2023

Whistleblowing" procedure adopted pursuant to Legislative Decree 10/3/2023 no. 24 for the submission and management of infringement reports

NIDEC ASI S.P.A.
registered office: Via Fratelli Gracchi n. 39, Cinisello Balsamo (Mi)
C.F. 00167500248 - P.I. 03238380962 - Cap. Soc. dei Soci Euro 15.644.000,00 i.v.
Single-member joint-stock company subject to management and coordination
exercised by Nidec Corporation Japan
PEC nidec-asi@legalmail.it - Tel. 02 64451

approved by the administrative body on 16 January 2024

Foreword

Legislative Decree No. 24/2023, issued in implementation of Directive (EU) 2019/1937, includes in a single piece of legislation the regime for the protection of individuals who report unlawful conduct of which they become aware in a work context (so-called *whistleblowing*).
By coordinating European law and national law, an integrated system of rules has been introduced with the aim of **incentivising the reporting of wrongdoing that affects the public interest or the integrity of the institution**.
In order to ensure the protection of the whistleblower's freedom, strengthen legality and transparency, and thus the prevention of offences, provision is made for

- the **whistleblower's right to protection** (with confidentiality and prohibition of retaliatory acts),
- **organisational obligations** for institutions (establishment of an internal reporting channel, instructions for the use of the external reporting channel and procedures to ensure confidentiality).

This procedure governs the handling of reports and provides for the forms of protection that are guaranteed to the author of the report, in order to prevent and combat unlawful conduct and behaviour that violates specific European and national provisions.
Anyone who finds himself or herself witnessing unlawful conduct, even if only potentially damaging, even if only in reputational terms, to NIDEC ASI S.P.A. and/or the community as a whole, may report it to the Company without the risk of suffering retaliation.

1. Definitions

The following definitions are adopted in this document:

- Procedure: this procedure.
- **Company**: NIDEC ASI S.P.A..
- **Reporting**: the written or oral communication of information on violations.
- **Anonymous report**: any report from which the identity of the reporter cannot be established.
- **Violation**: conduct, act or omission that harms the public interest or the integrity of the private entity within the meaning of the legislation.
- **Information on violations**: information, including reasonable suspicions, concerning violations that have been committed or that, on the basis of concrete evidence, might be committed.
- **Reporting** person: the natural person reporting information on infringements.
- **Reported** person: the natural or legal person mentioned in the report to whom the breach is attributed or in which it is implicated.
- **Reporting Manager** or **Manager**: Chairman of the Supervisory Board pursuant to Legislative Decree 231/2001, who is in charge of managing reports.
- **A.N.AC.**: National Anti-Corruption Authority.
- **Internal reporting**: communication submitted via the internal reporting channel.
- **Portal**: IT platform used by NIDEC ASI S.P.A., accessible via a link https://nidecasi.openblow.it/ and used for internal reporting.
- **External reporting**: the written or oral communication of information on violations, submitted through the external reporting channel, when the conditions provided for by the standard are met[1] .
- **Public dissemination**: making information about violations publicly available, through the press or electronic media or media capable of reaching a large number of people, if the conditions provided for by the legislation are met[2] .
- **Administrative body**: Board of Directors or Managing Director
- **Follow-up**: the action taken by the Reporting Manager to assess the existence of the reported facts, the outcome of the investigation and any measures taken/to be taken.
- **Acknowledgement**: communication to the reporting party of information concerning the follow-up given or intended to be given to the report.

[1] Article 6 D. No. 24/2023 (Conditions for external reporting)
[2] Article 15 D. Legislative Decree No. 24/2023 (Public Disclosures)

- **Work context**: the work activities in which a person acquires information about violations and could risk retaliation in the event of a report.
- **Retaliation**: any conduct, act or omission, even if only attempted or threatened, occurring by reason of the report, the report to the Judicial Authority or public disclosure and which causes or may cause the reporting person or the person making the report, directly or indirectly, unjust damage.

