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

Genoa, 14 July 2023

COMMUNICATION TO ALL STAFF

The new Whistleblowing discipline (Legislative Decree n. 24/2023)

INTRODUCTION

This **COMMUNICATION**:

- replaces the communication of *July 23rd 2019* concerning "Reporting of wrongdoing or violations in the work activity";
- illustrates to all staff the regulatory innovations introduced by Decree 24/2023 on the subject of Whistleblowing;
- is made available to all recipients on the Company's website and posted on notice boards for easy access.

1. LEGISLATIVE DECREE 24/2023 (THE NEW WHISTLEBLOWING DISCIPLINE)

The Legislative Decree 24/2023 (hereinafter also "the Decree"), of implementation of EU Directive 1937/2019, in force since March 30, 2023):

- it brings together in a single regulatory text **the discipline of the reporting channels and the protections granted to those who report violations** of national or European Union regulatory provisions, which harm the interest or the integrity of the Company and of which they have come to know knowledge in their work environment;
- it makes it mandatory for public bodies and businesses to set up reporting channels (**Whistleblowing**);
- it contains provisions concerning the protection of persons who report violations of national regulatory provisions.

1.1 Application date of the new regulation

In compliance with the times established by the Decree for companies with more than 249 employees and equipped with the Organization and Management Model pursuant to Legislative Decree 231/2001 (Administrative responsibility of the entities), **Carbofin S.p.A.** (hereinafter also **"The Company"**) applies the provisions of the new regulations starting from **15 July 2023**.

1.2 Subject of the reports

Behaviors, acts, omissions and information (for which the whistleblower has grounds, suspicions supported by concrete elements) that can materialize:

- actual or potential violations of European legislation, national legislation, company regulations;
- information about violations that may be committed;
- conduct aimed at concealing such violations;
- violations of ethical principles and standards to which the Company voluntarily adheres;

- negligence, too, but not necessarily criminal, which directly affects national or community strategic interests (for example, privacy, environment, tax crimes);

In particular, conduct, acts or omissions regarding:

- administrative and accounting, civil or criminal offences;
- significant illegal conduct pursuant to Legislative Decree 231/2001 or violations of the **Company's Organization and Management Model**;
- offenses falling within the scope of European Union or national regulations, relating to the following sectors: prevention of money laundering and terrorist financing; transport safety; environmental Protection; privacy protection and personal data protection; security of networks and information systems**;**
- acts or omissions affecting the financial interests of the Union;
- acts or omissions relating to the internal market;
- acts or behaviors that frustrate the object or purpose of the provisions referred to in the Union acts.

Disputes, claims or requests related to the personal interest of the whistleblower or to accounting aspects that pertain exclusively to his work or employment relationships with the Company are excluded from the scope of application of the new regulation;

Anonymous reports are accepted only if they are adequately detailed and capable of bringing out specific facts and situations. They will be taken into consideration only if they do not appear irrelevant, unfounded or unsubstantiated.

1.3 Form of notifications

Reports can be submitted:

a) in written form, even electronically,

b) orally through telephone lines or voice messaging systems;

c) through a direct meeting, at the request of the whistleblower, to be held within a reasonable time.

1.4 Subjects entitled to make reports

All those who, providing services for the Company in any capacity, even without payment, are witnesses or come to direct knowledge, in their workplace, of crimes or irregularities and intend to report them in the interest and for the integrity of the Company.

Such subjects can be:

- subordinate workers;
- self-employed workers and collaborators;
- suppliers of goods or services;
- freelancers and consultants;
- volunteers and trainees, even unpaid;
- subjects for whom the employment relationship has not yet begun, during the probationary period and after the termination of the relationship, provided that the information was acquired during the relationship itself or during the selection process;
- shareholders and persons with administrative, management, control, supervisory or representative functions, even where these roles are exercised only on a de facto basis;

- Trade union representatives provided that they are in a personal capacity and not as a category representative.
- “facilitators”, i.e. people who assist the whistleblower in the reporting process;
- persons linked to the whistleblower by a stable emotional or kinship bond;
- co-workers who work within the same Department/work context as the whistleblower.

1.5 Reporting channels

Decree 24/2023 provides for three reporting channels:

1. **Internal Channel** (within the working context);
2. **External channel** (ANAC- National Anti-Corruption Authority);
3. **Public Disclosure** (through the press, IT means (e.g. internet, social channels), means of diffusion capable of reaching a large number of people).

1.6 Report retention times

Internal and external reports and the related documentation are kept for the time necessary to process the report and in any case no later than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations pursuant to the legislation European and national legislation on the protection of personal data.

