

Whistleblowing Procedure





	Level	Level 2 - Group Policies ▾		Status	Active ▾
	Approved by	Chief Risk Officer, Lars Ottersen and Chief Financial Officer, Stian Grindheim		Last approved	8 Nov 2024

Table of contents

1. Whistleblowing statement	2
2. Who can report	3
3. What can be reported	4
4. What should not be reported	5
5. Where to report	5
6. The whistleblowing process and its actors	6
7. Country Managers	7
8. Documentation requirements	7
9. User access and management on Whistlelink	8

1. Whistleblowing statement

Visma will not tolerate any form of misconduct or critical conditions, such as violations of statutory rules, internal rules, policies or ethical standards, such as bullying, harassment, discrimination, corruption, money laundering or any other financial fraud, and will make efforts to ensure a safe, healthy and legal environment in all our business activities and companies.

Visma will comply with all applicable laws and regulations and act ethically and socially responsible. Breaches of any local and/or EU/EEA law may result in disciplinary actions, including termination / dismissal and reports to the relevant authorities.

The Visma Whistleblowing Channel is a tool enabling anonymous submission of any suspected breach of the local and/or EU/EEA law from both inside Visma and outside. It fosters confidential communication between reporter and Case handler and the reporter may rest assured that any Report is being handled in a discrete, professional and respectful manner - and by the correct, dedicated Case handler in each case.

Visma Whistleblowing is compliant with the EU Whistleblower Directive (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) and the regulations regarding whistleblowing in the WEA (local working environment and protection laws). Visma is also, in some jurisdictions, due to being licensed by local Financial Supervisory Authorities, obliged to have a specific whistleblowing system in place.

Objective

The objective of this procedure is to describe the handling of cases submitted to the Visma Whistleblowing Channel, according to the EU Directive, local legislation and the internal procedures while at all times ensuring the protection of the Notifier.

The output of this process is that the reported case is handled with discretion and closed, with necessary actions taken.

Definitions

Case handler - the dedicated and assigned person who will handle the Report and lead the investigation of the case in an objective and open manner.

Intake Management - a third-party service facilitated by the vendor of the whistleblowing tool which receives the Reports and assigns cases within one business day based on a predefined schema.

Notifier - a person who reports a breach of EU/EEA or local law. They can be any employee, former or existing, or self-employed person in Visma, a shareholder, or someone from outside of Visma, e.g third persons connected with the Notifier or Visma's suppliers and customers who need to notify of a breach or a potential breach of the local or EU/EEA legislation or any of Visma's internal rules/policies.

Report - the reported whistleblowing case.

Viewer - a Case handler with temporary and limited access to the whistleblowing tool, requested by the Case handler to the Whistlelink Administrator.

Whistlelink - the chosen tool for handling whistleblowing reports according to the Directive.

Country Manager - a Visma employee, typically from Management, HR, Legal or Finance, responsible for coordinating whistleblowing cases within their country. The Country Manager will not handle the case, but make sure the case is followed up by dedicated Case handlers per Visma company and will also be responsible for updating and informing the Case handlers within their country of the local whistleblowing procedure. Each country has assigned two Country Managers for backup purposes.

Whistlelink Administrator - one dedicated Visma employee who responds to user management requests at whistlelink.admin@visma.com and has the overall responsibility and overview of cases, statistics, Case handlers etc. The Whistlelink Administrator is the first contact point with the Intake Management and communicates regularly with this resource.

2. Who can report

This procedure applies to a Notifier who needs to report a breach or a potential breach of the local or EU/EEA law or any of Visma's internal rules/policies, such as Visma's Code of Conduct.

It also applies to third persons who are connected with the Notifier, and who could suffer retaliation in a work-related context, such as colleagues or relatives of the Notifier.

As a Notifier, you are protected by law. You should not be treated unfairly or lose your job because you 'blow the whistle'. You may also rest assured that the Report will not be handled by persons involved in the case, in order to avoid retaliation and uncomfortable situations. Visma welcomes all reports on any breaches of the above mentioned regulations and Intake Management will make sure each case is directed to the correct Case handlers in each case.

Example: a Notifier wants to report on harassment from their HR resource in the company. If the HR resource in fact is the Case handler in the company, Intake Management will make sure the Report will not be directed to that Case handler and instead reach out to the back-up Case handler or – if the case is not suitable for the back-up Case handler – the Country

Manager or the Whistlelink Administrator to discuss to whom the Report should be directed to.

3. What can be reported

All reports shall be based on justifiable grounds of suspicion. Evidence is not necessary, but reporting must not be made with the intention to cause harm or with the knowledge that the accusation is false. Hence, the Report you disclose must be made in the public interest. To identify if a Report is in the public interest, you should look at the following criteria:

- ❖ the number of people affected
- ❖ the nature or impact of the harm
- ❖ who is the reported individual
- ❖ the severity of the case.

In a nutshell, **the Report should go beyond the employee's personal circumstances.**

Some examples¹, include the following:

- ❖ a criminal offense, for example, fraud, bribery, money laundering
- ❖ someone's health or safety is in danger
- ❖ risk or actual damage to the environment
- ❖ a miscarriage of justice
- ❖ the company is breaking the law – for example, it does not have the right insurances
- ❖ you believe someone is covering up wrongdoing
- ❖ harassment and bullying between colleagues or from the leader
- ❖ unhealthy psychosocial working environment
- ❖ #MeToo cases

Whistleblowing that fulfils this criteria shall be treated as *"Qualified Reporting"* and handled in accordance with this procedure.