2. Normative references

- Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (so-called Whistleblowing Directive), available here
- Legislative Decree No. 24 of 2023, available at the link here
- Guidelines on procedures for the submission and management of external reports, prepared by A.N.AC, available here
- Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, so-called GDPR), available here
- Legislative Decree No. 196/2003, Personal Data Protection Code (so-called Privacy Code), available here

3. Reports

3.1. What to report

The Whistleblower communicates information on **Breaches**, i.e. conduct, acts or omissions that are likely to harm the public interest or the integrity of the Company. This broad formulation is then restricted to a list of violations that can be divided into three categories:

- offences falling within the scope of EU or national acts relating to **specific sectors**: public procurement; services, products and financial markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems;
- breaches of **European provisions** consisting of: acts or omissions detrimental to the financial interests of the Union; acts and omissions concerning the internal market; acts and conduct that frustrate the object or purpose of the provisions of Union acts in the areas mentioned above;
- violations of **national provisions** consisting of: **administrative, accounting, civil or criminal offences**; **unlawful conduct relevant under Legislative Decree No. 231/2001**.

Reports may concern violations that have already been committed or that are believed to be committed, on the basis of concrete, precise and concordant elements, or conduct aimed at concealing them.

3.2. Who can report

The natural persons who may make a Report of Violation, to whom the protections illustrated below apply, are: employees[3] of the Company; self-employed workers, collaborators[4] , freelancers, professionals and consultants; workers or collaborators of suppliers and third parties; persons with functions of administration, management, control, supervision or representation, even in the case of functions exercised on a de facto basis ; shareholders.

[3] This includes part-time, intermittent, fixed-term, temporary, apprenticeship, ancillary work, casual workers

[4] Holders of a collaboration relationship referred to in Article 409 of the Code of Civil Procedure, e.g. "... agency, commercial representation and other collaboration relationships that result in the provision of continuous and coordinated work, predominantly personal, even if not of a subordinate nature (...) e.g. lawyers, engineers (...) who provide their work for a private sector entity by organising it independently (para-subordinate relationship). - Holders of a collaboration relationship referred to in Article 2 of Legislative Decree No. 81/2015. These are - pursuant to para. 1 of the aforementioned provision - collaborations organised by the principal that take the form of exclusively personal and continuous work, the manner of performance of which is organised by the principal. This also applies if the manner of performance is realised by means of digital platforms.

3.3. Protected subjects

The protection of the **reporter** applies during the course of the employment relationship, before or after its establishment, including during the probationary period and after its termination.
Other persons, natural or legal, in the same employment context, although not directly making the report, enjoy protection in the event of involvement in the report, such as:

- the **Facilitator**, a natural person who assists the reporter in the reporting process, operating within the same work context and whose assistance must be kept confidential[5] ;
- persons in the same work environment as the reporter and who are linked to him by a stable **emotional or family relationship** up to the fourth degree;
- **colleagues** of the Whistleblower who work in the same work environment and have a regular and current relationship with that person;
- the entity owned or employed by the reporting person, or which operates in the same work environment as the reporting person.

3.4. Examples of actions, facts and conduct that can be reported

In order to facilitate the identification of facts that can be reported, some examples of conduct and/or behaviour are given below:

- discharge, emission or other release of hazardous materials into the air, soil or water;
- illegal disposal of hazardous waste;
- competition and state aid violations;
- falsification, alteration, destruction, concealment of documents;
- administrative irregularities in accounting and tax compliance or in the preparation of financial statements;
- the giving of a sum of money or other benefit to a public official or a person in charge of a public service in return for the performance of his duties (e.g. facilitation of a case) or for performing an act contrary to his official duties (e.g. failure to issue a tax irregularity report);
- Providing or promising money, goods, services or other benefit to bribe a supplier or customer;
- Agreements with suppliers or consultants to make non-existent services appear to have been performed;
- falsification of documentation, e.g. expense reports, in order to create funds for illegal activities;
- theft of goods or business assets;
- sexual harassment;
- use of one's authority to coerce colleagues into improper activities.

In case of **doubt** as to whether a conduct is legitimate or not, one can turn to the Reporting Manager.

