proximus

Group Compliance

Whistleblowing procedure

Latest review	12/09/2024
Owner	Maurizio Carlone – Manager Group Compliance
Contact	group.compliance@proximus.com

Table of content

1. What is a whistleblower ?

Whistleblowers are **people**, who work for an organization or are in contact with an organization as part of their professional activities, **who come forward to report wrongdoing they encounter in the context of their work.**

Whistleblower reports are important because they can lead to the effective detection, investigation and follow-up of wrongdoing and/or violations of the code of conduct, internal policies and procedures, laws and regulations that would otherwise remain hidden. Whistleblowers thus help to build and secure the future of the Proximus Group, mitigating the risk of reputational damage and limiting financial losses.

2. Legislative framework and scope of application

European and Belgian legislation has recently strengthened the legal framework for whistleblowing and the protection of whistleblowers. In order to comply with these laws, the Proximus Group Compliance Office has adapted the **whistleblowing system** already in place to the new legislation, in a harmonized way for the entire Proximus Group. This system **enables employees and external parties to report confidentially, and anonymously for those who wish to do so, any violation not only of the Code of Conduct, internal policies and procedures, laws and regulations, but also any breach of integrity** (see point 4).

Entity	Proximus SA	Belgian affiliates of Proximus SA (>50% and more than 50 FTE)	Foreign affiliates of Proximus SA (>50%)
Legislative framework	Law of December 8, 2022 on the protection of whistleblowers in the **public sector**[1]	Law of November 28, 2022, on the protection of whistleblowers in the **private sector**[2]	**Local law** of the country where the company is based
« Internal » whistleblowing channels	Compliance manager of the entity by : - e-mail - Phone - Postal mail	Compliance manager of the entity by : - e-mail - Phone - Postal mail	Compliance manager of the entity by : - e-mail - Phone - Postal mail
« External » whistleblowing channels	Federal Ombudsman	Federal Ombudsman	Cfr local law
Investigation of whistleblowing cases[3]	Compliance manager of the entity	Compliance manager of the entity	Cfr local law
Role of the Group Compliance Office	Consulting, expertise and reporting	Consulting, expertise and reporting	Consulting, expertise and reporting

[1] Public sector law
[2] Private sector law
[3] If the management of a whistleblowing channel is outsourced to a third party, the Compliance manager of the concerned Proximus Group entity remains fully accountable.

3. Who can report a concern?

This procedure is applicable to **any person who has acquired information about wrongdoing in a professional context within the Proximus Group**. Such persons may be employees, former or future employees, contractors, suppliers, shareholders or members of the administrative, management or supervisory bodies of a company, including non-executive directors, volunteers and paid or unpaid trainees.

4. What types of concerns can be raised?

The report must directly concern the activities of Proximus or one of its affiliates and may not relate to personal disputes that have nothing to do with the acts listed in this procedure or to accusations that you know to be false.

To benefit from the protection referred to in point 6, the report **must relate to one of the following elements:**

Proximus SA	**Belgian affiliates of Proximus SA (>50% and more than 50 FTE)**
(i) The performing or omission of an act which constitutes a threat to or an infringement of the general interest, and which : - constitutes a violation of directly applicable European provisions, Belgian norms and Proximus SA's internal policies and procedures; - involves a risk to the life, health or safety of persons or the environment; and/or - is evidence of a serious breach of the professional obligations or proper management of a federal public sector body. (ii) Knowingly instructing or advising others to commit a breach of integrity as described above.	(i) Violations of directly applicable European provisions or Belgian norms relating to the following areas: - public procurement ; - financial services, products and markets and prevention of money laundering and terrorist financing; - product safety and conformity; - transport safety; - environmental protection; - 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 networks and information systems; - combating tax fraud; - combating social fraud. (ii) violations affecting the financial interests of the European Union. (iii) violations relating to the European Union's internal market, in which the free movement of goods, persons, services and capital is guaranteed, including violations of the Union's rules on competition and state aid.

Do not use the reporting channels described in this procedure to report an immediate threat to life, health and safety or property, or for grievances you may have regarding your working conditions.

Please note that **complaints relating to the following** should not be made through the reporting procedure described here (internal or external), but **according to other more specific procedures under which you will also benefit from specific protection**:

- **Violence, moral and sexual harassment in the workplace**. These types of complaints should be addressed to your organization's contact person or to the Prevention Manager (Law of August 4, 1996, on the well-being of workers in the exercise of their profession);

- **Discrimination**. Complaints about discrimination should be addressed to Unia (Interfederal Center for Equal Opportunities) or the Institute for the Equality of Women and Men (anti-discrimination laws), as appropriate[4].

5. How to raise a concern?

Each Proximus Group entity has an internal whistleblowing channel in addition to the external whistleblowing channel provided for by law.

The law guarantees a free choice between these two channels. We recommend, but are in no way require, that you start with the internal channel, before moving on to the external one. By using the internal channel, the problem can be effectively handled internally by the Compliance manager of the entity concerned. This enables remedial action to be taken as quickly as possible.

