Whistleblowing Procedure

Level	Level 2 - Group Policies	**Status**	Active
Approved by	Chief Risk Officer, Lars Ottersen and Chief Financial Officer, Stian Grindheim	**Last approved**	18 Dec 2025

Table of contents

1. Whistleblowing statement

Visma is committed to maintaining a safe, healthy, and secure environment across all its business activities and companies. We have zero tolerance for misconduct or critical conditions, including violations of statutory rules, internal policies, or ethical standards such as bullying, harassment, discrimination, corruption, money laundering, or other financial fraud.

Visma adheres to all applicable laws and regulations, acting ethically and socially responsibly. Breaches of local and/or EU/EEA law may lead to disciplinary actions, including termination/dismissal, and reports to relevant authorities.

The Visma Whistleblowing Channel provides a secure and anonymous way for both internal and external individuals to report suspected breaches of local and/or EU/EEA law. It ensures confidential communication between the Notifier and the Case Handler, guaranteeing that all reports are handled discreetly, professionally, respectfully, and by the appropriate, dedicated Case Handler.

Visma Whistleblowing complies 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 local working environment and protection laws (WEA). In certain jurisdictions, Visma is also required to have a specific whistleblowing system due to licensing by local Financial Supervisory Authorities.

Objective

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

The outcome 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 transparent, although discrete, 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 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, when needed. 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 and to be a sparring partner when Case Handlers are in need of assistance. Each country has assigned two Country Managers for backup purposes.

Whistlelink Administrator - one dedicated Visma resource 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 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 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 against any retaliation. 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 ensure each case is directed to the correct Case Handlers.

For example, if a Notifier wants to report harassment from their HR resource in the company, and that HR resource is the designated Case Handler, Intake Management ensures the Report is not directed to them. Instead, it will reach out to the back-up Case Handler or, if unsuitable, to the Country Manager or the Whistlelink Administrator to determine who should handle the Report.

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 or does not fall within the scope of the whistleblowing service. 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 case
- who is the reported individual
- the severity of the case.

In a nutshell, **the Report should go beyond the Notifier´s personal circumstances**.

Some examples[1], include the following:

- a criminal offense, for example, fraud, bribery, corruption, 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 or does not follow the GDPR-regulations
- you believe someone is covering up wrongdoing
- harassment and bullying between colleagues or from the leader
- breaches of Visma Code of Conduct
- 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

Only cases that meet the specific reporting criteria should be submitted through the Whistleblowing Channel.

Any submission that does not fulfill these criteria will be categorized as "Non-qualified reporting" and will not be processed under the Whistleblowing Procedure.

[1] https://www.equalityhumanrights.com/en/whistleblowing

Do not use the Whistleblowing Channel to report:

- General opinions on business operations.
- General opinions on salary, leadership, or other personnel matters.
- General discontent with your work, leader, or colleagues.

Such matters must be addressed by reporting to the relevant manager or another appropriate person within the company's management. A standard response will be issued upon receipt of a non-qualified reporting.

5. Where to report

All reports must be submitted through the external secure page https://visma.whistlelink.com, which is the only official Visma Whistleblowing Channel.

A report is made by submitting a form. You can choose to submit it anonymously or with your full name. While disclosing your identity might, in some cases, increase the chance of resolving the reported case, the decision to disclose your identity is entirely yours.

If reporting anonymously, please include as much detail as possible, ensuring you provide at least the following information:

- The Visma company connected with the misconduct or legal breach (local/EU/EEA law).
- A description of the misconduct/breach and who is involved.
- Facts, evidence, or proof of the misconduct/breach.
- Relevant attachments/documentation, if any.

> Note: If an alert is received through a channel other than the official one, the recipient must use the Whistleblowing Channel to register the case or contact the relevant Country Manager. The same steps and procedure shall be followed for handling the case.

6. The whistleblowing process and its actors

Assigning the Case Handler

When a Report is submitted through the Whistleblowing Channel, the Intake Management immediately receives a notification. Their responsibilities include:

- Channeling the Report to the designated Case Handler for the company the Report pertains to.

- ❖ Ensuring no conflict of interest exists between the content of the Report and the assigned Case Handler.
- ❖ Consulting the Country Manager or Whistlelink Administrator if they are unsure of who should handle the case.

This setup ensures impartiality, efficiency, and transparency.

Acknowledgement of Receipt

Once the case is assigned to the main Case Handler, the Notifier receives an acknowledgement of receipt, within one business day after the Report was submitted.

Handling the Report

The provision in Article 8(3) of EU Directive 2019/1937 mandates that companies with 50 or more workers must establish internal reporting channels and procedures, particularly where such legal entities belong to a group of companies.

Visma's internal policy goes beyond this requirement: all Visma companies, regardless of size, should implement the Visma Whistleblowing Channel.

Local Implementation:

- Country Managers are responsible for creating local procedures for internal reporting.
- Each Visma company, irrespective of size, must assign two Case Handlers responsible for cases specific to their entity. Small companies have the option to share resources.

All cases reported through the official Whistleblowing Channel are tracked via tamper-proof logs, ensuring cases cannot be wrongfully deleted from the system.

Qualified or Non-Qualified Report

1. Initial Assessment and Qualification

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 the report as Non-Qualified, they may immediately close the report. This action requires sending a standardized reply to the Notifier via the platform and unchecking the "Whistleblowing case" checkbox, which excludes the report from compliance statistics.

Qualified Reports: If the report is determined to be Qualified, the relevant Case Handler is obliged to initiate the formal investigation process. These reports are automatically marked as a "Whistleblowing case" and are included in all relevant statistics and reporting.

2. Mandatory Data Fields and Clarification

During intake, Case Handlers must fill out the field: "Please select the Visma company this report pertains to." While this field is not mandatory for the Notifier to complete, the following action must be taken if the information is missing:

- The Country Manager or Whistlelink Administrator must follow up with the Notifier to confirm whether the report genuinely does not pertain to a specific Visma company, or if the Notifier is simply uncomfortable providing the information.
- It must be clearly communicated to the Notifier that providing the company name is crucial for the efficient handling of the case by the relevant personnel and ensuring full compliance with the EU Directive.

3. Resource Management

Intake Management has access to a continuously updated resource sheet listing all Visma companies and their assigned Case Handlers. This sheet is integrated with Visma Organizational Manager (VOM), ensuring the resource information remains accurate and current for proper case routing.

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.

Personal 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 related to the Whistleblowing Service.