3.5. Content of the Report and Anonymous Reports

Reports must include a detailed description of the facts and any supporting documents, in order to allow for a proper understanding and assessment of their reliability.
Unsubstantiated news, mere suspicions, information that is already in the public domain, as well as information acquired on the basis of mere supposition or rumour are therefore not included among reportable information.
The report must describe the **incident, with a** clear and complete description of the event, including the time and place of occurrence.
The Company also accepts **anonymous Reports**, provided they are substantiated, precise and detailed. The Reporting Manager will assess their reliability and whether to follow them up.

[5] By way of example, the facilitator could be a colleague from the reporter's office or another office who confidentially assists him/her in the reporting process. The facilitator could be a colleague who is also a trade unionist if he or she assists the whistleblower in his or her name and on his or her behalf, without using the trade union's acronym. If, on the other hand, he assists the whistleblower by using the trade union acronym, he does not play the role of facilitator.

3.6. Alerts not covered by the procedure

Disputes, claims or demands of a personal nature that relate exclusively to one's individual working relationships or with one's superiors cannot be reported.
Reports of a discriminatory nature or with a purely defamatory or slanderous purpose, relating exclusively to aspects of private life, without any direct or indirect connection with the reported person's business and/or professional activity, are prohibited.
The protections provided for may not be guaranteed in such cases, and the criminal, civil and disciplinary liability of the Whistleblower remains unaffected in the event of a slanderous or defamatory report, made with malice or gross negligence or with the sole aim of harming the reported person.
The regulation does not affect the application of certain regulatory provisions, such as legal professional secrecy and secrecy of court deliberations.

4. Types of Signalling

Four types of alerts can be distinguished, depending on the mode of presentation:
- those submitted through an **internal Company channel**;
- those submitted through an **external channel** set up and managed by the AC;
- **public disclosure**;
- the **Complaint to the Judicial Authority**.

4.1. Internal Reporting

The internal reporting channel is the tool to be used as a **priority.**
The internal channel **ensures the confidentiality**, including through the use of encryption tools, of the reporter, the facilitator, the content of the report and the related documentation.
Internal reports can be made in **written** form, also via an IT platform, and **orally**, through voice messaging systems managed by the same IT platform or through **direct** interview with the Reporting Manager.
The **Reporting Manager**, an autonomous, dedicated and specifically trained entity, performs the activities required by the legislation and set out below.

4.2. External Reporting

The reporting agent may make a report to the channel activated by the A.N.AC. 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;
- made an internal report that was not followed up;
- has reasonable grounds to believe, on the basis of the factual circumstances attached, that making an internal report would be ineffective or lead to a risk of retaliation;
- has well-founded reasons 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 on how to use the external reporting channel are available on the A.N.AC website, together with the general rules, at the following link: https://www.anticorruzione.it/-/whistleblowing

4.3. Public Disclosure

The reporter may make a public disclosure when one of the following **conditions** is met:
- has already made an internal and an external report, or has made an external report directly, without receiving a response within the time limits laid down in the legislation;
- has well-founded reasons to believe that the infringement may constitute an imminent or obvious danger to the public interest;

- has well-founded reasons to believe that the external report may entail a risk of retaliation or may not be followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may be colluding with or involved in the infringer.

The scope of the instrument is therefore **limited to very exceptional cases**.

4.4. Reporting to the Judicial Authority

The whistleblower may apply to the judicial authorities to make a complaint of unlawful conduct of which he/she has become aware in his/her private employment context.
The same rules on the protection of confidentiality and the content of reports are respected by the offices of the judicial authorities receiving the report.