2. INTERNAL REPORTING CHANNEL

It was designed by the Company, having consulted with the trade unions, with security measures to guarantee confidentiality:

- of the identity of the whistleblower,
- of the people involved and in any case mentioned in the report,
- of the content of the same and of the relative documentation.

2.1 Recipients of reports made through the internal Carbofin S.p.A channel

The recipient of the reports is the subject specifically designated by the Company to carry out the collection and management of the same in the most suitable way, currently constituted by the **Supervisory and Control Body**, in the person of the lawyer **Vittorio Drovandi**, who guarantees the utmost rigorous confidentiality on the report, on the subject of the report and on the identity of its author.

However, it is not excluded that the recipient of the report could also be an external, autonomous subject, equipped, where present, with specifically trained personnel, or a third party (e.g. Legal, Consultant, etc.).

Reports may be sent in the following ways, at the option of the reporting party:

a) through telephone contact to the landline number **+39 010 5722272** or mobile phone **+39 338 1489476;**

b) in writing by internal mail or to the following address: **CARBOFIN S.p.A., Organismo di Vigilanza, Via G. D’Annunzio 2-108, 16121 Genova**;

c) by email to the following address, which is designed to guarantee total confidentiality by allowing access only to its owner: **organismo.vigilanza@carboflotta.it;**

d) [1]**through the specially prepared IT platform, which can be accessed via the following web address: https://digitalplatform.unionefiduciaria.it/whistleblowing/**
the characteristics of which are indicated at the following link:
http://www.ufwhistleblowing.it/software/

[1] The methods of using the platform have been communicated and illustrated with specific initiatives, including the IT Department e-mail dated 17.6.2019 (see attachment).

The report may also be preceded by a confidential telephone contact with the person destined to receive it, with which a subsequent contact in person may also be agreed upon, always in compliance with the strictest confidentiality.

2.2 Requirements for reports made through the Carbofin S.p.A internal channel

Reports must be:

- strictly referring to facts or behaviors that took place in the performance of the whistleblower's work activity, or in any case having a direct and unequivocal connection with his work activity;
- detailed, i.e. contain, in addition to the elements that **identify** the unlawful act or the infringing behaviour, also those that **allow its placement in time**, **define its place**, indicate (in the case of certain knowledge) **the people present** or in any case **involved** or knowledge of the fact or behavior and all other circumstances that can make up the overall picture of the report in the most complete way.
- based on **precise and concordant factual elements**, of which the whistleblower has become aware due to the functions performed in his/her workplace.

It is reiterated that the reporting regime has the positive aim of common interest for all stakeholders to prevent the commission of offenses and protect the reputation of the Company, which rejects any distorted interpretation, tending to conceive reports aimed at pursuing personal ends and disconnected from purposes indicated above.

The Company will pursue the sanctioning interventions envisaged by the Internal Disciplinary System, any conduct based on this distorted conception.

As already indicated in the Introduction, the methods, conditions and procedures for making reports must be:

- clear, visible and easily accessible to all possible recipients, even those who do not frequent the workplace.
- published in a dedicated section on the company's website in order to ensure that all interested parties are aware of it;
- made available to interested parties on a bulletin board within the workplace.

2.3 Procedural process following the internal reporting :

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

- issue an acknowledgment of receipt to the whistleblower and, where necessary, request additions;
- maintain the relationship with the interlocutor and follow up on the assessment of the report;
- provide, within a maximum of 90 days, adequate feedback to the whistleblower.

The report received by an incompetent subject must be forwarded to the correct recipient within 7 days.

3. PROTECTIONS OF THE REPORTER

The anti-discrimination and anti-retaliation protections apply if, at the time of reporting, the whistleblower has reasonable grounds to believe that the information on the violations reported, publicly disclosed or denounced are true, fall within the objective scope and the procedure defined by the Decree has been complied with.

The subjects involved in the protection for the reporting of offenses are those who, for whatever reason, provide services to the Company, regardless of the nature of their activity and even in the absence of consideration.

By way of example, in addition to the whistleblower::

- individuals who have supported the whistleblower in the reporting process, the so-called "facilitators"
- additional figures "close" to the whistleblower, such as colleagues and family members
- employees or collaborators
- subordinate and self-employed workers
- freelancers
- volunteers and trainees, even unpaid,
- subjects in the pre-contractual negotiation phase
- probationary persons
- persons whose relationship with the entity has ceased (e.g. former employees, former consultants)
- shareholders
- persons with administrative, management, control, supervision and representation functions.

For all these subjects, protection is guaranteed by the Company in the threefold form of:

a) privacy protection,
b) protection against retaliation
c) protection in anticipation of causes of exclusion of liability[1].

