NOVEMBER FIRST

WHISTLEBLOWER POLICY

Approved by the Board of Directors: 16 December 2021
Valid from: 17 December 2021

1. Purpose

November First A/S ("N1") aims to have an open and healthy company culture and is committed to conducting business with integrity, securing our customers, partners, colleagues, and society. N1 encourages sharing concerns of any potential breach of laws or regulations applicable to N1, as well as N1 internal policies and procedures.

The purpose of this Whistleblower Policy is to secure a special, independent channel that increases the opportunity to report on violations, criminal or critical matters and to discover mistakes and negligence. N1's Whistleblower Policy encourages and protects employees who speak up when they encounter behaviour that is unethical, illegal or goes against N1 values. This includes e.g.:

- Accounting, internal accounting controls or auditing matters
- Money laundering or terrorist financing
- Market abuse
- Insider trading
- Breaching customer confidentiality or privacy
- Theft
- Bribery or corruption
- Discrimination, violence, assault, and harassment
- Violations of any other laws, regulations or N1 policies

The Whistleblower scheme (the "N1 Whistle Portal") is a supplement to the direct and daily communication in N1 and secures the option of remaining completely anonymous. Employees can use the Whistle Portal to raise their concerns without fear of reprisal.

Employees are always encouraged to share the concerns with their direct manager, management, colleagues, and Compliance. However, in situations where an employee may not feel comfortable in sharing their concerns, the Whistleblower scheme is to support N1 in such situations by providing a secure channel where employees can report on violations or negligence, as well as serious and sensitive matters anonymously, if needed.

The Whistleblower Policy also serves to set out principles and standards for managing Whistle Reports, as well as roles and responsibilities. The Whistle Portal alerts management to allegations of crime or other suspected misconduct and helps ensure appropriate and adequate action is taken to address the situation.

N1 take the utmost care to protect the identity of whistleblowers and the confidentiality of a Whistle report.

The Policy applies to all N1 employees (former and current), BoD members and external partners, customers and individuals associated with N1.

2. Scope

The Whistleblower Policy lays out the principles for N1's Whistleblower scheme.

3. Reporting via the N1 Whistle Portal

The N1 Whistle Portal is accessed at https://novemberfirst.whistleportal.net and gives access to N1's reporting pages in Danish and English.

The Whistle Portal, which is a special and independent channel managed by BDO Statsautoriseret Revsionsaktieselskab ("BDO"), is based on an Open Whistleblowing Framework by GlobaLeaks (www.globaleaks.org).

4. Content

Whistle Reports can be made by submitting the secure online questionnaire at N1's Whistle Portal, https://novemberfirst.whistleportal.net.

Who can report?

- Employees (former and current))
- BoD members
- External partners, customers and individuals associated with N1

What can be reported?

- Any breach of laws or regulations applicable to N1, as well as N1's internal policies and standards.
- Serious and/or criminal offenses such as theft, embezzlement, fraud, bribery, corruption, accounting fraud/manipulation, misuse of assets, misuse of financial means, etc.
- Serious matters regarding discrimination, violence, assault, and harassment.
- Serious violation of internal guidelines (serious violation meaning systematic, repeated, and significant violation of internal procedures.)
- Concerns that would not potentially cause financial losses for N1, impact N1's reputation, or the like.
- Concerns, even if whistleblower is uncertain whether the respective concern is an actual breach or potential breach, provided they have reasonable grounds to believe that the information reported was true at the time of reporting.
- Any employee of N1, including former employees; board members, any contractors or consultants employed by N1; any Process; and any department may potentially be the subject of a Whistle Report.

What cannot be reported?

- Employment relationship, e.g., absence and co-operational problems, alcohol, terms of employment etc. and matters that are not serious, should not be reported via the N1 Whistle Portal, but are internally dealt with via e.g., direct manager or management.
- Customer complaints must be submitted to complaints@novemberfirst.com.

