

Reporting misconduct: the NIDEC ASI S.P.A. whistleblowing system

The Company attaches the utmost importance to compliance with all applicable regulations and aims to always act with integrity and in accordance with the principle of legality.

Legislative Decree No. 24/2023, issued in implementation of Directive (EU) 2019/1937, introduced a regime for the protection of individuals who report unlawful conduct of which they become aware in a work context (so-called *whistleblowing*).

Anyone who witnesses unlawful conduct, even if only potentially damaging, even in reputational terms, to the Company and/or the community as a whole, may report it without the risk of suffering retaliation.

To this end, the Company has adopted a set of rules (the "whistleblowing" Procedure) to deal with any reports independently and in strict compliance with the principles of confidentiality and privacy, starting from the moment they are received and throughout the entire process of investigating the reported violations. The System also offers the possibility of submitting reports and communications anonymously.

Who can report

The natural persons who may make a report, and to whom the protections provided for apply, are the Company's employees, self-employed workers, contractors, freelancers and consultants, workers or collaborators of suppliers and third parties, shareholders, persons with administrative, management, control, supervisory or representative functions.

What safeguards are in place

The main protection measures are the **protection of confidentiality** and the **prohibition of retaliation**. The identity of the Whistleblower and any other information from which this identity may be inferred, directly or indirectly, may not be disclosed to persons other than those competent to receive and follow up the reports, without the express consent of the Whistleblower.

Retaliatory acts are absolutely forbidden. Any retaliatory behaviour may give rise to disciplinary proceedings against the manager and may be reported to the A.N.AC, using the external reporting channel.

How to Send a Report to the Company

Internal alerts can be submitted in the following ways:

- in writing, via the <https://nidecasi.openblow.it/> portal.
- orally, upon request for a face-to-face meeting using the same portal and filling in the report form with the meeting request.

How a report is handled

After the submission of the report, confirmation of its receipt is received, and the information contained therein is subsequently examined by an independent Reporting Manager.

Further information may be needed and therefore a way of further contact is requested, even if an anonymous report is submitted.

An investigation will be initiated if the initial examination of the report reveals elements that give rise to the suspicion that a breach has been committed.

At the end of the investigation, if any, the results of the investigation will be assessed and appropriate measures will be taken, communicating the outcome to the reporter, if possible.

The 'external' reporting

A report may be made to the National Anti-Corruption Authority when one of the following conditions is met:

- the internal signalling channel has not been activated or, if activated, does not comply with the regulations;

- an internal report was not followed up;
- there are reasonable grounds to believe, on the basis of the concrete circumstances attached, that an internal report would not be effective or would lead to a risk of retaliation;
- there is good reason to believe that the breach may constitute an imminent or obvious danger to the public interest (e.g. to safeguard the health and safety of persons or to protect the environment).

Instructions for using the external signalling channel are available at the following link: <https://www.anticorruzione.it/-/whistleblowing>

Processing of personal data

The personal data of all persons involved in the report are processed in accordance with the current legislation on the protection of personal data set out in Regulation (EU) No. 2016/679 and Legislative Decree No. 196/2003 and on communication between competent authorities.

It should be noted that personal data are processed by the Company in its capacity as Data Controller, which determines the purposes and means of the processing of personal data, providing appropriate information to data subjects.

The data controller takes the necessary precautions to avoid the undue circulation of personal information, not only externally, but also within the organisation, by ensuring that the processing of personal data is restricted to authorised persons only.

The data controller formally identifies and appoints authorised persons, i.e. those who are authorised to process personal data in the reporting process, and provides them with appropriate operational instructions.

The Data Controller, the Data Processors and the persons authorised to process personal data are required to comply with the general principles of privacy legislation.

The reporting process provides for the processing only of personal data that are strictly necessary and relevant to the purposes for which they are collected, and reports may not be used beyond what is necessary to adequately follow up on them.

Personal data that are manifestly not useful for processing a specific alert are not collected or, if accidentally collected, are deleted immediately.

The data controller identifies and adopts appropriate technical and organisational measures to ensure a level of security appropriate to the specific risks arising from the processing operations performed, on the basis of a data protection impact assessment.

The Data Controller regulates the relationship with any external suppliers that process personal data on its behalf pursuant to Article 28 of the GDPR (the Data Processors).

The rights of the persons concerned (right of access, rectification, deletion so-called 'right to be forgotten', restriction of processing, portability, objection), especially those of the reported person, may be exercised within the limits of the provisions of the Privacy Code, which determines their suspension where they may result in an actual and concrete prejudice to the confidentiality of the identity of the reported person. In such cases, therefore, the Data Subject is also precluded from addressing the data controller and, if he/she considers that the processing that concerns him/her violates his/her rights, to lodge a complaint with the Garante privacy, in the absence of a reply from the latter.