5. Submission and management of internal reporting

5.1. Submission of Internal Reporting

Internal reports can be submitted through the internal channel in the following ways:

- **in writing via the https://nidecasi.openblow.it/ portal.**

The portal is also freely accessible via the link available at https://www.nidec-industrial.com/ under 'compliance'.
The platform used OpenBlow:
- separates the identification data of the reporter from the content of the report, providing for the adoption of codes replacing the identification data, so that the report can be processed anonymously and the identity of the reporter can be subsequently reconstructed only in the permitted cases;
- manages reports, ensuring the traceability of the process;
- keeps the content of reports confidential throughout the entire report handling phase;
- adopts secure protocols for data transport over the network as well as the use of encryption tools for the contents of reports and any attached documentation;
- adopts appropriate data and documentation storage methods (physical, logical, hybrid);
- adopts policies to protect confidentiality through IT tools (decoupling of the reporter's data from the reporting information, encryption of data and attached documents);
- adopts data access policies (access officers, computer system administrators).

The reporter accesses the portal by filling in a standard form, with the necessary elements for proper reporting, and obtaining personal credentials.
If the reporter provides his or her personal details, the Reporting Manager receives the identification data and must guarantee confidentiality.
If the reporter does not provide his or her personal details, the report will be treated as anonymous.
The personal credentials attached to the first Report are subsequently required for further communication with the Manager (receiving messages and/or requests for clarification, sending further information that may become known to supplement the reported facts). In the event of loss of personal credentials, they cannot be recovered or duplicated in any way; in this eventuality, the Reporter must make a new Report and identify himself.
In order to allow further investigation of the reported facts, the portal allows the establishment of a confidential 'dialogue' between the reporter and the Reporting Manager, as well as the possible sending of electronic documents as attachments.
The portal acts as an electronic register of reports and allows:
- the allocation of a unique progressive code,
- traceability of the management process; even in the case of reports received by other means, by uploading them to the portal itself.

- **orally through the aforementioned platform or, at the request of the reporter, by means of a face-to-face meeting.**

It is possible to register one's own messages on the above-mentioned platform or to request a direct meeting with the manager, which must be arranged within a reasonable period of time. The request must be made by filling in the reporting form.
The date for the meeting will be communicated within 7 days of receipt of the request.

5.2. Receipt and Acknowledgement of Receipt

Depending on the signalling channel chosen, the reception and recording modes are:
a) **Reports received through the portal**: the report is registered in the portal.
b) **Reports received by face-to-face meeting:** during a meeting, the report is documented, with the consent of the reporting person, by means of minutes or a recording of the meeting. The reporting person is requested to verify, rectify or confirm the minutes with his/her signature.
Within seven days of receipt, the Manager issues an **acknowledgement of receipt to the Reporting Officer**.
The report is recorded in a computer register (excel file, password-protected) The report is **recorded in a computer register (excel file, password-protected) of Reports**, with date and time of receipt and allocation of a unique code, in which any documents collected and the results of the checks carried out will subsequently be noted.
In the event that the Handler is the reported person, or if the Handler has a possible conflict of interest, connected to the report, such as to compromise its impartiality and independence of judgement, he/she shall abstain from expressing his/her judgement on the report.

5.3. Preliminary Evaluation and Classification of the Report

The Manager promptly carries out a preliminary analysis of the Report, if necessary requesting further information and/or documentation from the Reporting Party via the Portal.
At the end of this preliminary analysis, the Manager will classify the report into one of the **following categories**:
a) **Irrelevant** report: a report that is not relevant within the meaning of Article 3.1 above. **It is filed by acknowledging it to the Whistleblower,** if contact details are available. If the Manager considers the report to be well-founded and sufficiently detailed, even if it cannot be traced back to an offence, he may consider bringing it to the attention of the administrative body; if it is forwarded, the Whistleblower is informed if contact details are available.
b) **Relevant report but not actionable**: relevant report, but without sufficient information and/or elements it is not possible to proceed with further investigation. **It is closed by giving feedback to the reporter,** if contact details are available.
c) **Prohibited Report**: a report falling within the cases identified in Section 3.6. The Manager may consider submitting the prohibited report to the administrative body for the possible initiation of disciplinary proceedings and inform the Whistleblower of this, if contact details are available. Should the Manager ascertain the presence of the requirements laid down in Legislative Decree No. 24/2023 for possible disciplinary proceedings, the same will be followed up. The **Report shall be filed with mention of the possible disciplinary proceedings and their outcome**.
d) **Relevant and Processable** Report: relevant and sufficiently substantiated report. The Manager initiates the verification phase.

