Moore Whistleblower Policy

CONTENTS

The significance of this policy:

This document represents the policy adhered to by Moore Belgium, registered in the Register of Legal Entities under number 0406.878.277, registered office at 1020 Brussels, Esplanade 1, box 96, and by its affiliated companies. The Moore group companies hereinafter referred to as 'Moore'. Moore can, at its unilateral initiative, amend this policy based on legislative changes and changes to its policy, without such being deemed unlawful. Employees shall be informed in good time of any such amendments.

1. Introduction

a. This policy has been drawn up in order to comply with the applicable laws and legislation that deal with protecting whistleblowers, specifically:

- 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;
- The Law of 28 November 2022 on the protection of reporters of breaches of Union or national law within a private sector legal entity (hereinafter referred to as the Whistleblower Protection Act).

b. Through this policy, Moore aims to provide **transparency** to its staff and to other parties with regard to the existing channels for reporting (potential) irregularities within Moore. Thus, Moore hopes to lower the threshold for reporting malpractice. Furthermore, this policy aims to **protect** the whistleblower or reporter. Moore guarantees its staff that an independent and confidential investigation will be conducted in the wake of any such reports.

c. In itself, **no obligation to disclose** malpractice is imposed on Moore staff and/or other parties under this policy – the opportunity to report any wrongdoing is provided, while no obligation whatsoever exists for doing so.

2. Definitions

‘Breaches’: acts or omissions that are unlawful, fall within specific domains and that contravene the objectives or the application of the rules within these domains;

‘Information on breaches’: information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur, and attempts to conceal such breaches;

‘Report’ or ‘to report’: the oral or written communication of information on breaches;

‘Internal reporting’: the oral or written communication of information on breaches within a private sector legal entity;

‘External reporting’: the oral or written communication of information on breaches to the federal coordinator or the competent authorities;

‘Public disclosure’ or ‘to publicly disclose’: making information on breaches available in the public domain;

‘Reporting person’: a person who reports or publicly discloses information on breaches;

‘Work-related context’: current or past work activities in the private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;

‘Facilitator’: a natural person assisting a reporting person in the reporting process in a work-related context, and whose assistance must be confidential;

‘Person concerned’: a natural or legal person referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated;

‘Retaliation’: any direct or indirect act or omission occuring as a result of internal or external reporting or by disclosure and which causes or may cause unjustified detriment to the reporting person;

‘Anonymous report’: a report made where no one, not even the recipient, is aware of the identity of the reporting person;

‘Reporting manager’: the impartial person or department authorised to follow up on the reports, communicate with the reporting person, request further information from that reporting person, where necessary, provide feedback and, where applicable, receive reports.

3. Scope

3.1. What issues can be reported?

a. Breaches or information concerning **the following matters** can be reported using the reporting channel Moore has made available on its intranet (Touch):

- public procurement;
- financial services, products and markets, prevention of money laundering and financing of terrorism;

- product safety and compliance;
- transport safety;
- protection of the environment;
- radiation protection and nuclear safety;
- food and feed safety, animal heal and animal welfare;
- public health;
- consumer protection;
- protection of privacy and personal data and security of network and information systems;
- the financial interests of the EU are threatened or the internal market is disrupted;
- combatting tax evasion;
- combatting social security fraud.

b. What **does not fall within the scope** of the Whistleblower Policy:

- complaints concerning violence, bullying and sexual harassment;
- reports concerning information covered by medical professional privilege;
- complaints concerning the services provided by Moore (such as invoice queries);
- complaints concerning an individual's employment (unpaid salaries, incorrect salaries, an obligation to work overtime, a prohibition on working on Sundays and public holidays, unsafe or unhealthy working conditions, etc) that does not relate to social security fraud.

In order to report any of the above issues, you can use the existing channels such as, depending on the issue to be reported, your confidential advisor as listed in the company rules and regulations, HR or a client's account manager.

3.2. Who can report?

All staff, contractors and third parties affiliated with Moore and who have obtained information on breaches in a **work-related context** can report an issue. This includes, among others, **the following persons**:

- staff;
- a subcontractor's staff;
- freelancers;
- shareholders or directors;
- interns;
- volunteers who, in a work-related context, have obtained information on breaches;
- former members of staff;

- job applicants.

4. Avenues for reporting

A reporting person has **three different options** for reporting an issue. While it is not required, Moore believes it is best to first use the internal reporting channels.