5.1 Internal whistleblowing channels

If you become aware of a breach of integrity, as set out above (see point 4) you can report the problem or breach directly using one of the **following whistleblowing channels so that your report is treated confidentially, and your legal protection assured**:

By a tool managed by an external independent supplier, Grant Thornton, through the following URL

https://proximus.grantthornton-whistle.com/en/home

By phone (Monday to Friday 09:00 to 17:00) : +32 (0) 800 45 002

By postal mail to (please clearly indicate « confidential » on the envelope)

- **Compliance manager of the Groupe Proximus** : Proximus – Maurizio Carlone, Group Compliance, 27 Boulevard du Roi Albert II, B 1030 Bruxelles
- **Chairperson of the Audit and Compliance Committee**: Proximus – Catherine Vandenborre, Chairwoman of the Audit and Compliance Committee, 27 Boulevard du Roi Albert II, B 1030 Bruxelles.

By making an **appointment** with the Compliance manager or the Chairperson of the Audit and Compliance Committee by phone or e-mail.

[4] The Law of May 10, 2007, designed to combat certain forms of discrimination; the law of May 10, 2007, designed to combat discrimination between women and men; the law of July 30, 1981, designed to punish certain acts inspired by racism or xenophobia.

5.2 External whistleblowing channel

An external whistleblowing channel has been assigned by the Belgian government, namely the **Federal Ombudsman's Centre for Integrity** which you can contact as follows :

Online : Reporting integrity violations or breaches of law | Federaalombudsman.be

By phone : Monday to Friday from 9.00 to 12.30 and from 13.30 to 17.00 :

- From Belgium (toll-free number) : 0800 99 961
- From abroad +32 2 289 27 27

By e-mail : contact@mediateurfederal.be

5.3 Federal Institute for Human Rights (FIRM/IFDH)

The Federal Institute for Human Rights is the central information point for the protection of whistleblowers. It is responsible for applying or ensuring the application of support measures to which whistleblowers are entitled. These include :

- full, independent information and advice, which is easily accessible to the public and free of charge, on the procedures and remedies available, on protection against reprisals, and on the rights of the person concerned, including his or her personal data protection rights;
- technical advice before any authority involved in the protection of the whistleblower;
- legal assistance as well as legal advice or any other legal assistance, such as second-line legal aid and legal aid, in criminal and civil proceedings, in accordance with articles 495, paragraph 3, 508/7 to 508/25, 664 to 699ter, and 1723/1 to 1737 of the Judicial Code, article 47bis of the Code of Criminal Investigation, articles 2bis, 16 and 24bis/1 of the law of July 20, 1990 on preventive detention, and articles 10/1, 10/3 and 34/1 of the law of December 19, 2003 on the European arrest warrant;
- support measures, including technical, psychological, media and social support ;
- financial assistance for people who have issued alerts in connection with legal proceedings.

Contact of the Federal Institute for Human Rights:

By phone : 0479/88.57.23 (in French or Dutch)

By email : kl-la@firm-ifdh.be

By postal mail : Institut Fédéral des Droits Humains (IFDH), Rue de Louvain 48, 1000 Bruxelles

https://federaalinstituutmensenrechten.be/en/do-you-have-any-questions-contact-us

5.4 Remaining anonymous

You can file a report anonymously. This means that the recipient of the complaint will not know your identity. To do this, you can **use the web tool managed by Grant Thornton or send your complaint by letter**. If you file your complaint by letter, we insist that you mark CONFIDENTIAL on the envelope so that your letter can be handled confidentially by our internal postal services.

An anonymous report can only be considered valid if it contains sufficient factual elements to enable the facts to be investigated. Therefore, please **include as much details as possible** in the interest of successful investigation and follow-up of an anonymous report.

The law foresees the filing of anonymous reports. However, we strongly recommend that you state your identity when reporting a problem. Confidentiality is guaranteed. Anonymity can make communication between the person reporting and the person to whom the report is addressed more difficult. Being able

to contact you for further information may be necessary for a diligent follow-up and information verification, as well as for your protection (or for the protection of other concerned parties).

5.5 Follow-up

Once you have made a report using the internal channel, you will receive an **acknowledgement of receipt within 7 calendar days** (maximum).

The person responsible for following up on your report will record it in a separate register. He or she will initiate a preliminary investigation to check whether the concern falls within the scope of the law and appears to be well-founded. This person will also stay connected with you and, if necessary, ask for further information.

You will be **informed within a maximum of 3 months (after acknowledgement of receipt) of the action taken** on the alert.

The identity of the whistle-blower will always be kept confidential.

5.6 Duty of Confidentiality

When you report a problem, the secrecy of your identity as a whistleblower will be guaranteed in accordance with applicable laws and regulations.

Your identity will not be disclosed without your explicit consent, other than to those authorized and competent to receive and follow up reports. This also applies to any other information from which your identity can be (in)directly deduced.

Only if there is a necessary and proportionate obligation imposed by European or national law in the context of investigations by national authorities or legal proceedings may your identity or information from which it can be deduced be disclosed, including to safeguard the rights of defense of the person concerned.

Please bear in mind that an anonymous report will only be considered valid if it contains sufficient factual elements to enable the facts to be investigated. Therefore, please include as much detail as possible in the interests of the investigation (see point 5.4).