4. What should not be reported

Types of cases other than those listed above should not be reported. Such cases that do not fulfil the criteria will be treated as *"Non-qualified reporting"*. A non-qualified reporting will not be handled within the Whistleblowing Procedure.

Examples of cases that should not be reported through the Whistleblowing Channel are

¹ <https://www.equalityhumanrights.com/en/whistleblowing>

- ❖ General opinions on how the business is run
- ❖ General opinions on salary, leadership or other personnel matters

Such cases shall be handled by reporting to the relevant manager or any other relevant person within the management of the company in question.

A standard response will be sent to the Notifier in case of a “non-qualified reporting”.

5. Where to report

Reporting shall be made through the external secure page <https://visma.whistlelink.com> which is the only and official Visma Whistleblowing Channel.

Reporting is made by submitting a form either anonymously or with a full name. Providing the full name might in some cases increase the chance of resolving the reported case, however, it is fully the Notifier's decision to disclose their identity or not.

If the report is done anonymously please make sure to include as much information about the matter as possible and at least the following:

- The Visma company connected with the misconduct/breach of local/EU/EEA law
- Description of the misconduct/breach and who's involved
- Facts, evidence or proof of the misconduct/breach
- Relevant attachments/documentation, if any

Note! If an alert is received through a different channel than the official one, the recipient shall use the Whistleblowing Channel to register the case or contact the relevant Country Manager. The same steps shall be used in handling the case.

6. The whistleblowing process and its actors

Assigning the Case handler

When Visma receives a Report submitted through the Whistleblowing Channel, the Intake Management will immediately receive a notification for channeling the alert to the designated Case handler for the company in which the Report pertains to. Intake Management will make sure that there is no conflict of interest between the content of the Report and the designated Case handler receiving the case. In cases where Intake Management is unsure of who should receive the report, the Report will be directed to the Country manager or the Whistlelink Administrator in order to assess who should handle the case. Visma uses this set-up also to ensure impartiality, efficiency and transparency.

Once the case is assigned to the main Case handler, the Notifier will receive an acknowledgement of receipt. According to our contract with Intake Management, this will happen within one business day after the Report was submitted.

A standard automatic response which will be sent to the Notifier.

Handling the Report

The provision in Article 8(3) of the EU Directive 2019/1937 specifies that each company with 50 or more workers is required to set up channels and procedures for internal reporting, where such legal entities belong to a group of companies. In Visma, all companies regardless of size, should implement the Visma Whistleblowing Channel.

The Country Managers have the responsibility to create local procedures for internal reporting, while the local cases are facilitated through Case handler assignment.

Each Visma company, regardless of size, should therefore assign two Case handlers responsible for cases pertaining to their company. The possibility for shared resources may however be an option for small companies.

All cases reported through the official Whistleblowing Channel will be tracked through logs that can't be tampered with, hence, cases can't be deleted from the system in a wrongful manner.

Qualified or Non-Qualified Report

The Case handlers on the platform will need to decide as per each internal procedure and local legislation whether the Report is to be treated as a Qualified or Non-Qualified report.

If the Case handler assesses that the Report is Non-Qualified, the Report can be immediately closed by sending a standardized reply to the Notifier through the platform and by unticking the “Whistleblowing case” box which will exclude it from statistics.

If the Report is considered to be Qualified, the relevant Case handler is obliged to start the investigation process. The Report will be marked as a “Whistleblowing case” and included in the statistics.

One of the fields to fill out is “Please select the Visma company this report pertains to.”, however this is not a mandatory field. If this information is not provided, the Country Manager or Whistlelink Administrator should double-check with the Notifier if the Report does not pertain to one of the listed Visma companies, or they are not comfortable providing this information. It should be made clear that this information is important in order for the case to be handled efficiently by the relevant people and in accordance with the EU directive.

Intake Management is provided access to an everyday updated sheet where all Visma companies and their Case handlers are listed. The sheet is integrated with Visma Organizational Manager (VOM) and is always updated on the correct resources.

7. Country Managers

The Country Managers are responsible for coordinating whistleblowing cases within their country. The list of Country Managers can be found [here](#) (link only available within Visma).

8. Documentation requirements

All activities related to the case must be documented. Necessary documentation must be gathered by the Case handlers or the Board of the Visma company (when applicable) who shall document everything during the process.

All documentation shall be stored on the Whistlelink platform which allows tracking all changes made in relation to a Report (e.g. document added, messages sent, etc.)

Even though the Reports can be exported from the platform in a pdf format, we don't recommend doing so, because we lose track of changes and progress in handling them.

Personnel data will be processed in accordance with the [Visma Privacy Statement](#).

9. User access and management on Whistlelink

The whistleblowing platform has four types of users: Owner, Administrator, Case handler and Viewer.

For safety reasons, there are only two users that have elevated rights: the Whistlelink Administrator and the Intake Management.

Whistlelink Administrator may be contacted at whistlelink.admin@visma.com for any questions or inquiries you may have related to the Whistleblowing Service.