal aid.

5. PUBLIC DISCLOSURE

A further reporting method (***intended to be used only as a last resort***) is 'public disclosure', through the press, electronic means or other means of dissemination capable of reaching a large number of people.

As with external reports, the conditions are set out under which the reporting person may use this method and benefit from the same protection measures provided for by Legislative Decree no. 24/2023 as those available when using the internal/external reporting channel, namely where:

- the reporting person has previously made an internal report and an external report, or has made an external report directly, and no feedback has been provided within the prescribed time limits as to the measures planned or taken to follow up the reports;
- the reporting person has reasonable grounds to believe that the breach may pose an imminent or obvious danger to the public interest;
- the reporting person has reasonable grounds to believe that making an external report may expose them to a risk of retaliation or may not be followed up effectively due to the specific circumstances of the case, for example where evidence may be concealed or destroyed, or where there are reasonable grounds to fear that the person who received the report may be colluding with the author of the breach or may be involved in the breach itself.

In addition, it is possible to make a report by way of public disclosure where making an external report may:

- expose the reporting person to a risk of retaliation;
- not be followed up effectively due to the specific circumstances of the specific case (*for example where evidence may be concealed or destroyed, or where there are reasonable grounds to fear that the person who received the report may be colluding with the author of the breach or may be involved in the breach itself*).

6. PERSONAL DATA PROCESSING

Throughout the process described by Legislative Decree no. 24/2023, any processing of personal data must take into account and comply with the obligations laid down by applicable law.

In particular, the entire procedure must be **GDPR-compliant** from the outset ("**data protection by design**"), in the following phases:

- design,
- setting up the arrangements for receiving and handling internal reports,
- relations with suppliers,
- communications between the various parties involved,
- privacy information notices to be provided to all interested parties,
- interested parties' rights,
- risk analysis covering all parties involved (*reporting persons, reported persons, third parties*),

CARBOFIN S.p.A.

CAPITALE SOCIALE € 20.100.000 I.V.

R.E.A. GENOVA N° 232544
CODICE FISCALE ED ISCRIZIONE REGISTRO IMPRESE DI GENOVA N° 00103850822
PARTITA I.V.A N° 03796990103
WWW.CARBOFLOTTA.COM



- adoption of appropriate technical and organisational measures to safeguard the rights and freedoms of interested parties,
- level of protection and security appropriate to the likelihood and severity of the risks identified.

Therefore, all documentation relating to each individual report, whether in paper or electronic format, will be filed and retained in an appropriate manner for the period necessary to properly comply with the obligations under Legislative Decree no. 24/2023, while meeting the requirements of Regulation (EU) 2016/679 (GDPR).

SANCTIONS

Without prejudice to any other forms of liability, ANAC applies the following administrative pecuniary sanctions to the person responsible for the breach; such sanctions must be effective, proportionate and dissuasive:

a) EUR 10,000 to EUR 50,000, where it finds that:

- retaliation has occurred;
- reporting has been obstructed;
- an attempt has been made to obstruct reporting, or the confidentiality obligation has been breached;
- reporting channels have not been established;
- no procedures have been adopted for making and handling reports;
- the adopted/implemented procedures are not compliant with applicable law.

b) EUR 500 to EUR 2,500, where it finds:

- a breach of the confidentiality obligation regarding the identity of the reporting person;
- the criminal liability of the reporting person for the offences of defamation or false accusation.

The whistleblowing platform can be accessed at the following address using a standard web browser:
<https://digitalplatform.unione fiduciaria.it/whistleblowing/>.

Once the website has loaded, enter the token CARBOFINWB and click '*Collegati*' (Connect) to access the guided reporting procedure dedicated to our Company. Please follow the field labels and the information notes carefully before proceeding on each screen or closing the browser.