Within the framework of this policy, Proximus and its subsidiaries may collect personal data based on the obligations imposed on it by the European directive and national laws, in strict compliance with the General Data Protection Regulation (GDPR), and only to the extent necessary for the purposes of the investigation and the taking of corrective measures. All personal data collected as part of this procedure will be processed as explained in point 8 below.

6. Protection of the whistleblower

The law has strengthened the protection of whistleblowers against reprisals and the severity of sanctions against those who take reprisals. No whistleblower who reports an event based on reasonable grounds may be subject to retaliation (e.g. be penalized or subjected to any discriminatory measure) for having reported an alert via the whistleblower mechanisms. **The Proximus Group prohibits and sanctions all forms of retaliation against those who, in good faith, report a violation or suspected violation.**

If you report a problem and it turns out that you were genuinely mistaken, you will not be punished. Protective measures also extend to facilitators and third parties with a professional or family link to the whistleblower.

If, because of your whistleblowing, you feel threatened or subject to reprisals, we invite you either to reintroduce a report to the internal reporting channel, or to introduce a report directly to the external reporting channel, one of whose statutory missions is to offer you protection against reprisals. You can also ask the FIRM/IFDH[5] for assistance in this process (see point 5.3).

7. Control plan

The Group Compliance Office will develop a dedicated control plan to verify the correct application of this procedure in the Group.

8. Processing of personal data

This section describes how the entities of the Proximus Group process your personal data in their capacity as data controller in the context of this whistleblowing procedure. This information is intended for all whistleblowers and anyone who is the subject of a report.

- **Categories of personal data**: We may collect and process the following categories of personal data when a report is made via the whistleblowing channels described in this policy:
    - the identity, functions and contact details of the whistleblower (in compliance with the confidentiality rules mentioned in section 5.4), of the persons mentioned in the report and of the persons involved in receiving and following up the report; and
    - the events reported, the information gathered during the investigation, and any action taken because of the investigation, as far as this information relates to personal data.
- **Purposes**: We process the above-mentioned personal data for the purposes of managing reports and detecting, investigating and following up wrongdoings or violations of the code of conduct, internal policies and procedures, laws and regulations.
- **Legal basis**: As explained in section 2 of this procedure, we have a legal obligation to make reporting channels available for certain types of offences. Where reporting falls within the scope of this **legal obligation**, it is on this legal basis that we will process the data. For all other reporting, we rely on our **legitimate interests** in ensuring that the conduct of our employees complies with legal requirements, industry standards and Proximus internal policies and standards.
- **Recipients of the data**: Only those persons authorized and competent to receive and follow up reports within the Proximus Group have access to the above-mentioned personal data. Only if we are legally obliged to do so may this data be communicated to national authorities or legal enforcement proceedings.
- **Data retention**: Personal data obtained in connection with a report is retained for as long as necessary to process the report, including any consequences thereof, such as legal action. Personal data that is clearly not relevant to the processing of a specific alert is not collected or, if collected accidentally, is deleted without delay. The name, position and contact details of the whistleblower and of any person to whom the protection and support measures extend, as well as of the person concerned, including,

[5] FIRM-IFDH (federalinstitutehumanrights.be)

where applicable, his or her company number, are stored until the reported violation is time-barred. As far as Proximus SA is concerned, it will only keep personal data relating to the reports it receives for the duration of the investigation, unless legal proceedings or disciplinary measures are initiated against the person concerned, the person who filed the report or any other person involved in the case. In such cases, Proximus will keep the personal data until the proceedings in question are closed and the time limits for lodging an appeal have expired.

- **Your rights** :
  - Right of access: You have the right to ask us about the personal data we hold about you. We can provide you with a copy free of charge, but this is not possible for all documents. This is because we also want to respect the rights and freedoms of others.
  - Right of rectification: Do you think your data is inaccurate or outdated? You have the right to ask us to correct it.
  - Right to object: Under the conditions laid down by law (Article 21 of the GDPR), you have the right to ask us to stop processing your personal data.
  - Right to limit processing: You can ask us to limit the processing of your personal data, for example when we verify the accuracy of your personal data.
  - Right to be forgotten or to have your personal data deleted: Under the conditions laid down by law (Article 17 of the GDPR), you have the right to ask us to delete your personal data.

  You can exercise your rights by contacting the Proximus Data Protection Officer: privacy@proximus.com. You also have the right to lodge a complaint with the competent supervisory authority. In Belgium, this authority is the Data Protection Authority:
  - Rue de la Presse 35, 1000 Brussels
  - +32 (0)2 274 48 00
  - contact@apd-gba.be

  Please note that, insofar as the exercise of your rights set out in Articles 14 (right of information where personal data is not collected from the data subject), 15 (right of access) and 16 (right of rectification) of the GDPR may hinder, prevent, obstruct or delay the follow-up of the alert or requests for protection or identification of the authors of the alert, it is possible for Proximus SA to derogate from these rights. Despite these restrictions, you retain the right to take legal action in accordance with Article 79 of the GDPR and to lodge a complaint with the supervisory authority in accordance with Article 77 of the GDPR.