5.4. Verification phase and internal investigations

If the report received is classified as relevant and treatable, the Manager will proceed with the initiation of **internal verifications and investigations in** order to **gather further detailed information and to verify the validity of the facts reported**. The verifications may be carried out, by way of example, through the analysis of documents, interviews, questionnaires. The Manager may request further information or documentation from the Whistleblower and, in the case of anonymous reports, ask for his consent to disclose his identity.
It is not up to the Manager to ascertain individual responsibilities, nor to carry out checks of legitimacy or merit, which will be the responsibility of the institutionally competent subjects in the company.

In this phase, the Manager will rely on the support of the corporate functions, which must provide full cooperation and, where deemed appropriate, of specialised consultants whose involvement is functional to the investigation of the report, guaranteeing confidentiality.
The Manager ensures that the acknowledgement is updated in favour of the reporter, if necessary.

5.5. Conclusion of the verification phase and feedback to the reporter

Upon completion of the verification phase, the Manager:
- prepares a **report summarising** the investigations carried out and the evidence that emerged, sharing it, on the basis of the results, **with the company managers** concerned, in order to define the **actions to be taken** to protect the Company, without any indication from the Whistleblower;
- **shall, within three months of the** date of the acknowledgement of receipt or, failing this, within three months of the expiry of the period of seven days from the submission, give feedback to the Reporting Party by means of the Platform or other appropriate means as to the action which has been taken or is intended to be taken.

For the purpose of assessing any disciplinary measures to be taken and/or any notifications to the competent authorities, the Manager shall inform the administrative body and the Board of Auditors**.**

5.6. Periodic information

The Manager informs the administrative body and the Board of Auditors on a half-yearly basis about the number of reports received during the period and their developments.

5.7. Relevant and addressable report concerning senior management

In the event of a relevant and negotiable report concerning persons in charge of deciding possible disciplinary measures, complaints or other actions, the Manager immediately involves the Chairman of the Board of Directors, in order to coordinate and define the investigation process.
In the event of a material and negotiable report concerning the Chairman of the Board of Directors, or one of the members of the Board of Directors, the Reporting Manager notifies the Board of Auditors.

5.8. Filing and storage of the Report

The Reports and related documentation are kept for as long as necessary to process them, and in any case **no longer than five years** from the date of the communication of the final outcome.

6. The protection measures envisaged

The protection **measures** fall under the following safeguards:
- right to confidentiality;
- prohibition of retaliation;
- supporting measures;
- limitations of liability with respect to the disclosure of certain categories of information under certain conditions.

To benefit from the protection measures, the person must be one of the persons identified in Section 3.3. and the report must have been made in accordance with this procedure.
Waivers and settlements of the rights and remedies provided for herein are generally prohibited.

Right to confidentiality. The identity of the Whistleblower and any other information from which that identity can be inferred, directly or indirectly, cannot be disclosed to persons other than those competent to receive and follow up the reports, without the express consent of the Whistleblower. **A protection regime** is thus **guaranteed**.

Prohibition of retaliation. Retaliatory acts are prohibited. They are null and void if they are taken, upon declaration by the judicial authority. The burden of proving that such conduct is motivated by reasons unrelated to the reporting is on the employer.
Examples of retaliation are dismissal, suspension or equivalent measures; demotion in rank or non-promotion; change of duties, change of workplace, reduction in salary, change in working hours; suspension of training or any restriction on access to it; negative merit notes or negative references; adoption of disciplinary measures or other sanction, including a fine; discrimination or otherwise unfavourable treatment; early termination or cancellation of a contract for the supply of goods or services.
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[6] .

Support measures. The A.N.AC. stipulates agreements with third-sector entities to provide support measures to the reporter, providing assistance and advice free of charge. A list of third-sector entities providing such services is established at the A.N.AC.

