

Whistleblowing policy

1 Purpose

NRB (hereinafter referred to as "the Company") wants to act with integrity and ethically and therefore wants to ensure that its employees have the possibility, in accordance with the modalities and conditions set out below, to report in the most serene and confidential manner any identified or suspected breaches of statutory and regulatory rules in the Company as referred to in section **2.2** of this policy.

This policy is adopted in accordance with the Belgian Act of 28 November 2022 concerning the protection of reporting persons of breaches of Union or national law within a legal entity in the private sector, transposing the European Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

This policy aims, concerning good faith reports complying with the conditions laid down in Article 8 of the Belgian Act of 28 November 2022 as implemented by Article 3.2 of this policy, to:

- enable the confidential, if applicable anonymous, reporting of information on possible or actual breaches;
- provide protection to persons reporting a breach;
- establish the procedure to be followed by the reporting person of a breach;

This policy is available on the Company's website and intranet.

2 Scope

2.1 Personal scope

The reporting persons eligible for protection under this policy are :

- employees of the Company, former employees of the Company and candidates for recruitment to the Company ;
- persons who work or have worked on an independent basis with the Company and candidates for independent cooperation in pre-contractual negotiations;
- volunteers and trainees (paid or unpaid);
- shareholders and persons belonging to the administrative, management or supervisory body of the Company (including non-executive members);
- any person who works or has worked under the supervision and direction of contractors, subcontractors and/or suppliers of the Company;

The protective measures referred to in this policy shall apply in addition to:

- facilitators, i.e. natural persons who assist a reporting person during the reporting process and whose assistance should be confidential;

- third parties who are connected to the reporting persons and who could be at risk of retaliation in a professional context, such as colleagues or relatives of the reporting persons;
- legal entities owned or worked for by the reporting persons, or with which they are connected in a professional context.

The facilitators, third parties and legal entities referred to above may, however, only benefit from the protection afforded by this policy if they had reasonable grounds for believing that the reporting person himself/herself fell within the scope of protection of this policy.

All the above-mentioned persons shall only benefit from the protection provided by this policy if their report complies with the conditions laid down in Article 8 of the Belgian Act of 28 November 2022 as implemented by Article 3.2 of this policy, and therefore in particular if their report was made in good faith.

2.2 Material scope

Breaches¹ that are subject to reporting under this policy are those relating to the following areas:

- Public procurement;
- Financial services, products and markets, prevention of money laundering and terrorist financing;
- Product safety and product compliance;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, and security of network and information systems;
- Prevention of tax fraud;
- Prevention of social fraud .

3 Report

3.1 Purpose of the report

Reporting persons may report, i.e. communicate in writing or orally, through one of the channels referred to below any violations relating to the areas referred to in point **2.2** as well as any information on such violations, including reasonable suspicions of actual or potential violations that have occurred or are very likely to occur within the Company as well as attempts to conceal such violations within the Company.

¹ Defined by Article 7 of the Belgian Act of 28 November 2022 as, among other things, an unlawful act or omission or an act or omission that defeat the object or purpose of a rule.

3.2 The conditions for protection of reporting persons

The report must be made in good faith and must not be based on unsubstantiated rumors or hearsay nor must the report aim to harm the Company.

Reporting persons are granted the protection of this policy provided that :

1. they had reasonable grounds to believe that the information reported on the violations was true at the time of reporting and that the information fell within the scope of the Act; and
2. they made an internal report, an external report or a public disclosure in accordance with the conditions of this policy and the Act.

The first criterion is assessed in comparison with a person placed in a similar situation and with comparable knowledge

The reporting person who made a report in good faith does not lose the benefit of the protection solely because the report turned out to be inaccurate or unfounded.

The purpose of this policy is to protect the Company from malicious, fraudulent, fanciful or abusive reporting and from any use of this policy to harm the Company or its business.

4 Reporting channels

Any person referred to in point **2.1** paragraph 1 of this policy who has information relating to breaches referred to in point **2.2** is invited to report it to the Company as soon as possible, provided that the report is made in good faith and complies with the conditions laid down in Article 8 of the Belgian Act of 28 November 2022 as implemented by Article 3.2 of this policy.

4.1 Internal reporting channels

The internal reporting channel is *a priori* the most appropriate channel when it is possible to remedy the violation effectively within the Company.

This channel is therefore to be privileged by the reporting person, in compliance with the provisions of this policy.

4.1.1 Recipients of internal reporting channels

The internal reporting channels set up by the Company and detailed in section **4.1.2** of this policy are open to the Company's employees, as well as to the persons listed in section **2.1**.

