



# LEGAL NOTES ON HOW TO MAKE A REPORT AND PRIVACY POLICY

## 1 WHAT DOES WHISTLEBLOWING/REPORT MEAN?

The term "whistleblowing" refers to the **spontaneous disclosure** by an individual, known as the "whistleblower", of an offence committed within the company, of which he or she has been a witness while performing his/her tasks. This disclosure is made through a "**Report**", to be made and managed in accordance with current regulations (Legislative Decree 24/2023 transposing EU Directive 2109/1937). The purpose of the regulations is to combat and prosecute illegal episodes in general, by implementing channels aimed at making them emerge and protecting the Whistleblower at the same time.

## 2 WHO CAN REPORT AND WHAT CAN BE REPORTED?

Different categories of individuals can make a **Report**:

- In-company individuals (e.g., employees, collaborators, interns, volunteers, shareholders, administrators, board members, etc.);
- Individuals outside the company who have a relationship/contact with [Decover srl](#) (e.g., customers, suppliers, consultants, etc.).

In general, **any incident that may constitute a violation of national or Community law** (illegal incident) or a violation of company codes/regulations, which has been witnessed at the company or of which there is direct knowledge, can be reported. No reports can be made concerning complaints/grievances of a personal nature.

## 3 WHAT ARE THE WHISTLEBLOWER'S PROTECTIONS AND RESPONSIBILITIES?

| PROTECTIONS FOR THE WHISTLEBLOWER   | LIABILITY OF THE WHISTLEBLOWER  |
|---|---|
| <ul style="list-style-type: none"><li>• The identity of the whistleblower is kept confidential and known only by the Platform Manager and the SB, except in cases expressly provided for by law (e.g., criminal investigation)</li><li>• No form of retaliation or discriminatory measure, direct or indirect, affecting the working conditions for reasons related to the report, is allowed or tolerated against the whistleblower.</li></ul> | <ul style="list-style-type: none"><li>• The report must be made promptly with respect to the knowledge of the facts, in order to make the verification concretely possible.</li><li>• The reporting party is responsible for the veracity of the contents of the report (no content can be entered based on gossip or suspicion).</li></ul> |

The legislation is without prejudice to the **criminal and disciplinary liability of the whistleblower**, in the event of slanderous or defamatory reporting, pursuant to the Criminal Code and Art. 2043 of the Italian Civil Code. Any forms of abuse, such as manifestly opportunistic reports and/or reports made for the sole purpose of harming the defendant or other individuals, and any other hypothesis of improper use or intentional instrumentalization, are also a source of responsibility, in the disciplinary and other competent forums.

## 4 WHAT ARE THE COMPANY'S OBLIGATIONS?

- Decover, falling within the parameters of application of the regulations, is required to activate a channel for reports, which meets certain security and confidentiality requirements for any information entered.
- Decover is required to define, train and make known the persons in charge of managing reports and any related investigations.
- For each report, Decover is required to carry out an **assessment of the validity** of the contents entered, on the basis of which any further investigation shall be provided for, by means of checks, investigations, complaints to Supervisory Bodies/judicial authorities/ law enforcement agencies.
- Decover is required to provide adequate feedback to the Reporting Party regarding the evolution of the assessments/investigations on the report made.
- Lastly, Decover is required to ensure the processing of any personal data contained in the report, in accordance with current regulations on privacy (EU Regulation 2016/679 "GDPR" and Legislative Decree 196/2003, as amended by Legislative Decree 101/2018.)

## 5 WHO ARE THE PARTIES RESPONSIBLE FOR MANAGING THE REPORTS?

Decover has opted for a fully outsourced solution (platform and manager), which guarantees the appropriate skills and adequate protection tools, entrusting the position of Platform Manager to the company:



# LEGAL NOTES ON HOW TO MAKE A REPORT AND PRIVACY POLICY

Galli Data Service Srl – Strada della Viggiioletta, 8 – 29121 Piacenza – VAT no.: 01690860331 (company with many years of exclusive competence in the field of compliance processes, regulatory adjustments, privacy and data protection).

According to the regulatory requirements, the management of the reports is entrusted to the **Supervisory Body**, established pursuant to Legislative Decree 231/01. The aforementioned individuals are the only ones authorized to access the contents of the reports, and must guarantee the maximum security and confidentiality, with particular reference to the identity of the reporting party, which can be communicated exclusively within the framework of the regulatory obligations.

## 6 HOW TO MAKE A WHISTLEBLOWING REPORT?

**REPORTING PLATFORM** Reporting must normally be carried out through the internal reporting channel, i.e. the secure digital platform (supervised by the Reporting Manager), which can be reached at the link:

<https://discover.trusty.report>

The compilation of the report is extremely simple and immediate; in any case, a further information brochure is available on the website of the Data Controller.