4.1. Internal reporting

The **internal reporting channel** is a **Whistleblower Software** web-based app and reporting platform provided by an external company that you can use to make a **written or oral** report as **a reporting person**. Moore and its affiliated companies work together to manage, investigate and follow up on any reports. When making a report, you are asked from which Business Unit the report originates or which Business Unit it concerns. The phrase 'Business Unit' is not a legal term but is used within Moore to specify the department in which a given activity is performed.

The in-house **position of reporting manager** is held by Irene Timmermans of the Accountancy Business Unit. If a report concerns the prevention of money laundering and financing of terrorism, then the reporting manager has the right to notify Moore's AMCLO (the internal coordinator for anti-money laundering legislation) and/or the most senior person in respect of the application of anti-money laundering laws. For all other reports, the reporting manager will work with the designated persons in the Business Unit concerned for the purpose of their investigation. In the event of ambiguity or of additional questions being raised with regard to the report, the reporting manager could ask for further information from the reporting person. The reporting person also has the option to contact the reporting manager at any time to discuss the report.

The anonymity of the reporting person and of their report is guaranteed at all times.

4.2. External reporting

Aside from the internal reporting channel, a reporting person can also use an external reporting channel. While it is not required, it is still preferred that a person only uses the external channel after first making a report via the internal channel. A reporting person

can, therefore, also make a report directly to one of the designated authorities – agencies that can receive reports, provide feedback and follow up on them.

At the request of the reporting person, these agencies will support the persons concerned with respect to all administrative or judicial bodies that play a role in protecting them against retaliation and, in that regard, can specifically confirm that the reporting person has made a report in accordance with the law.

The competent government agencies are:

Public procurement	The Public Procurement Agency from the FPS Chancellery of the Prime Minister
Financial services, products and markets, prevention of money launder and terrorism financing	The FSMA is responsible for the rules within the meaning of article 45 of the Law of 02 August 2002, the NBB covers those rules referred to in articles 12*bis* and 36.2 of the Law of 22 February 1998 and the Audit Oversight Board deals with those rules within the meaning of article 32 of the Law of 07 December 2016
Product safety and product compliance	The FPS Economy, FPS Public Health, the Federal Agency for Medicines and Health Products, the Belgian Institute for Postal Services and Telecommunications and the FPS Mobility and Transport
Transport safety	The FPS Mobility and Transport and the National Authority for Maritime Security
Protection of the environment	The FPS Public Health, Food Chain Safety and Environment, Brussels Environment, the Commission for Electricity and Gas Regulation, the Directorate-General for Energy and the

	Agency for the Cooperation of Energy Regulators
Radiation protection and nuclear safety	The Federal Agency for Nuclear Control
Food and feed safety, animal heal and animal welfare	The Federal Agency for the Safety of the Food Chain, the FPS Public Health, Food Chain Safety and Environment
Public health	Sciensano, the FPS Public Health, Food Chain Safety and Environment, the Federal Agency for Medicines and Health Products and the Patients' Rights Federal Commission
Consumer protection	The FPS Economy
Protection of privacy and personal data and security of network and information systems	The data protection authority, the Belgian Centre for Cybersecurity and the European data Protection Supervisor

In the absence of an applicable designated agency, the Federal Ombudsman acts as the competent authority. You can contact this agency as follows:

- Using the reporting form: https://www.federaalombudsman.be/en/whistleblower-reporting-form
- By email: integrity@federalombudsman.be
- By appointment: send an email to integrity@federalombudsman.be or call 0800 999 61 to make an appointment with a member of staff at the Centre for Integrity.