4.1.2 Procedure

1- Within the Company, internal reports can be made by e-mail to lanceur.alerte@nrb.be or Whistleblowing@nrb.be

Reports must be submitted in French, Dutch or English. Any report submitted in another language must be translated, which could alter the accuracy of the content of the report.

It is also possible to request a face-to-face meeting with the Report Manager as mentioned below in section **4.1.3** of this policy.

Each of the above mentioned channels is designed, established and operated in a secure manner that ensures the confidentiality of the identity of the reporting person and any third parties mentioned in the report is protected. Access to the channels is strictly limited to employees who have access to them based on responsibilities and/or powers.

These channels ensure at all times the protection of the privacy and personal data of the reporting person and of any third person mentioned in the report.

These channels are managed by a Report Manager, whose identity is mentioned below under point **4.1.3** of this policy.

2- Following the introduction of a report through one of the above-mentioned channels, the reporting person will receive an acknowledgement of receipt of the report within 7 days of its receipt.

3- The Report Manager will ensure both the receipt and the follow-up of the report and maintain communication with the reporting person. If necessary, the Report Manager will ask the reporting person for any additional information needed to investigate the report.

4- The Report Manager will diligently follow up on the report by means of an internal investigation in order to assess the accuracy of the allegations made in the report and, if necessary, to remedy the reported violation.

In all cases referred to him/her, the Report Manager will provide feedback to the reporting person, i.e. communication to the reporting person on the measures envisaged or taken as a follow-up and the reasons for such follow-up.

The above-mentioned feedback shall take place within a reasonable period of time, which shall in any case not exceed 3 months from the acknowledgement of receipt of the report.

The Report Manager will inform the reporting person through the chosen internal reporting channel.

4.1.3 Report Manager

The Company has entrusted the task of monitoring internal reports to :

- Aurélie VERJUS, Compliance Officer
- Francis OUAAÏ, Data Protection Officer

The Report Manager shall perform his/her duties independently and without any conflict of interest. He/she is subject to a duty of confidentiality.

4.2 External reporting channels

The Federal Coordinator is designated by the Belgian legislator with coordinating reports introduced via external channels.

He/she is responsible for receiving external reports, checking their admissibility and forwarding them to the competent authority for investigation, which will be different depending on the subject of the report. The list of competent authorities is set out in the Royal Decree of 22 January 2023 implementing the Act of 28 November 2022.

In exceptional cases, the Federal Coordinator may also conduct the investigation in depth.

The Federal Coordinator's contact details are as follows:

Address :	Rue de Louvain 48 bte 6, 1000 Bruxelles
Online complaint:	https://www.mediateurfederal.be/fr/contactez-nous
E-mail :	contact@mediateurfederal.be
Téléphone :	0800 99 961
Fax :	02 289 27 28

4.3 Public disclosure

Public disclosure is the making of information on breaches available in the public domain.

This public disclosure can firstly be used by any reporting person who first made an internal and external report, or directly an external report, but no appropriate action has been taken in response to the report within the prescribed timeframe (3 months in case of an internal report).

A person may have direct recourse to public disclosure as defined above when he or she has legitimate reasons to believe that :

- the breach may constitute an imminent or manifest danger to the public interest ; or
- in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

5 Protective measures

The Company is committed to making every effort to provide appropriate and effective protection to reporting persons whose reporting in good faith complies with the conditions laid down in Article 8 of the Belgian Act of 28 November 2022 as implemented by Article 3.2 of this policy.

5.1 Duty of confidentiality

The Company guarantees to do everything in its power to ensure that the reporting person can report in complete confidentiality.

The Company also undertakes to take all necessary measures to ensure that the identity of the reporting person cannot be disclosed without the reporting person's express and free consent to any person other than the authorised staff members competent to receive or follow up on reports.

By way of derogation from the previous paragraph, the identity of the reporting person of any other information may be disclosed where this is a necessary and proportionate obligation imposed by national authorities or in the context of judicial proceedings, including with a view to safeguarding the rights of defence of the person concerned.

In the latter case, the reporting person will be before his or her identity is disclosed, unless such information would jeopardize the related investigations or judicial proceedings. This is the case, for example, if the reporting person represents an important witness in court or in cases of unjustified or unlawful reporting to protect the person's defence rights.

