



Nexova Group Whistleblowing Policy

Document type: Policy

Document ID: 241191

Document classification: Public

Table of contents

1	Introduction	3
2	Definitions	3
3	General principles	4
4	Management of Reports	4
	4.1 Reporting channels	4
	4.2 Content and submission of Reports	5
	4.3 Receipt of the Reports	5
	4.4 Verification of the Reports	5
	4.5 Result of the Verifications	6
5	How Reports are stored	6
6	Reporting outside the company	7
7	Protecting the Whistleblower’s right to report	7
	7.1 Confidentiality.....	7
	7.2 Anonymity	8
	7.3 Protection against retaliation and discrimination	8
	7.4 Protection of personal data	8
Annex A		10

1 Introduction

The Nexova Group Whistleblowing Policy (hereinafter the “**Policy**”) sets out the procedure for submitting a Whistleblowing Report relating to Breaches, the guidelines for handling Reports and the standards of protection for Whistleblowers and other people involved in the investigation. This Policy also guarantees the principles of confidentiality, protection of anonymity and prohibition of retaliation, in accordance with applicable local, regional, national and international regulations.

Nexova Group S.A. and its affiliate (hereinafter “**Nexova**”) are committed to responsible business practices, and to always acting, in accordance with their values, policies and procedures, and relevant laws and regulations, including the Whistleblower Directive (*Directive EU 2019/1937*).

Nexova encourages its employees, freelancers, shareholders, suppliers, customers and, more generally, all stakeholders to report, in good faith, any behaviour – acts or omissions – carried out at Nexova or in relations with it, that constitutes a Breach (or induces a Breach) of applicable laws and regulations, or Nexova’s values, policies or procedures.

Nexova understands that it takes courage to report a Breach, so therefore it is committed to providing the Whistleblower with an easy and safe way to do so. Reporting a Breach is an essential element that enables Nexova to protect its people, its company values, its stakeholders and society as a whole.

The provisions of this Policy do not prejudice or limit in any way the right or obligation (as they may be defined by locally applicable regulations) to report to the competent regulatory, supervisory or legal authorities in the countries where Nexova operates, to any other body designated for this purpose by local legislation and/or to any supervisory body established within Nexova.

2 Definitions

Addressees of this Policy are natural persons who have directly or indirectly obtained information about Breaches, including but not limited to:

- Employees, collaborators, members of the corporate bodies of Nexova.
- Employees, collaborators, members of corporate bodies and shareholders of customers, suppliers, sub-suppliers (including the entire supply chain) and other business partners.
- Consultants, freelancers and service providers.
- More generally any of Nexova’s stakeholders.

Breach(es) means an act or omission committed during the course of business or in connection therewith, by any person within Nexova, on its behalf or in dealings with Nexova, that have occurred, may reasonably be expected to have occurred or are very likely to occur, including any attempts to conceal such actions or omissions and that constitute a breach, or an incitement to a breach of:

- Laws and other applicable regulations, at all levels (local, regional, national, international).
- The values and principles laid down in Nexova’s Code of Conduct.
- Nexova’s policies and procedures.

Facilitator is the person who assists a Whistleblower in the reporting procedure, connected to the latter through a working relationship.

Related Person is any person who has a personal or professional relationship with the Whistleblower.

The extensions or limitations to the legal protection afforded to Whistleblowers and other related/supporting parties (by way of example, but not limited to: legal entities owned by the persons referred to above, or legal entities for which a person referred to above works or to which such person is otherwise professionally related) may vary depending on locally applicable regulations, their role and the type of Breach reported.

Reports mean the communication, via the procedure set out in the following sections, of information concerning Breaches.