<u>Additional protective measures should be indicated:</u>

- the nullity of any waivers and transactions relating to the rights and protections provided for by the decree;
- a general exemption (which also excludes civil and administrative liability, in addition to criminal liability) in favor of the subject who carries out (pursuant to article 16) the reporting, denunciation or public disclosure of information covered by secrecy, copyright or protected by data protection regulations, provided that at the time of disclosure there were reasonable grounds to deem it necessary to report the violation;
- the exclusion of any other responsibility for the acquisition or access to information on violations, except in the hypothesis in which the conduct constitutes a crime, with the exclusion of conduct not strictly necessary to reveal the violation or, in any case, not connected to the reporting, reporting or public disclosure.

[1] Protection must also be ensured when the employment relationship has not yet begun, during the probationary period or after the termination of the relationship provided that the information was acquired during the relationship itself or during the selection process.

Furthermore, as already in the previous regulation, the reversal of the burden of proof is foreseen: retaliation is presumed to have taken place and any damage suffered is a consequence of the report and is charged to the person who carried out the deed or the behavior the burden of proving that conduct and acts had been motivated by reasons unrelated to reporting or disclosure or denunciation.

3.1 What is meant by retaliation

"Any behaviour, act or omission, even if only attempted or threatened, put in place as a result of the report, the complaint to the judicial or accounting authority, or the public disclosure and which causes or may cause, the reporting person or the person who has filed a complaint, directly or indirectly, of unjust damage, to be understood as unjustified damage".

Examples of retaliatory behavior:

- dismissal;
- suspension from work;
- demotion of rank;
- lack of promotion;
- change of functions;
- change of place of work;
- salary reduction,modifica dell'orario di lavoro;
- suspension of training;
- negative merit notes;
- adoption of disciplinary measures or other sanctions, including financial ones;
- coercion, intimidation, harassment and ostracism;
- discrimination or otherwise unfavorable treatment;
- failure to convert a fixed-term employment contract into an open-ended employment contract, where the worker has a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media;
- economic or financial prejudices, including loss of economic opportunity and loss of income;
- cancellation of a license or permit;
- request for submission to psychiatric or medical tests;
- …

Evaluation and management of retaliatory communications are the responsibility of ANAC (National Anti-Corruption Authority).

4. EXTERNAL SIGNALING CHANNEL

External reporting can only be activated if the whistleblower:

a) in its specific working context:

- does not have an active internal signaling channel available
- the channel is active, but does not comply with the regulatory requirements;

b) has already made an internal report, but the report was not answered or ended with a negative final provision;

c) has reasonable grounds to believe that, if it were to make an internal report, it would not be followed up effectively *(for example in the event that the head of the Office/Department is involved in the violation); ;*

d) reporting may involve the risk of retaliation;

e) has reasonable grounds to believe that the reported violation may constitute an imminent or manifest danger to the public interest.

As with internal reporting, external reporting can be made:

a) in written form via an IT platform ,
b) in oral form through telephone lines or voice messaging systems,
c) through a direct meeting set within a reasonable time, at the request of the whistleblower.

Reports made through the external channel must be sent to the ANAC (National Anti-Corruption Authority) as the only body responsible for their assessment and management.

4.1 The role of the ANAC

The ANAC (which on 30 June 2023 published its Guidelines on the matter, for the purpose, in particular, of providing indications on the application of law 179/2017[2]) has activated an "external reporting channel" which guarantees the confidentiality about:

- the identity of the whistleblower,
- the identity of the person involved,
- the identity of the person mentioned in the report,
- the content of the report and related documentation.

The guarantee of confidentiality is also ensured in the event that the reports arrive through a channel other than the one set up, as well as to a person other than the designated one.

Furthermore, it is up to the ANAC :

a) the power to sanction entities that fail to comply with the obligations of the Decree;
b) allow the correct functioning of the entire reporting process by the *whistleblower*;
c) offer the same confidentiality guarantees provided for the internal reporting channel;
d) handle communications of retaliation.

4.1.1 ANAC agreements with third sector entities

To provide whistleblowers with additional support measures, Anac has entered into agreements with third sector entities, of which it makes the updated list available.

[2] Law 179/2017 on Whistleblowing, for the protection of public and private employees, approved on 11/15/2017, provides that "at least one alternative reporting channel suitable for guaranteeing, using IT methods, the confidentiality of the whistleblower's identity".

The support measures provided free of charge consist of information, assistance and advice on how to report and on the protection from retaliation offered by national and European Union legal provisions, on the rights of the person involved, as well as on the methods and conditions of access sponsorship at the expense of the State.

