

# Whistleblowing

## Whistleblowing Procedure

### 1 – SCOPE OF APPLICATION

This Whistleblowing Procedure (hereinafter “Procedure”) applies to Bn&a Buzzi, Notaro & Antonielli d’Oulx and is addressed, in particular, to the following recipients:

- corporate top management and members of corporate bodies;
- shareholders;
- company employees and collaborators (by way of example only: interns, trainees, agency workers, etc.), including during a trial period or after termination;
- business partners, clients, suppliers, consultants, partners and, more generally, anyone who is in a relationship of interest with the company (hereinafter collectively “Recipients”).

### 2 – INFORMATION NOTICE

Law 179/2017, Legislative Decree 231/2001 and Legislative Decree 24/2023, provide for the adoption of an IT tool within Public and Private Organizations, through which employees, collaborators and all subjects identified by regulations as possible Whistleblowers, report, to specific individuals or bodies (including police forces and public authorities) a possible fraud, crime, unlawful act or any irregular conduct committed by other persons belonging to the organization.

The objective of the European directive is to establish common minimum standards to ensure a high level of protection for persons reporting violations of Union law, creating secure communication channels both within an organization and externally. In specific cases, the possibility is provided of making the report through public disclosure via the media.

The new discipline applies to violations of national and European Union regulatory provisions that harm the public interest or the integrity of the public administration or the private entity, of which the reporting persons became aware in a public or private work context.

This Procedure also aims to regulate the process of receiving, analyzing and handling reports, sent or transmitted by anyone, even anonymously, and describes the communication channels established through which reports can be made pursuant to this Procedure.

Whistleblowing is to be considered a fundamental tool to combat possible unlawful acts and to spread among employees a culture of ethics and legality within organizations, to create a climate of transparency and a sense of participation and belonging.

### 3 – PROCEDURE

All Recipients of this Procedure are required to report potential unlawful activities that may violate the law, the Code of Ethics or the policies of Bn&a Buzzi, Notaro & Antonielli d’Oulx.

Reporting of possible violations is encouraged, to allow the company to investigate the matter and adopt the necessary corrective measures. Such measures allow Bn&a Buzzi, Notaro & Antonielli d'Oulx to reduce any risks or damages for the individual employee, colleagues, the company itself or the communities in which it operates.

To this end, anyone wishing to make a report can, at their own choice and discretion, use the communication channel accessible through connection to the GRC CORA WHISTLEBLOWING portal, which allows reports to be made anonymously or by name.

The reporting person can obviously also use other external reporting channels provided this is done in compliance with the law.

## 4 – FORMS OF PROTECTION

Bn&a Buzzi, Notaro & Antonielli d'Oulx has provided for the assignment of report management to specifically designated responsible figures. Such figures, as report investigators, have been duly authorized and appointed for the processing of personal data and trained accordingly.

During the course of the checks, other persons internal to the company may be involved to request information or opinions but will remain absolutely extraneous to the details of the report and to any element that could lead to the identification of the reporting person.

The portal allows:

- separating the identifying data of the reporting person from the content of the report, providing for the adoption of substitute codes for identifying data, so that the report can be processed anonymously and make possible the subsequent reconstruction of the identity of the reporting person only in permitted cases;
- managing reports transparently through a defined procedural process communicated externally with certain deadlines for the start and conclusion of the investigation;
- keeping, as far as possible, the content of the reports confidential during the entire report management phase;
- adopting secure protocols for data transport over the network as well as the use of encryption tools for the content of reports and any attached documentation;
- adopting adequate methods for the storage of data and documentation (physical, logical, hybrid);
- adopting confidentiality protection policies through IT tools (decoupling of the reporting person's data from information relating to the report, encryption of data and attached documents);
- adopting data access policies (officials authorized to access, IT system administrators);
- allowing the reporting person, through appropriate IT tools, to verify the progress of the investigation;
- does not allow tracing back to the identity of the reporting person except in any disciplinary proceedings against the reported person: this is due to the fact that the identity of the reporting person cannot be revealed without their consent, unless knowledge thereof is absolutely indispensable for the defense of the accused as provided by Art. 54-bis, paragraph 2, of Legislative Decree 165/2001;
- implements audit procedures for system access, the consultation of which must be reserved exclusively to persons entitled thereto;
- having functionalities compliant with the ANAC software model;

- possibility of entering personal identification data even after sending the report;
- having HTTP Link Referrer Privacy: in order to guarantee user privacy, appropriate countermeasures have been taken for access to external resources from within the platform, integrating behaviors that obscure the application Referrer;
- having advanced security Headers: all requests are handled with the aid of advanced headers for application security, such as Strict-Transport-Security and X-Content-Security-Policy.

The GRC CORA Whistleblowing platform is a Web-Based application accessible from any PC and Mobile device (tablet, smartphone). The platform allows the completion, sending and receiving of reports as well as the possibility of dialoguing with the investigator anonymously.

Bn&a Buzzi, Notaro & Antonielli d'Oulx ensures the confidentiality of the reporting person's identity, prohibits any form of retaliation or discrimination against anyone who has made a report and against third parties connected to the reporting person, and adopts measures aimed at protecting the rights of the reported persons.

Persons involved in any capacity in the management of reports are required, within the limits provided by law, to maintain confidentiality regarding the existence and content of the report and the activity carried out in this regard, and guarantee confidentiality regarding the identity of the reporting person, the reported person and other persons involved in accordance with applicable regulations.

## PLATFORM SECURITY

With regard to *Cyber Security* aspects, GRC CORA Whistleblowing is periodically subject to *Application Security Assessment* (ISO 27001, OWASP) of the Systems in pre-production and production environments.