Report Manager means the department or person(s) in charge of managing the report received. In Nexova, the Report Manager is the Group General Counsel, appointed by Starion Group S.A., a sister company to Nexova Group S.A., which provides legal services as well as other Corporate services to Nexova. Depending on the topic of the Report, additional consultation could be received from Starion Group S.A. (e.g. Data Protection Officer, Human Resources, Security Officer). Only the Legal Department of Starion Group S.A. will be in contact with the Whistleblower via the Whistleblowing Platform. In case of a conflict of interest with the Report Manager, the persons directly or indirectly involved on the suspected Breach will not be authorized to participate in the assessment of the Report, nor in the decision as to the follow-up measures, where these are needed.

Reported Person is the author or alleged author of the Breach.

Whistleblower means a person who submits a Report.

Whistleblowing Platform is the SpeakUp platform operated by an independent service provider called People Intouch B.V., headquartered in the Netherlands, and available 24/7. On that Platform a Whistleblower can set up a secured electronic post-box that will allow them to communicate securely and anonymously with the Report Manager. The Report submitted via the Whistleblowing Platform cannot be traced in any way.

3 General principles

Nexova undertakes to respect the following general principles in managing the Whistleblowing process and requires Whistleblowers and other persons involved to respect these principles to the extent of their competence:

- **Principle of confidentiality:** Nexova guarantees the confidentiality of Whistleblowers, Whistleblowing Reports and the information contained therein.
- **Principle of proportionality:** Nexova's investigations are adequate, necessary and proportionate to achieving their purpose.
- **Principle of impartiality:** the analysis and processing of Reports are carried out impartially, irrespective of the opinions and interests of the persons responsible for handling them.
- **Principle of good faith:** the protections afforded to Whistleblowers (specified in Section 7) are applicable even in cases where the Report proves to be unfounded, if it was made in good faith (i.e., the Whistleblower had reasonable grounds to believe that the information relating to the Breaches was true at the time of the Report and that the information fell within the scope of the Policy); no Whistleblower may take advantage of these protections to avoid a disciplinary sanction against them.

4 Management of Reports

4.1 Reporting channels

A Whistleblower may submit a Report in a variety of ways. For many matters, it can be a good first step to talk to the person involved directly. If this is not possible, or the Whistleblower does not feel comfortable doing so, the following channels are available:

- The Whistleblower may talk to their manager or their manager's manager. If this is not possible, or they do not feel comfortable doing so:
- The Whistleblower may talk to HR. If this is not possible, or they do not feel comfortable doing so:
- Use the Whistleblowing Platform.

4.2 Content and submission of Reports

Addressees who become aware of Breaches are encouraged to report facts, events and related circumstances promptly and in good faith, provided that they have reasonable grounds to believe that such information is true. Please note that general assertions cannot be investigated. Therefore, if possible and when known to the Whistleblower, the Report must include:

- The name of the Whistleblower and relevant contact details for further communication. However, Reports may also be submitted **anonymously** via the Whistleblowing Platform.
- A detailed description of the events that occurred (including date and location) and how the Whistleblower became aware of them.
- Which law, internal regulation, etc. is alleged to have been breached.
- The name and role of the Reported Person(s) or information identifying them.
- The name and role of any other parties who may refer on the reported events.
- Any documents or other elements that may substantiate the reported events.

The Report can be submitted in several languages in the following ways:

- Through the reporting platform <https://stariongroup.speakup.report/ethicsline>
- Via the phone line available through the telephone number listed in Annex A.

All listed channels are designed and operated in a secure manner, to prevent access to information by unauthorized persons and to ensure that the identity of the Whistleblower and other persons involved in the investigation remains confidential (see chapter 7.4 Personal Data).

Once the Whistleblower has submitted a Report, the Whistleblower will receive an individual report number (the “**Report Number**”) which is needed each time they want to access the system. It is important that the Whistleblower takes note of his/her Report Number and password and keeps this safe. Neither the operators of the Whistleblowing Platform nor Nexova will be able to reset the password. In such case, please re-submit a Report.