4.3. Public disclosure

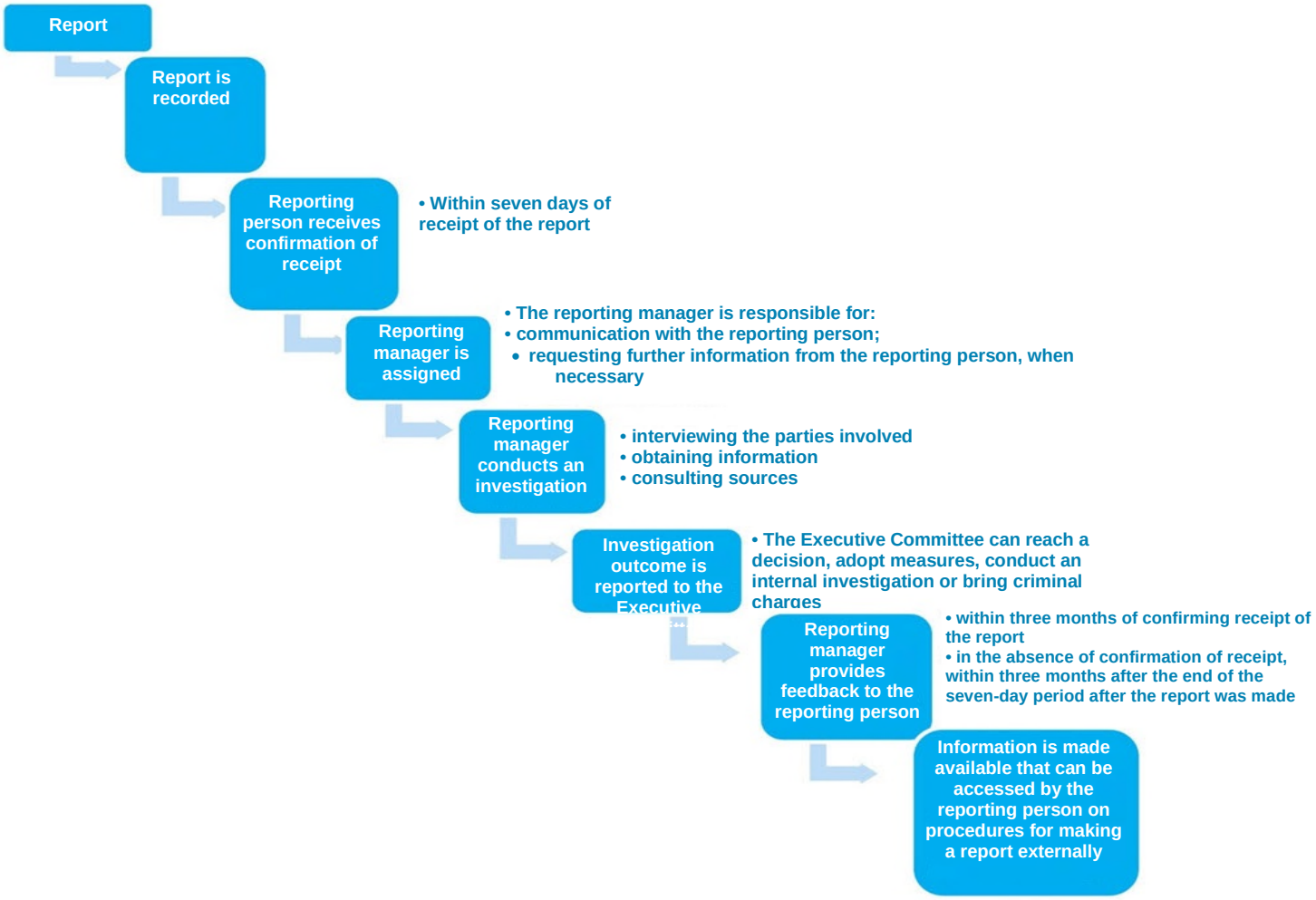
Protection of a reporting person making a public disclosure is only available in specific cases. First, the reporting person must have first made an internal or external report, or immediately made an external report, after which no appropriate measures were taken

within the stated period. The reporting person must also have well-founded reasons for believing that:

- the breach could be a potential or actual danger in the public interest; or
- there is a risk of retaliation when making a report externally; or
- there is only a small chance that the breach will be remedied, due to the special circumstances of the matter (for example, evidence could be withheld or destroyed, etc).

5. Course of the investigation after a report is made internally

The procedure that is triggered after a report is received can be represented as follows:



1. The reporting person makes a **report** using the designated channel.
2. The **report** is recorded by the platform together with the date on which the report was made.
3. Within seven days of receipt, the reporting person receives **confirmation of receipt** of the report.
4. After receipt of the report, the **reporting manager is assigned**. This person is responsible for communicating with the reporting person and conducting the investigation.
5. During their **investigation**, the reporting manager shall verify the accuracy of the claims made in the report, follow up on the report and, where necessary, tackle the reported breaches.

   The reporting manager is authorised, in their capacity as reporting manager, to launch an independent investigation, and can:

   - interview the persons involved;
   - obtain information;
   - consult sources.