Limitations of liability. The Whistleblower shall not be punished, even if the facts reported turn out to be unfounded and/or insubstantial, or he/she discloses information covered by the obligation of secrecy (including official secrecy, professional secrecy, scientific or industrial secrecy)[7] , not to disclose information relating to the organisation and production methods of the company, copyright protection, personal data protection or offend the reputation of the reported person, if at the time of the report he had reasonable grounds to believe that the disclosure of the information was necessary to discover the breach and the procedures provided for in the legislation were used. This immunity may apply provided that the acquisition of information or access to documents was lawful.

6.1. Protecting the confidentiality of the reporter

The protection of the whistleblower's confidentiality is also guaranteed in judicial[8] and disciplinary[9] .
The reporter loses the right to confidentiality if he/she is found to be criminally liable, even in a court of first instance, for the offences of defamation and slander, and in the event of civil liability on the same grounds of wilful misconduct or gross negligence.
If the person making the public disclosure turns to a journalist, he or she is protected by journalists' professional secrecy (as the source of the news) and does not fall within the scope of Legislative Decree No. 24/2023, thus benefiting from greater protection.
On the other hand, confidentiality protection does not apply if the Whistleblower has intentionally disclosed his or her identity (using social networking sites), without prejudice to all other forms of protection provided for. In the event that the person making the disclosure does not reveal his or her

[6] Legislative Decree no. 24/2023 provides that communications of retaliation are to be transmitted exclusively to ANAC for the investigations attributed to it by law and for the possible imposition of the administrative sanction on the person responsible. It is important, therefore, that those who have suffered retaliation do not transmit the communication to parties other than ANAC so as not to nullify the protections that Legislative Decree no. 24/2023 guarantees, first and foremost, confidentiality. "Where the communication of retaliation is mistakenly received by public or private subjects, instead of ANAC, such subjects are required to guarantee the confidentiality of the identity of the person who sent it and to transmit the communication to ANAC, giving contextual notice of such transmission to the subject who made it". "The most representative trade unions in the administration or entity in which the retaliation was carried out cannot communicate it to ANAC" (ANAC Guidelines).
[7] Articles 326 (Disclosure and use of official secrets), 622 (Disclosure of professional secrets), 623 (Disclosure of scientific or industrial secrets) of the Criminal Code, Article 2105 of the Civil Code (Duty of loyalty).
[8] "In the context of criminal proceedings, the identity of the reporter is covered by secrecy in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure"; "compliance with the obligation of confidentiality requires that the administrations and bodies involved in the management of reports guarantee such confidentiality during all the stages of the reporting process, including the possible transfer of the reports to other competent authorities". (ANAC Guidelines)
[9] "Within the framework of the disciplinary proceedings activated by the administration against the alleged perpetrator of the reported conduct, the identity of the reporter may not be disclosed, where the accusation of the disciplinary charge is based on investigations distinct and additional to the report, even if consequent to it. If the identity of the reporter is indispensable for the defence of the person charged with the disciplinary offence, it may be disclosed only with the express consent of the reporter". (ANAC Guidelines)

identity (using a pseudonym or nickname, resorting to social networking sites), such disclosures are comparable to anonymous reports.

6.2. Protecting the confidentiality of the reported person

In order to prevent any abuse, i.e. in order to prevent slander, defamation, even the disclosure of personal data of the reported person that could entail damage to his/her reputation, discrimination, or other disadvantages, measures are also foreseen to protect the reported person.
The Whistleblower is informed by the Manager of his or her involvement in the reporting process, at the time deemed appropriate, in order to avoid compromising the internal verification and investigation phase.
The reported person may not be subject to disciplinary sanctions in the absence of objective evidence of the reported breach, i.e. without having investigated the reported facts and contested the relevant charges in accordance with the law and/or the contract.
The reported person may be heard, or, at his/her request, shall be heard, by means of written submissions and documents.
Decisions on any disciplinary measures, complaints or other actions to be taken, following the results of the investigations conducted, are taken by senior management, according to the powers/delegations granted, and in any case by persons other than those who conducted the investigations, in order to avoid conflicts of interest or lack of impartiality.
The protection of the reported person applies without prejudice to legal provisions imposing an obligation to disclose his/her name, for instance when requested by the judicial authorities.

