

# DEXELANCE

WHISTLEBLOWING POLICY

DEXELANCE GROUP

## 1. Premises

The EU Directive n. 1937/2019 ("Whistleblowing Directive") has come into force also in Italy after the approval and publication in the Official Gazette of the Legislative Decree n. 24/2023. This Legislative Decree has cancelled and amended the previous regulations. Now the protection of those who report illegal conduct, in violation of domestic and European laws, is incorporated in just one law, applicable to both public and private sectors. In addition to a more detailed legal discipline of some aspects, which were already covered by the previous legislation, it is now mandatory for private companies to introduce a Whistleblowing process.

They are requested to include in their control management system the creation of an internal reporting channel through which can go the warnings of law violations in a protected and timely manner. It is also confirmed that the reporting of law violations can be addressed also to the National Anti-Corruption Authority (ANAC), once that the private company has adopted its own Whistleblowing process.

Dexelance Group, with the aim to make this law enforceable, approves the following Whistleblowing Policy and launches a dedicated digital platform, called "Whistleblowing Portal", to do the reporting also in an anonymous way, so to protect the identity of who is making the report.

## 2. The scope and recipients

This Whistleblowing Policy (hereinafter also the "Policy") aims to regulate the receipt, analysis and treatment of reports made also in anonymous way.

It is applied to all Dexelance Group. In particular, the recipients of this Policy are:

- Dexelance S.p.A. Key Officers and members of the company Management Board;
- Key Officers and members of the Group companies Management Board;
- All the employees of Dexelance S.p.A. and of the other Group companies;
- Partners, customers, suppliers, advisors, consultants, shareholders and, more extensively, anyone who has relationship with Dexelance Group (so called "Third Parties").

The recipients, who are aware of facts that can be reported, are strongly invited to make reports in a timely manner, following the instructions included herein and to refrain from doing their own analysis and/or investigations.

## 3. The report/Whistleblowing

"Whistleblowing" is defined as any report, made in the interest of the Company and its subsidiaries, of illegal conduct and/or violation of the Company Code of Ethics, the Organizational Model 231 and of the internal Group policies as of any other external applicable law, grounded on precises and proved facts that the Recipients are aware of as per their job and functions within the company. The reports must be:

- made in good faith;
- supported by detailed information so to be easily checked;
- made with spirit of responsibility and referred to the Dexelance Group interests;
- related to non-compliance facts and/or episodes for which this reporting system has been adopted.

Are "out of scope" of this Policy those reports which refer to commercial claims, sales offers, marketing activities that must be reported through the customer care channels.

## 4. The Whistleblowing portal

You can reach the Whistleblowing portal by clicking on the following web address: [idb.whistleblowing.italiandesignbrands.com](http://idb.whistleblowing.italiandesignbrands.com). The reports can be sent also to the 231 Surveillance Committee at the dedicated email address. The access to the portal is subject to a "no-log" policy so to protect the

identity of who is making the report and wants to remain anonymous: this means that IT systems cannot detect the IP address also when the access is made through a computer connected with the company computer network. The reports which flow through the Whistleblowing portal and pertaining to the holding company Dexelance are received, at the same time, by the Head of Internal Audit, the Group CFO and the President of the 231 Surveillance Committee. Whether the reports pertain to one of the Group companies are received, at the same time, by the Group CFO, the company Head of Finance & Administration and by the company 231 Surveillance Committee.

#### 5. The protection of who makes the report and his/her responsibility

No direct/indirect retaliation or discrimination can be perpetrated on who has made a report in good faith. In addition, the law gives sanctions to those who challenge the protective measures ensured for the reporting individuals.

At the same time, there are also sanctions against who has made the report with willful misconduct or gross negligence or in case the reports are proven as false, clearly ungrounded, with slander purpose and anyhow made to damage the company, the person targeted by the report as well as the other people in any way affected by the report. In this case the Company will consider the appropriate legal actions.

#### 6. The protection of the person targeted by the report

The report is not sufficient to open a disciplinary procedure against the person targeted by the report. When, on the basis of "fact based" allegation, the Company takes the decision to go on with an internal investigation, the person targeted by the report might be contacted and he/she will be allowed to provide any defensive elements and/or allegation.