   Based on the investigation, the reporting manager must verify the accuracy of the claims made in the report. While obtaining information, the anonymity of the persons concerned is safeguarded.
6. The **reporting manager shall present their written findings to the Executive Committee**. However, if the report concerns a member of the Executive Committee, then the report will be addressed to the chairperson of the Executive Committee. The Executive Committee reaches a decision and adopts measures based on the reporting person's report. Depending on the findings of the reporting manager, an internal investigation can be launched or Moore can file a criminal complaint.
7. Once the investigation is finalised, the reporting manager provides **feedback** to the reporting person with respect to the planned follow-up and the associated reasons, the measures adopted in order to verify the accuracy of the claims and the measures adopted to tackle the breach. Both the reporting person and the persons concerned are informed of the conclusion of the investigation. The

reporting person will receive a message that the feedback is ready and available for them to read on the platform. This will happen no later than three months after confirmation of receipt or three months after the end of the seven-day period after the report.

6. Confidentiality and protection of personal data

The report and handling of a report are always conducted with respect for **secrecy and confidentiality**.

The **details of the reporting person are kept confidential**. The reporting person is also given the opportunity to make a report anonymously. Moreover, **unauthorised staff** do not have access to the internal reporting channel.

Furthermore, the **identities of the reporting person and the other persons concerned** (the facilitator, other persons associated with the reporting person who could be the victim of retaliation in a work-related context) are kept confidential. The same applies to all other information that can be used to directly or indirectly infer the identity of the reporting person. The identities of the reporting person and the other persons concerned are known only to the reporting manager, unless the reporting person has granted the reporting manager written permission to divulge such. The obligation to maintain confidentiality with respect to the other persons concerned no longer applies once the investigation is concluded.

In return for this secrecy and confidentiality, the reporting person is required to **treat their report as confidential** and not disclose it publicly, whether directly or via third parties, before the reporting manager has informed them of the conclusion of the investigation.

The **processing of personal data** within the framework of an internal report is performed in accordance with Regulation (EU) 2016/679, the General Data Protection Regulation, and in accordance with Moore's privacy policy, which is available here. Moore is deemed to be the controller with respect to the processing of personal data as part of the whistleblower procedure. Every report is recorded in a register provided for that purpose. Moore works together with an external provider (Whistleblower Software Aps) for its internal reporting channel, with that provider acting as its external processor. Both Moore and its external processor provide the necessary safeguards in terms of

confidentiality and security. The personal data are only processed within the European Union.

7. Protection

7.1. Conditions for receiving protection

A reporting person can apply for protective measures if they have **well-founded reasons** for believing that the **information concerning breaches was correct at the time of making the report** and **fell within the scope of this policy**, on the condition that the **correct procedures** were followed in respect of the internal or external report or the public disclosure.

Facilitators and other persons associated with the persons making the report can also apply for the protective measures set out below if they had well-founded reasons for believing that the reporting person falls within the scope of this policy for protection.

In the event that the **report turns out to be incorrect or unfounded**, then the reporting person will still receive protection if the **report was made in good faith**. That means the company cannot claim damages from the reporting person. The reporting person is exempted from civil or criminal liability and disciplinary proceedings.

Furthermore, reporting persons cannot be held liable for the acquisition of or access to the **information that is reported or publicly disclosed**, unless such an acquisition or access constitutes a criminal offence in itself.

The applicable law remains in force with respect to any other liability on the part of the reporting persons that is the result of actions or omissions **unrelated to the report or the public disclosure or** which were **not essential for the divulging of a breach**.

A reporting person who **deliberately made a manifestly unfounded report**, and thus made unlawful use of the reporting procedure under this policy, can be sanctioned.

7.2. Protection in the form of the prohibition of retaliation

If the reporting person, the facilitator or other persons associated with the reporting person meet the aforementioned conditions, then they will receive **protection from any form of unfair treatment, adverse decisions or retaliation**.

7.3. If the reporting person still suffers retaliation

7.3.1. Internal reporting

If the reporting person believes they have suffered retaliation, such incidents can be **reported to HR** at any time, so that a solution can be found within Moore.

7.3.2. Legal procedures

Legal procedures are also available for the reporting person in the event of retaliation against them.

8. Support measures

Everybody who wishes to make a report is entitled to:

- information and advice on the procedures and remedies that provide protection against retaliation as well as on the rights of the persons concerned;
- technical, psychological and social support.

The **Federal Institute for the Protection and Promotion of Human Rights** plays an important role in the provision and support of such measures, and any person can approach them in that respect.