6.3. Further protection of the confidentiality of the reported person and protection of the confidentiality of any others involved in the reporting process

The protection of the identity of the persons mentioned in the report is to be guaranteed by the Company and, where appropriate, by the A.N.AC until the conclusion of the proceedings initiated as a result of the report, and in compliance with the same guarantees provided for in favour of the Whistleblower[10] .

6.4. 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[11] .
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.

[10] "The legislator then considered that confidentiality should be guaranteed: - To the facilitator as regards both identity and the activity in which the assistance takes place. - To persons other than the reported person but nevertheless implicated in so far as they are mentioned in the report or in the public disclosure (e.g. persons mentioned as witnesses). The rationale of the new rules is to be found in the need to safeguard the rights of persons who, as a result of the report, might suffer damage to their reputation or other negative consequences even before it is proved that they are not involved in the reported facts. (..) An exception to this duty of confidentiality of the persons involved or mentioned in the report is the case where reports are made to judicial authorities and the Court of Auditors. This is confirmed by the fact that the legislator, in providing for the protection of confidentiality in judicial proceedings, refers only to the identity of the reporter and not also to the identity of the person involved or mentioned in the report" (ANAC Guidelines) (see Article 12, paras. 3, 4 and 7 of Legislative Decree no. 24/2023).

[11] The disclosure of personal data by EU institutions, bodies, offices or agencies is made in accordance with EU Regulation 2018/1725. Regulation (EU) 2018/1725, published in the OJEU on 21 November 2018, on the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data. It complements the rules laid down in Regulation (EU) 2016/679, which lays down general rules for the protection of natural persons with regard to the processing of personal data and on the free movement of personal data within the Union, and aims to align, as far as possible, the data protection rules for Union institutions, bodies, offices and agencies with those adopted for the public sector in the Member States.

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.
he 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, and possibly, in the absence of a reply from the latter, from lodging a complaint with the Garante privacy.

7. Training and Information

The procedure is published on https://www.nidec-industrial.com/, in the 'compliance' section of the portal https://nidecasi.openblow.it/ and is displayed in workplaces.

8. Breach of procedure

Any breach of the Procedure may constitute a **disciplinary offence punishable by the** Company, in accordance with the following paragraph.
In particular, it is pointed out that they are sanctionable:
- retaliation against the Whistleblower for reasons related, directly or indirectly, to the report;
- attempt to hinder or obstruct reporting;
- failure to verify and analyse reports received;
- breach of confidentiality and data protection obligations;
- Conviction, including by a judgment at first instance, for offences of defamation and slander, or proven civil liability by a judgment at first instance in the event of reporting made with intent or gross negligence.

9. Sanctioning system

Failure to comply with or violation of the rules contained in the procedure may lead to enforcement by the Company:
- **disciplinary measures** against employees in the cases provided for by the law and the applicable National Collective Labour Agreement;
- **termination of** the contract and/or collaboration with respect to collaborators and third parties.

In any case, the Company may take all criminal, civil or administrative actions established by law, should the grounds for criminal, civil or administrative liability arise.

10. The Nidec Group's reporting system

Even before the adoption of the measures set out in Section 2, the Nidec Group had already had a general internal channel to which it could report any violations of the Group Code of Conduct.
The Nidec Group has a very clear policy of non-retaliation and protection for anyone who reports a breach of the Code of Conduct in good faith.
The Nidec Group has always been committed to providing employees with a safe and reliable way to report information, using an independent company, EthicsPoint, to handle all reports.
Even through this channel it is possible to report information anonymously and confidentially, insofar as anonymous reporting is permitted by law.
The service is available in several languages and reports can be made via the EthicsPoint telephone numbers or the website.
You can find out how to use group channels at https://www.nidec-industrial.com/, in the 'compliance' section.
Reports received by the Group will be communicated to the Reporting Manager and processed in accordance with this procedure.

11. Updating the procedure

The procedure is subject to annual review and is approved by the Administrative Body of NIDEC ASI S.P.A..