Sensitive information on an individual, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life not relevant for the Whistle Report should be avoided. However, this information should be documented if any of the following exceptions apply: 1. It is relevant to the Whistle Report; and/or 2. Consent was given by the individual to include this information (which is given in the questionnaire's step 5).

5. Protection of the employees

Employees who submit Whistle Reports must not be subjected to unfavourable treatment or be disadvantaged due to their concerns. Protection covers all forms of repatriation, discrimination, and other unfair treatment. The protection of employees applies to information provided in "good faith". That is, an employee must not knowingly submit false or misleading information.

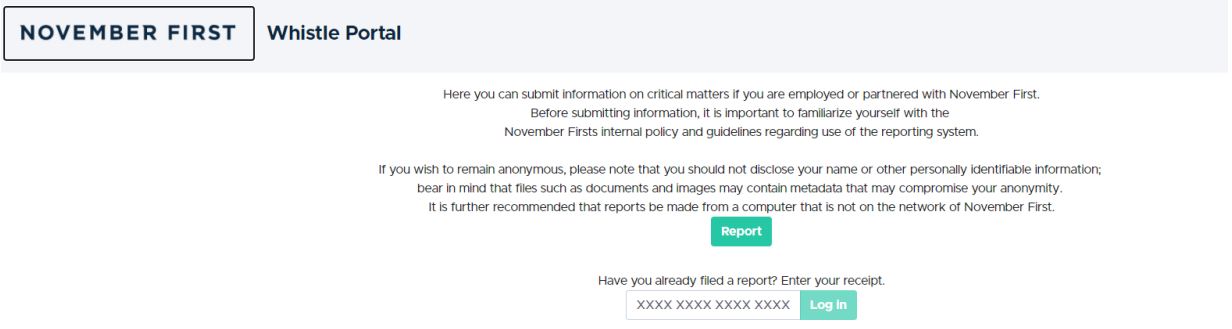
If a whistleblowing concern is reported deliberately in bad faith, this may result in disciplinary action and the individual will not be protected by the Whistleblower scheme.

6. Confidentiality and anonymity

All information submitted via the N1 Whistle Portal is treated with confidentiality and discretion.
The Whistle Portal is designed to remove or limit the storing of information when visiting the site and when using the portal to secure the anonymity.
Additional security measures are taken to ensure the protection of the confidential data stored in the Whistle Portal.

If an individual wishes to remain completely anonymous, it is essential to be aware of the questionnaire's 3rd and 4th step, as seen in the following.

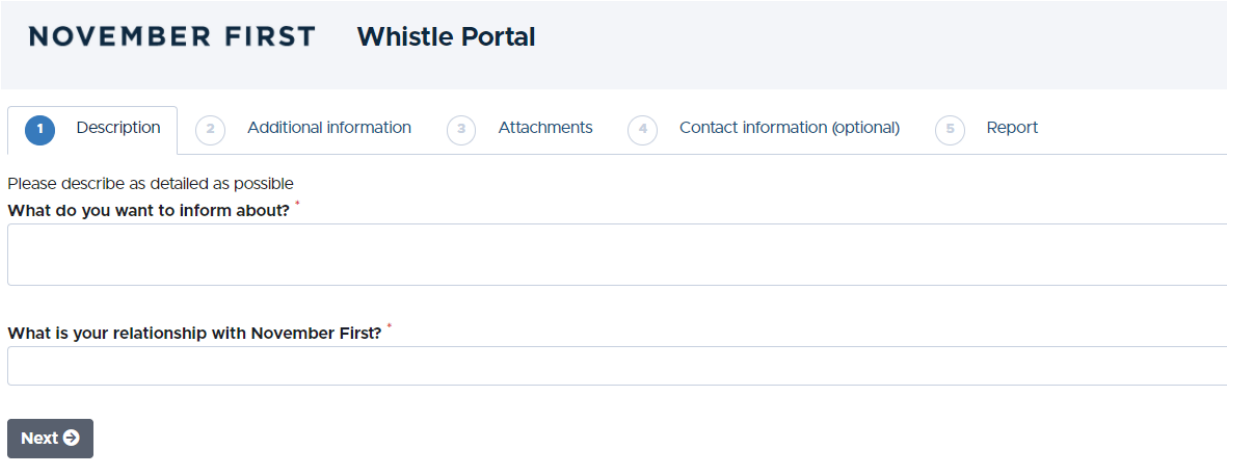
When accessing https://novemberfirst.whistleportal.net below introduction will appear:



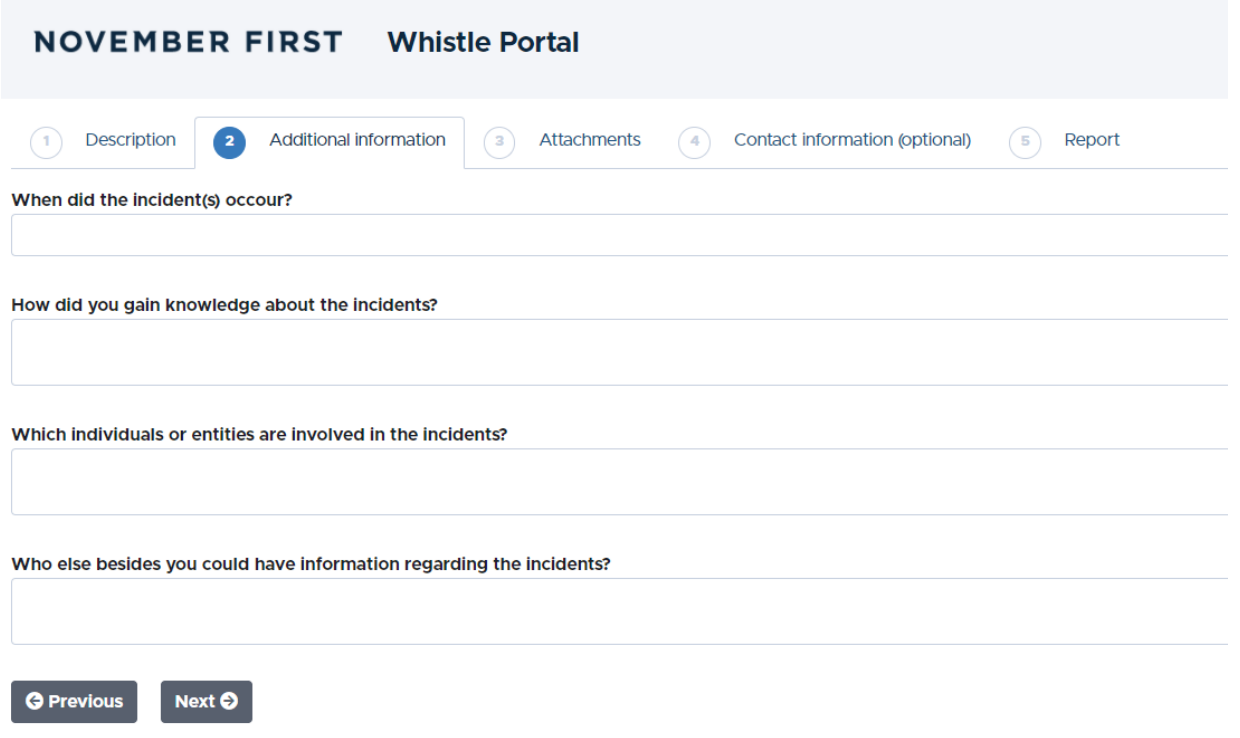
To initiate a report, press 'Report', and the following steps will appear:

Step 1. Description:

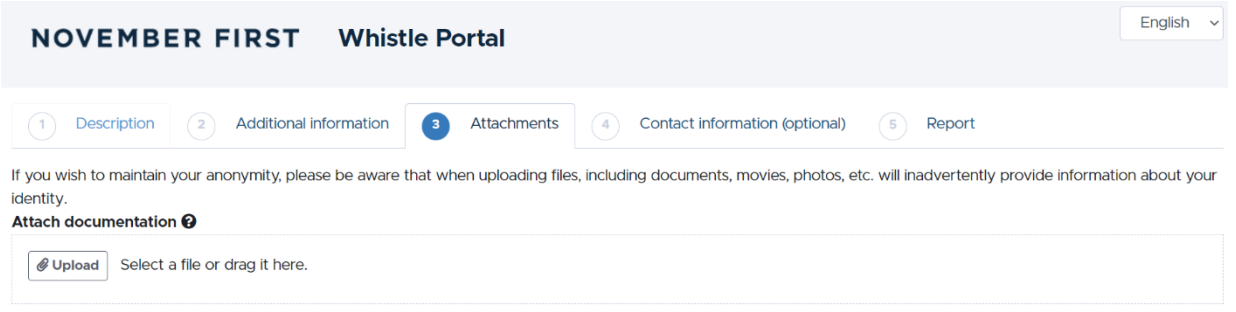
It is important to describe all matters as detailed as possible. As far as possible, claims and information must be documented, as factual information and physical documentation enlightens and support the case as best as possible.



Step 2. Additional information:

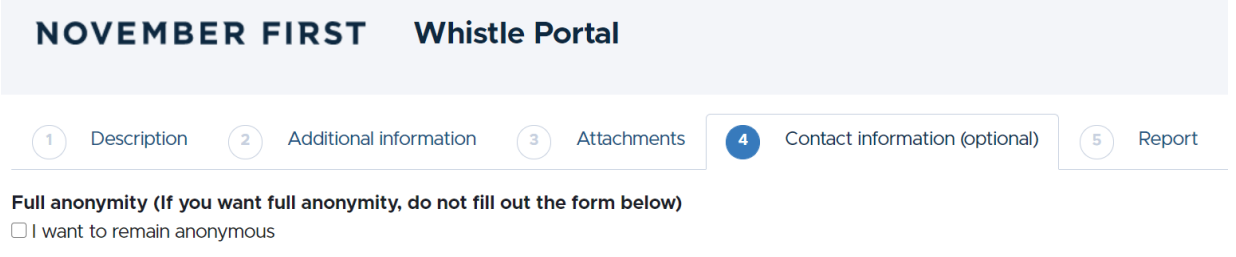


Step 3. Attachments:
In the 3rd step where documentation etc. can be attached, it is important to be aware to remove metadata and/or not to disclose any documents that can provide information about the whistleblowers identity.

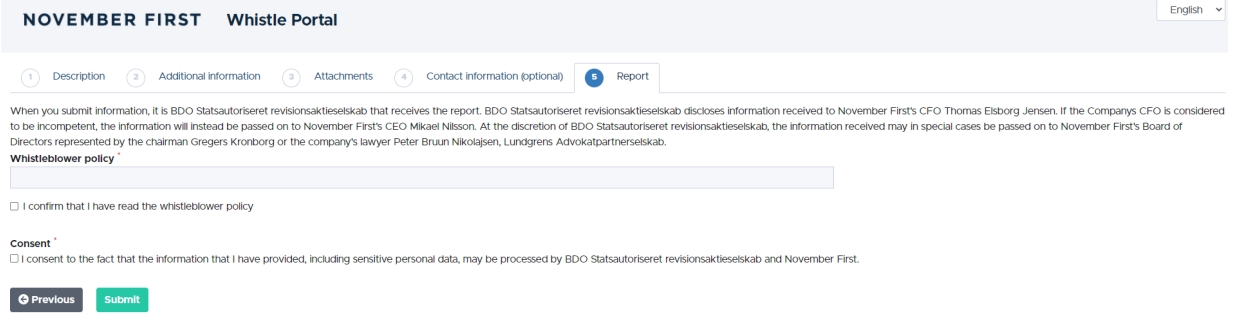


Step 4. Contact information (optional):
In the 4th step, it is important to **not** fill in the contact information form, if the whistleblower wishes to remain fully anonymous.