*(If the whistleblower has reasonable grounds to believe that the internal reporting system is not effective/adequate, or in the event of a failure/feedback, an external report can be made to the National Anti-Corruption Authority (ANAC) at the following link: <https://servizi.anticorruzione.it/segnalazioni> )*

**CONTENT OF THE REPORT** The Reporting Party must provide all the elements useful to allow the due and appropriate verifications and assessments to be carried out, to ascertain the substantiation of the facts subject matter of the report. The name of Discover must be clearly indicated, as the company in which the offence was found, and a precise, detailed and truthful description of the facts must be provided, by filling in the required fields. You can upload files, paying attention to their content, and also to copyrights and metadata. You are requested not to enter data that is manifestly excessive or irrelevant, with a correct assessment of the incident subject matter of the report.

**IDENTITY OF THE WHISTLEBLOWER** Except in cases where a liability by way of slander and defamation can be configured, in accordance with the provisions of the Criminal Code or the Civil Code, and in cases where anonymity is not enforceable by law, (e.g., criminal, tax or administrative investigations, inspections of control bodies) **the identity of the whistleblower is protected in any context subsequent to the report.** As regards, in particular, the scope of the disciplinary proceedings, the identity of the whistleblower may be disclosed to the disciplinary authority and to the accused only in those cases where: there is the express consent of the whistleblower, or the dispute of the disciplinary charge is based, in whole or in part, on the report and the knowledge of the identity of the whistleblower is absolutely essential to the defence of the accused. It is possible to make reports anonymously, which however will be considered for further checks only if they relate to particularly serious events and with a content that is adequately detailed, not being able to verify that the reporting party falls within the categories authorized to report (referred to in point 2 of this document). In the case of anonymous report, whistleblower protections are also not applicable, nor is the possibility of carrying out investigation procedures that expressly provide for the identification of the whistleblower.

**SUBSEQUENT FEEDBACK** At the time of sending the report, the platform generates **access codes** (which the Whistleblower is required to save) that allow any further subsequent access to the report. Through subsequent accesses, the Whistleblower may add additional specifications to the information originally entered and check the evaluation status, as well as any comments, by the Channel Manager.

**7 HOW IS THE WHISTLEBLOWING REPORT HANDLED?** Within **7 days** of entry, a specific notice of receipt of the report is issued. Subsequently, the merits assessment activities are carried out, as well as any investigation needed. Within **3 months** from the date of the acknowledgement of the receipt, a complete acknowledgement will be provided through the platform. The Whistleblower may in any case verify at any time, through access with the reporting credentials, the presence of any notes/comments/feedback regarding the report.

**8 WHAT ARE THE GENERAL PURPOSES OF WHISTLEBLOWING REGULATIONS?** The report is an act of **manifestation of civic sense**, through which the Whistleblower contributes to the emergence and prevention of risks and situations prejudicial to the collective public interest and to his/her company. Therefore, Whistleblowing legislation aims to encourage reporting and to protect, precisely because of its social function, the Whistleblower, who must also use this opportunity responsibly.



# LEGAL NOTES ON HOW TO MAKE A REPORT AND PRIVACY POLICY

## PRIVACY POLICY

### Pursuant to Article 13 of EU Regulation 2016/679 "General Data Protection Regulation" (GDPR)

All personal data managed in the context of reports are processed in accordance with current regulations on privacy (EU Regulation 2016/679 "GDPR" and Legislative Decree 196/2003, as amended and supplemented by Legislative Decree 101/2018).

#### Type of data processed

All personal data contained in the reporting process are processed, therefore relating to the whistleblower, reported individual, any additional individuals included in the report, as well as in any subsequent investigation. The person entering the data (usually the whistleblower) is responsible for the relevance, correctness and non-excessiveness of the data entered. The platform manager/SB may delete any data that clearly does not comply with the general principles set out in Article 5 of the GDPR.

#### Purposes and legal basis of data processing

Data are processed for the purpose of correct management of reports, connected regulatory compliance, feedback to the whistleblower and any further investigation. The legal basis of the processing is to be found in Article 6, paragraph 1(c) "*the processing is necessary to fulfil a legal obligation to which the Data Controller is subject*".

#### Data processing methods

Data are processed in a manner and with tools designed to guarantee maximum security and confidentiality. The identity of the whistleblower is protected in accordance with the provisions of Art. 12 of Legislative Decree 24/2023, "*Obligation of confidentiality*".

#### Data retention

Data are processed for times compatible with the regulatory requirements, with specific reference to Art. 14 of Legislative Decree 24/2023 "*Preservation of documentation relating to reports*": the reports and the related documentation are retained for the time necessary to process the report, and, in any case no later than five years from the date of communication of the final result of the reporting procedure.

#### Scope of data knowability

Only formally designated, authorized and trained individuals may access the data, including: manager of the reporting platform, SB manager of the reports. In case of investigations, the data may be known by the public authorities in charge. In general, the data may be known within the scope of the provisions of Article 12 of Legislative Decree 24/2023.

#### Data controller and rights of the data subjects

The Data Controller is the undersigned company, in the person of its Legal Representative pro-tempore. More information about Whistleblowing can be found on the company's website. It should be noted that the rights referred to in Articles 15 to 22 of the GDPR can be exercised within the limits of the provisions of article 2-undecies of Legislative Decree 196/2003 "*Restrictions on the rights of the interested party*", that is, by contacting the Guarantor Authority directly.