The Whistleblower must act in good faith, and the Report must be founded on substantiated concerns. In case of abusive reporting or reporting in bad faith, the Whistleblower may incur disciplinary, civil or criminal sanctions.

4.3 Receipt of the Reports

When a Report is sent, within 7 days of its receipt the Report Manager sends a communication via the Whistleblowing Platform to the Whistleblower confirming that the Report has been received and acted upon. After the submission of the Report, a transcription of the voice message or web report is sent to the Report Manager.

4.4 Verification of the Reports

The Report Manager examines the Report to determine whether it is substantiated. Initially, it conducts a preliminary analysis to determine whether there is sufficient evidence for a potential or actual Breach (known as the "plausibility check").

If such evidence exists, the Report is further investigated. Otherwise, the Report will be filed in line with locally applicable data retention regulations; the Whistleblower will be informed of this and, if the Report does not fall within the scope of this Policy, it may be referred to other channels or other company procedures.

If it is possible to believe that the facts contained in the Report constitute a criminal offence, the Report Manager shall assess, in consultation with the other competent company departments and Nexova's management, whether and when the information contained in the Report should be notified to the competent judicial authorities, including on the basis of locally applicable regulations.

The Report Manager is then responsible for verifying the Report and for conducting a prompt and thorough investigation, in accordance with the principles of impartiality, fairness, proportionality and confidentiality towards the Whistleblower, the Reported Person and all the parties involved in the Report.

During the course of these verifications, the Report Manager may rely on the support of the relevant company departments and/or specialized external consultants, guaranteeing the confidentiality of the information and anonymizing as much personal data as possible.

During the investigation, the Report Manager may ask the Whistleblower to provide further necessary and proportionate supporting information; the Whistleblower has the right to complete or correct the information provided to the Report Manager, in compliance with the principle of good faith (Nexova reserves the right to take measures to protect itself against Whistleblowers who knowingly submit false reports). The Report Manager may also conduct interviews or request information from other persons who may have knowledge of the reported events.

The Reported Persons are guaranteed the right of defence, within the terms of the locally applicable regulations: this may include the right to be informed about the Report within a reasonable period of time (to be determined taking into account the risk of compromising the investigation and/or the risk of destroying evidence), to be heard by the Report Manager, and to have access to the documents which concern them (without prejudice to maintaining the confidentiality of the identity of the Whistleblower or of any other third party in the absence of their explicit consent), and to be informed of the outcome of the investigation.

The presumption of innocence and honour of the Reported Persons shall always be respected. The verification phase must be completed within 3 months from the date of receipt of the Report (without prejudice to any locally applicable regulations providing for a shorter time period), unless there are justified reasons. If the investigation has not been completed by the above-mentioned deadline, the Whistleblower is nevertheless updated as to the status of the investigation, where technically possible.

4.5 Result of the Verifications

Once the verification phase is complete, the Report Manager prepares a report summarizing the investigation carried out, the methods used, the results of the plausibility check and/or investigation, the supporting evidence gathered, and recommendations for an action plan. If the Report is closed, the reasons will be stated. On the basis of the results, the report is then shared with the Managers of the departments involved (at Company, Region and/or Group level) on a “need-to-know” basis (including the possibility of sharing an anonymized version of the document) in order to determine, in consultation with the relevant departments, an action plan (where necessary) and/or any other measures to be taken (including possible disciplinary measures against employees). The Whistleblower is informed of the outcome of the investigation and of any actions planned to remedy the problem detected in the Report, insofar as this is technically possible and in accordance with locally applicable regulations. The documentation relating to each Report received, even if the investigation concludes that there is insufficient supporting evidence, is retained in accordance with confidentiality requirements within the timeframe and in the manner established by locally applicable regulations.