If information is being submitted from N1's network, there can be a risk of the individual being logged as part of the ordinary logging of user activities. To avoid this risk, N1 encourages to submit on a private or public device that is not associated with N1's network.



Step 5. Report:



7. Case procedure

Submitted reports are accessed by trusted employees at BDO, who receives, register and process the reports.

The reports are forwarded to N1's CEO. If N1's CEO is considered to be conflicted or partial, the information will instead be forwarded to N1's CCO & President. If the report concerns the management of N1, the report will be forwarded to the chairman of the board at N1. At the discretion of BDO, the information received may in special cases instead be passed on to N1's lawyer.

In rare cases involving serious crimes, and where the identity is known due to the individual actively choosing to disclose their personal information in step 4, identity information might be passed on to authorities to be used for case management purposes.

A preliminary examination of the report will be made by BDO to assess whether the report is within the scope of the Whistleblower scheme, and whether there are grounds for a procedure and further examination, or whether the report is manifestly unfounded (e.g., if the report concerns circumstances that are not within the scope of the Whistleblower Scheme).

If there are grounds for further examination of the report such will be initiated. If necessary, legal, or external advisory assistance might be involved.

8. Involved person(s)

Unless specific and legitimate reasons due to considerations of public interest, including state security and prevention, investigation, disclosure, or prosecution in criminal cases prevents it, the involved person(s) will be informed about the case procedure, when the report is received, and an investigation has been initiated. The other acts of the case are confidential, and implicated persons are never informed about who submitted information on the Whistle Portal.

9. Receipt

It is possible to remain completely anonymous and follow the case by using the 16-digit code (receipt) that is being shown after a report has been submitted.

This channel can be used to ask additional questions to the individual without disclosing the identity of the individual.

Furthermore, the channel can be used to communicate a conclusion to the case, if the individual that has submitted the report is anonymous.

If the individual submitting the report remains anonymous, the following deadlines apply:

- Within 7 days confirmation is given that the report has been received.
- The case will be processed as soon as possible, and it is aimed that the case procedure will not exceed 3 months.
- A conclusion to the case will be available through the anonymous channel.
- As a main rule all reports are deleted from the Whistle Portal within 90 days after they have been submitted, unless the deadline is extended manually be the recipient.
- The individual that has submitted a report has access to the case via the Whistle Portal and the 16-digit code until the case gets deleted in the Whistle Portal. However, the maximum access to view the case will be a year from the day the report was submitted.

10. Deletion of data

If the report does not fall within the scope of the Whistleblower scheme, or is assessed to be manifestly unfounded, the personal data will be deleted immediately.

Furthermore, personal data are deleted when it is no longer necessary to store the data, including when the case is closed.

Reports will as a main rule be deleted after 90 days in the Whistle Portal, unless the deadline is manually extended by the recipient.

The standard deletion rules apply. If there is a disciplinary action case or sanction due to the information provided, or that other factual grounds speak to the necessity of storing the information on an employee, the information will be stored in the respective employee's HR folder.

11. Escalation, reporting and follow up

When a Whistle report is submitted, the Escalation Policy will be activated. The Escalation Policy contains the requirements for appropriate and timely internal reporting of potentially problematic cases in N1.

Reports are provided to the BoD and Compliance Committee and reports relevant to the Financial Supervisory Authorities on the number of Whistle Reports received, including an analysis of the types of concerns raised in the Whistle Reports.

Case data must be kept complete and current in the appropriate system of record to provide required parties and other parties with the necessary metrics, reporting and analytics, which are applied to support appropriate actions and an overview of Whistle Reports. All reporting information, including information retained for statistical purposes, shall be made anonymous, including the removal of information that may result in indirect identification.