The main security features of the platform are listed below:

- **Data Retention Policy:** Each report stored in the Database increases the attractiveness for potential Hackers. Reports have a validity date that can be extended by the *Receiver*; an expired report is removed along with all its data;
- **Server Resiliency:** The Server is configured to render D/DOS type attacks harmless. Massive requests coming from the same IP address that could constitute an attack are automatically blocked;
- **Web content security:** Communication between front end and back end uses internationally shared best practices, including security headers and encryption of communication with TLS 1.3;
- **File Encryption:** A receiver can use their own PGP key, if they have one. Each file is saved on disk using a random symmetric AES key, the key is saved on ramdisk;
- **GDPR:** The Whistleblowing Platform complies with the general data protection regulation (GDPR – General Data Protection Regulation, EU Regulation 2016/679).

## 5 – WHAT TO REPORT

Reports concern facts (of any nature, including merely omissive ones), already occurred or very likely to occur, attributable to Persons of the company Bn&a Buzzi, Notaro & Antonielli d'Oulx or to Third Parties that may constitute unlawful acts, irregularities or conduct otherwise carried out in violation of:

- administrative, accounting, civil or criminal offenses;
- unlawful conduct relevant pursuant to Legislative Decree 231/2001, or violations of the organization and management models provided therein;

- unlawful acts falling within the scope of application of European Union or national acts relating to the following sectors: public procurement; financial services, products and 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 protection and security of networks and information systems;
- acts or omissions that harm the Union's financial interests;
- acts or omissions relating to the internal market;
- acts or conduct that defeat the object or purpose of the provisions of Union acts.

Reports must concern facts of which the reporting person has direct knowledge, the reporting person having well-founded reasons to believe that the reported information is true at the time of the communication.

Reports must be made promptly with respect to knowledge of the facts so as to make verification concretely possible.

Communications, complaints, claims, and requests concerning matters other than those of the reports are excluded. Reports must not concern grievances of a personal nature.

## 6 – WHY SHOULD YOU MAKE A REPORT?

Reports made in good faith and in the interest of the common good can make it possible to identify in time and remedy irregular or unlawful conduct that may harm the company.

## 7 – VIOLATION OF THIS PROCEDURE AND LIABILITY OF THE REPORTING PERSON

Employees who violate this Procedure will be subject to disciplinary proceedings. For other Recipients other than employees, violation of this Procedure may give rise to contractual and non-contractual liability.

Slandorous or defamatory reports are prohibited and sanctioned according to law. Any forms of abuse of this procedure, such as manifestly unfounded, opportunistic reports and/or reports made for the sole purpose of harming the reported person or other persons, and any other case of improper use or intentional exploitation of the institution that is the subject of this procedure, may also give rise to disciplinary liability.

## 8 – CONTENT OF THE REPORT

The reporting person must provide all the elements useful to allow the necessary and appropriate checks and verifications to be carried out to confirm the validity of the facts subject to the report.

For this purpose, the report should preferably contain the following elements:

1. capacity of the person making the report;
2. description of the facts subject to the report, indicating, if known, the circumstances of time and place in which they were committed;
3. personal details or other elements that allow identification of the person(s) who carried out the reported facts;
4. indication of any other persons who may report on the facts subject to the report;

5. any persons aware of the facts;
6. attach any documents or multimedia files useful to the facts;
7. any other information that may provide a useful confirmation regarding the existence of the reported facts.

## 9 – TRANSMISSION OF THE REPORT

---

In order to allow the reporting person to proceed with the report in a timely manner, Buzzi, Notaro & Antonielli d'Oulx has made available on its website a dedicated GRC CORA Whistleblowing portal accessible at the following web address: **whistleblowing**. After accessing the Portal, the reporting person will be guided through the completion of a questionnaire consisting of open and/or closed questions that will allow them to provide the elements characterizing the report (facts, time context, economic dimensions, etc.)

The reporting person may or may not provide their identity. In any case, the reporting person may provide their personal details at a later time, again through the Portal.

In order to prevent identification of the reporting person, access to the Portal is subject to a “no-log” policy: this means that the company’s IT systems are not able to identify the point of access to the Portal (IP address) even if access is made from a computer connected to the company network.

At the time the report is sent, the Portal will issue the reporting person a unique 16-digit identification code (KEY CODE). This code, known only to the reporting person, cannot be recovered in any way if lost. The KEY CODE will be used by the reporting person to access, again through the Portal, their own report in order to:

- monitor its progress;
- request further information through the chat;
- provide their personal details;
- respond to any follow-up questions.

This KEY CODE must absolutely not be lost.

In addition, reports can be made through the following channels, although these are not preferred:

- direct meeting with an investigator, the meeting will be recorded in writing and signed.

## 10 – MANAGEMENT OF THE REPORT

---

Reports transmitted through the Portal are received by the investigator who manages the reports and who proceeds to carry out the checks in compliance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate. In particular, reports are subject to the following investigative procedure:

- notify the reporting person of receipt of the report within 7 days from the date of its receipt;
- maintain communications with the reporting person and request from them, if necessary, additional information;
- diligently follow up on reports received;
- carry out the investigation necessary to follow up on the report, including through hearings and acquisition of documents;

- provide feedback to the reporting person within 3 months or, if justified and reasoned grounds exist, 6 months from the date of the notice of receipt of the external report or, in the absence of such notice, from the expiry of 7 days from receipt;
- communicate to the reporting person the final outcome of the report.

## 11 – RETENTION OF THE REPORT AND PRIVACY

Internal and external reports and the related documentation are retained for the time necessary to process the report and in any case not beyond 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations under European and national regulations on the protection of personal data.

**SEND A REPORT →**

<https://wb.media-form.it:8443/t/cedef5a5-e588-42ed-b407-84254401e7c9/#/>