5 How Reports are stored

The information that the Whistleblower provides will be hosted by People InTouch, utilizing Amazon Web Services, with servers located in Frankfurt (primary) and Paris (secondary). People Intouch is based in the Netherlands and is committed to the *EU General Data Protection Regulation (GDPR)*. People Intouch has a *Privacy Information Security Management System (PISMS)* in place. This risk

and control framework is based on *ISO27001*, *ISO27002*, *ISO27701* and the *Dutch IT Auditing Privacy Standards*.

6 Reporting outside the company

Although the Whistleblower is encouraged to file any Reports internally, Nexova recognizes that the Whistleblower may have the right to file Reports with the relevant local, regional, national or international authorities, bodies or institutions, to the extent permitted by locally applicable regulations. It is up to the Whistleblower to decide whether to file a report internally or externally, or both (e.g. if an internal report is not handled properly, the Whistleblower may subsequently refer the matter to an external competent body), taking into account, also, the locally applicable regulations.

In addition, public disclosure of Breaches may be made to the extent permitted by locally applicable regulations. External reporting or public disclosure does not limit the Whistleblower's protection as defined in Section 7, subject to locally applicable regulations.

7 Protecting the Whistleblower's right to report

Protecting the Whistleblower's right to report a Breach is essential. Nexova wants to create a safe environment where the Whistleblower can report suspected Breaches within Nexova in full confidence. To this end, the following measures are taken:

- Confidential treatment of the Whistleblower's identity.
- Possibility for the Whistleblower to stay anonymous.
- Protection measures against all forms of retaliation and discrimination against the Whistleblower.

Support measures (e.g. technical advice, legal and financial assistance, social and psychological support) can also be resorted to and are foreseen by law and provided by different public entities.

The Whistleblower will be protected by these measures if they acted in good faith at the time the Report was submitted, i.e. they had reasonable grounds to believe that the information reported on the Breach was true and that the Breach fell under the scope of this Policy.

7.1 Confidentiality

In encouraging Addressees to promptly report any Breach, Nexova guarantees the confidentiality of each Report and of the information contained therein, including the identity of the Whistleblower, the Reported Person(s), the Facilitators and any other person involved. Their identities will not be disclosed to anyone other than the Report Manager or people who need to be involved, except when:

- a) They give their explicit consent, or have intentionally disclosed their identity within the context of public disclosure.
- b) Disclosure is a necessary and proportionate obligation in the context of investigations conducted by the authorities or within the framework of judicial proceedings, in accordance with locally applicable regulations. In this case, the Whistleblower must be informed in advance and given a written explanation of the reasons for the disclosure, unless the provision of such information would prejudice any legal proceedings. Following this disclosure, the Whistleblower has the right to submit objections in writing. If these objections are deemed inadequate, disclosure of the information is permitted.

All internal and external parties involved in the investigation and follow-up are bound by an obligation of confidentiality.

7.2 Anonymity

At the Whistleblower's choice, the Whistleblower can stay anonymous throughout the procedure, in which case Whistleblower's identity will not be divulged to the Report Manager.

7.3 Protection against retaliation and discrimination

Nexova will not tolerate any form of threat, retaliation or discrimination, either attempted or actual, against the Whistleblower, Facilitators, Related Persons, Reported Persons or anyone who has cooperated in the investigation to establish the validity of the Report (including their respective Related Persons).

Retaliation is defined as any act or omission caused by an internal or external whistleblowing report or a public disclosure, which causes or can cause an unjustified prejudice to the author of the Report.

Unless duly justified, the following can constitute retaliation measures:

- Employment measures, e.g. dismissal, salary reduction, refusal to grant a promotion, change of roles, disciplinary sanctions, low performance review.
- Decisions having negative consequences on work conditions, e.g. suspension of training, change of working hours, leave refusal.
- Certain behaviours, e.g. coercion, intimidation, harassment, discrimination.
- Early termination or cancelation of contract for delivery of services or products, or blacklisting of a person or company.
- Exclusion or suspension of a member or its appointed delegate.