5. PUBLIC DISCLOSURE

Another way to report (**hopefully residual**) is "public disclosure", whether in print, electronic media or dissemination media capable of reaching a large number of people.

As for external reports, the conditions are defined in the event of which the whistleblower can use this method and benefit from the same protection measures granted by the Decree for the use of the internal/external channel:

- the reporting person has previously made an internal and external report or has made an external report directly and no response has been given within the established deadlines regarding the measures envisaged or adopted to follow up on the reports;
- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the reporting person has reasonable grounds to believe that the external reporting may involve the risk of retaliation or may not be followed up effectively due to the specific circumstances of the concrete case, such as those in which evidence may be hidden or destroyed or in which there is well-founded fear that whoever received the report may be colluded with the author of the violation or involved in the violation.

In addition, a report may be made through public disclosure when external reporting can:

- involve the risk of retaliation;
- not have an effective follow-up due to the specific circumstances of the concrete case *(e.g. in the event that the evidence of the violation can be concealed or destroyed, or in which there is a well-founded fear that the person who received the report could be colluding with the perpetrator of the violation or involved in the violation).*

The whistleblower will benefit from the same protection measures granted by the Decree for the use of the internal/external channel, only if,

6. PROCESSING OF PERSONAL DATA

In the entire process described by Legislative Decree 24/2023, any processing of personal data must take into account and comply with the obligations established by the GDPR or Legislative Decree 51/2018[3].

In particular, the entire procedure must be *compliant* from the outset ("**Data Protection by Design**") with the provisions of the GDPR, in the phases of:

- planning,
- fine-tuning of the procedures for receiving and managing internal reports,
- relationships with suppliers,
- communications between the various parties involved,
- information to be provided to all interested parties,
- rights of data subjects,
- risk analysis concerning all the figures involved (*whistleblowers*, reported persons, third parties),
- adoption of technical and organizational measures suitable to guarantee the protection of the rights and freedoms of the interested parties,
- level of protection and security appropriate to the probability and severity of the risks identified.

Furthermore, the art. 13 of Decree 24/2023 expressly prescribes the obligation, for all subjects required to define the internal reporting channel, to carry out, before starting the treatment already in the planning phase of the organizational design, the impact assessment on data protection (DPIA) required by Article 35 of the GDPR.

In short, in order to activate the internal reporting channel, the Company is required to:

- design the treatment, aligning each operation, right from the design, with the principles of protection of personal data established by art. 5 of the GDPR and by art. 3 of Legislative Decree 51/2018 (Principles applicable to the processing of personal data);
- define the roles of responsibility starting from the indication of the Data Controller ~~(Data Controller)~~ and, in the presence of co-ownership (if the channel and its management are shared between several companies) of the Joint Controller, of the internal Data Processors, determining their respective areas and responsibility;
- perform the DPIA (Data Protection Impact Assesment);
- train and authorize the subjects called to manage the reporting channel for processing;
- inform all interested parties;
- designate and contract in written form, the Data Processor Outsourcers (External Data Processing Managers) called to carry out the processing on behalf of the company, provide instructions to

[3] Decree 51/2018 regulates the processing of personal data for the purpose of preventing and repressing crimes, executing criminal sanctions, safeguarding against threats to public safety and preventing them, by both the judicial authority and the police forces.

them and make sure that they adopt suitable security measures and provide guarantees of compliance with the GDPR, as required by art. 28 of the Regulation.

7. SANCTIONS

Without prejudice to the other profiles of responsibility, the ANAC applies the following pecuniary administrative sanctions to the person responsible for the violation, which must be effective, proportionate and dissuasive:

a) **from 10.000 to 50.000 euros** when it is ascertained that:

- reprisals have been committed
- reporting was blocked,
- an attempt has been made to obstruct it or that the obligation of confidentiality has been violated;
- no reporting channels have been established;
- no procedures have been adopted for making and managing reports,
- the adoption or implementation of the procedures do not comply with the law.

b) **From 500 to 2.500 euros,** when it is ascertained that**:**

- the violation of the obligation of confidentiality regarding the identity of the whistleblower.
- the criminal liability of the whistleblower for the crimes of defamation or slander.

In compliance with the provisions of the Decree, Carbofin S.p.A. implements and highlights, in its Internal Disciplinary System, the sanctions expressly intended for those who are recognized.

The Whistleblowing platform can be reached at the following address, using a common browser:

https://digitalplatform.unionefiduciaria.it/whistleblowing/

Once the site has loaded, it will be necessary to enter the CARBOFINWB token and click on "Connect" to reach the reporting wizard dedicated to our company.

Scrupulously follow the wording of the fields and the information notes before proceeding to each screen or closing the browser.