5.2 Prohibition of retaliation

1- Any form of retaliation against the persons referred to in Article **2.1** that are entitled to protection under this policy, including threats of retaliation and attempts of retaliation, is prohibited

2- Any person benefiting from the protection against retaliation referred to under this point who believes that he or she has been the victim of, or is threatened with, such retaliation may submit a motivated complaint to the Federal Coordinator, who will initiate an extrajudicial protection procedure and verify the existence of reasonable suspicion of retaliation.

The Federal Coordinator's contact details are as follows:

Address :	Rue de Louvain 48 bte 6, 1000 Bruxelles
Online complaint:	https://www.mediateurfederal.be/fr/contactez-nous
E-mail :	contact@mediateurfederal.be
Telephone :	0800 99 961
Fax :	02 289 27 28

3- Any person benefiting from the protection against retaliation referred to herein who is the victim of such retaliation when the report made in good faith complies with the conditions set out in Article 8 of the Act of 28 November 2022 as implemented by Article 3.2 of this policy may request damages in accordance with the provisions of the law concerning contractual or extra-contractual liability, the amount of which varies from 18 to 26 weeks' remuneration. This compensation cannot be cumulated with the compensation applicable in cases of manifestly unreasonable dismissal, in accordance with CLA no. 109 concerning the motivation of dismissal.

If the person concerned is not an employee of the Company, the compensation will be set at the actual loss suffered, the extent of which must be proven by the victim.

4- To this end, persons who consider themselves to be victims of a retaliatory measure may take action before the Labour Court with territorial jurisdiction, if necessary in summary proceedings.

5.3 Measures of support

The Company wishes to ensure that the persons falling within the scope of this policy, as listed in section 2.1 of this policy, receive consistent and high quality support.

In addition to the support they can obtain internally, the Company specifies in this context that these persons can, if they wish, obtain information and advice on the applicable procedures from the following external bodies :

1° The Federal Coordinator

Address :	Rue de Louvain 48 bte 6, 1000 Bruxelles
Online complaint:	https://www.mediateurfederal.be/fr/contactez-nous
E-mail :	contact@mediateurfederal.be
Téléphone :	0800 99 961
Fax :	02 289 27 28

2° The Federal Institute for the protection and promotion of Human Rights

Address :	Rue de Louvain 48, 1000 Bruxelles
E-mail :	info@firm-ifdh.be
Website:	https://institutfederaldroitshumains.be/fr

5.4 Liability exemption

Reporting persons who make an internal/external report or public disclosure in good faith that complies with the conditions laid down in Article 8 of the Act of 28 November 2022 as implemented by Article 3.2 of this policy shall not incur any liability in relation to that report or public disclosure provided that they had reasonable grounds for believing that the report or public disclosure of such information was necessary to reveal a breach in accordance with this policy.

Any other liability, if any, of the Reporting Persons arising out of acts or omissions not related to the reporting or public disclosure or not necessary to disclose a breach in accordance with this Policy shall continue to be governed by applicable law.

6 Processing of personal data

In the context of the internal reporting procedure, the Company is considered to be the data controller of the personal data processed in the framework of the internal reporting procedure. In this regard, we refer to the Privacy Policy for more information on the processing of personal data by the Company.

In the context of the external reporting procedure, the Company cannot be considered as the data controller: it will be the competent authority or, if there is no competent authority, the Federal Coordinator.

Any processing of personal data carried out pursuant to this policy will be carried out in accordance with the applicable personal data protection laws, including the European General Data Protection Regulation ("GDPR").

Personal data which are manifestly not relevant for the handling of a report shall not be collected or, if accidentally collected, shall be deleted without undue delay

7 Record keeping of reports

1- The Company keeps records of all reports received, in compliance with the confidentiality requirements provided in section **5.1** of this policy.

Reports will be kept for 5 years after the contractual relationship between the reporting person and the Company has ended. As regards third parties to the Company, reports will be kept for 5 years.

2- Where an individual requests a meeting with the Company's staff to make an internal or external report, the Company will ensure, with the consent of the reporting person, that complete and accurate records of the meeting are kept in a durable and retrievable form.

8 Staff training

The Company organises training to ensure that staff members responsible for handling reports are sufficiently aware of the applicable data protection rules, to handle reports and to ensure communication with the reporting person, as well as to ensure appropriate follow-up of reports.

9 Modification of this policy

The Company reserves the right to amend this policy at any time, at its sole discretion, in line with changes in relevant legislation and the Company's operational requirements.

Any such changes will be communicated to current or future employees and any person in a contractual relationship with the Company by adapting this policy, which is available on the Company's intranet and website.

10 Entry into force

This policy is effective from 15 February 2023 for an indefinite period.