Nexova will take appropriate measures against anyone retaliating or threatening to retaliate. If the Whistleblower or anyone having helped the Whistleblower fears retaliation measures or is under the impression to have suffered retaliation, the Whistleblower must inform the Report Manager, who will impartially assess the case and ensure that appropriate measures are taken to prevent or remediate the retaliation measures.

7.4 Protection of personal data

Personal data communicated through the reporting system, operated by People Intouch B.V., is processed by Starion Group S.A., a sister company offering Corporate services to Nexova Group S.A., acting as data controller, with registered offices at Rue des Etoiles 140, 6890 Libin, Belgium.

Starion Group S.A. collects and processes such personal data in compliance with the *EU Regulation 2016/679 (the 'GDPR')*, among other legal services provided to Nexova.

To ensure confidentiality and, as the case may be, anonymity, Starion Group S.A. has contracted People Intouch, which acts as data processor for Starion Group S.A. and sub-data processor for Nexova. People Intouch provides a secure and certified IT solution to operate Nexova's internal reporting channel.

Categories of personal data and purpose of processing

The following categories of personal data are processed to ensure the appropriate handling of Reports:

- Whistleblower's identity, role, email address and telephone number, and other data allowing identification of the author of the Report, unless the Whistleblower chose to stay anonymous.
- Information on the facts reported – including potential Breaches of the law, Breaches of codes of conducts/ethics and governing rules or other serious facts.
- Documents, data or proof collected in the course of the handling of the Report.

- Identity and conduct of all persons mentioned in the Report, other personal information likely to enable the identification, and the names of persons working in or outside Nexova who may have knowledge of the facts reported.
- In certain cases, sensitive personal data such as information on race and ethnic origin, political beliefs, religious or philosophical beliefs, trade union affiliation, health information and sexual relations or sexual orientation, and criminal records.

The purpose of the processing is to enable the implementation of an effective Whistleblowing reporting system for Whistleblowers, as required by applicable laws. By law, the processing of personal data must remain strictly limited to what is necessary for the purpose of the handling of the Reports. Starion Group S.A. does not transfer personal data outside the European Economic Area for that purpose.

Data retention

Personal data entrusted to Starion Group S.A. via the Whistleblowing Platform, which is not needed for the handling of the Report, is deleted without delay.

Any information the Whistleblower submits that is not needed will be archived, as permitted by local law and in line with our internal procedures. In addition, once the Report Manager has responded to the Report or completed any investigation, all information submitted will be anonymized, deleted and/or archived, as appropriate and permitted by local law and Starion Group S.A. internal procedures.

Reports containing information that may trigger a disciplinary, civil or criminal responsibility are stored until the corresponding procedures or statutes of limitation lapse, in compliance with applicable law.

Rights of concerned persons

Any person identified or identifiable via the data introduced in the internal Whistleblowing Platform has the following rights:

- The right to ask Starion Group S.A. to provide them with copies of personal data that it holds about them. When such access is granted, the personal data of third parties such as the author of the Report or testimonies are removed from the documents.
- The right to ask Starion Group S.A. to update and correct any out-of-date or incorrect personal data that Starion Group S.A. holds about them. For instance, a rectification can be made to the contact details of the concerned person, but no rectification can be made to the location, time or facts until a mistake can be shown.
- The right to erasure, the right to oppose to the processing of their personal data and the right to data portability within the limits afforded by data protection legislation. These rights can only be used if it does not compromise the handling of the Report.

How a Whistleblower can exercise their rights

The Whistleblower may at any time exercise the abovementioned rights in accordance with data protection regulations, by sending a request with a copy of their ID card (passport or other proof of identity) to privacy@nexovagroup.eu.

April 2024

Legal Department
Group General Counsel

Annex A

- 1) Online Whistleblowing Platform: <https://stariongroup.speakup.report/ethicsline>
- 2) Telephone number. Please use code **115790** when prompted.
 - Belgium: Freephone 0800 89 326