#### 7. How to fill in and deliver the report

Who is intended to make the report, once clicked on the portal web site, needs to fill in a questionnaire with questions which aim to feature the report with all the necessary information (about time, location, actions done and so on ...) as well as with those documents and stuff to be alleged to the report. At the completion of the questionnaire, who is making the report can choose to give or not his/her personal data identity. Anyhow the personal data can be provided through the portal also at a later stage. When the report is filed, the portal will release an identification code (ticket). This code number, known only by who is making the report, cannot be longer recovered in case of loss and it will allow to give access again to the filed report for the following purposes: the monitoring of the investigation progress; the inclusion of additional facts and elements to attach to the report; the later stage provision of the personal details (first name and last name); response to the queries. In fact, the portal allows to create a virtual conversation with whom has made the report always preserving the anonymity.

#### 8. The report management

Through the portal the reports are delivered to the attention of the Head of Internal Audit Department and are subject to the following management process.

##### Preliminary Assessment

The Head of Internal Audit is committed to give a first feedback by 7 days. In particular, the reports will be preliminary audited by the Internal Audit Department to check the presence of those data and information helpful to assess the report groundness. In this ongoing assessment the Head of Internal Audit can ask – in case this is necessary to handle specific issues that are in the report – the support of the internal Legal Department (if present), as well as of the other appropriate company functions (e.g. Security) and also of the external advisors who have specific skills (e.g. legal, digital forensic). In addition, the Head of Internal Audit can require further information and documents via chat through the portal. At the completion of this preliminary

assessment phase, whether no proven and grounded facts are arisen, the report will be archived with appropriate justifications. On the contrary, when from this preliminary assessment arise facts which can make the report grounded, a further deeper investigation phase is started-up.

#### Deeper investigation

The Internal Audit Department will take care of:

- a) carrying on specific checks assisted, if necessary, by the competent departments of the Company and/or by the external advisors with the appropriate skills;
- b) agreeing, with the management responsible of the function affected by the inquiry, the action plan needed to tackle the reported weaknesses of the internal control system;
- c) agreeing with the Legal Department (and with the other functions involved) any measure to be taken for the protection of the Company interests (as court actions, suspension/cancellation of any supplier from the company list);
- d) requesting, if feasible, in agreement with the HR Department, the commencement of a disciplinary procedure vs. who has made the report. This in case it is proved that the report has been made in bad faith and/or with purely slander purpose, confirmed also by the absence of any grounded allegation;
- e) submitting, at the end of the process, the results of the investigation to the HR Department, to the President of 231 Surveillance Committee and/or Statutory Auditors, depending upon the major focus of the investigation, in order to adopt the most appropriate decisions, also disciplinary actions, against who has been proved liable for the violation occurred;
- f) closing the investigation at any time when it is proved that the report is ungrounded, out of what is already stated in letter e) and g);
- g) agreeing with the Statutory Auditors and/or with the President of 231 Surveillance Committee any other initiative to be taken prior to the definitive closure of the inquiry;
- h) starting-up the needed communication flows between the management/control bodies and all the other bodies of the internal control system, in particular the Internal Control and Risks Committee and the Manager responsible for the accounting documents.

All the activities as described can be executed non necessarily in the order described above. In performing this tasks the Internal Audit Department is committed to be compliant with the international standards of the Internal Audit practice and with Dexelance Group Code of Ethics.

#### 9. The regular Report

On a quarterly basis the Head of Internal Audit Department is due to provide a summary of the reports received to the President of 231 Surveillance Committee, the Statutory Auditors and the Internal Control and Risks Committee. When the report refers to one of the Dexelance group company, the Internal Audit Department will send it also to the 231 Surveillance Committee and to the Statutory Auditors of that company. This periodical summary report will contain the outcomes of all the concluded investigations, including any disciplinary measure that has been taken (or why no disciplinary measure has been adopted).

#### 10. The documentation filing and data protection

The Internal Audit Department is responsible for the safe filing of all the documentation about the reports received for a period of 2 years from the closure of the investigation, so to ensure proper management and tracking of all the activities performed. All the "sensitive" data part of the report, including those related to the identity of who has made the report as well those of other individuals involved in the investigation, will be

handled in compliance with the data protection laws and the GDPR Privacy Policy adopted by Dexelance Group.

#### 11. The update of this Policy

This policy and the Whistleblowing portal will be periodically updated to ensure the compliance with the applicable laws and to make it always aligned with the digital evolution.