Nortal Group

Privacy policy for whistleblowing system

Prepared for:
Nortal Group,
Except Nortal LLC (USA)

Date prepared:
17.12.2023

Valid for:
Until updated

Where it *matters* most.

Nortal

Table of contents

1. The purpose of processing personal data in the whistleblower system 3
2. Categories of personal data that is processed 3
2.1. Information about the reporter 3
2.2. Information about the reported person 3
3. Basis of processing 4
4. Making available and disclosing personal data 4
5. Deletion of registered data 4
6. Data subjects rights 5
6.1. The right of access 5
6.2. The right to rectification 5
6.3. The right to erasure/be forgotten 5
6.4. The right to object 5
6.5. Right to request restriction 5
6.6. The right to object 5
7. Contact details for questions 6
Document control 7
Revision history 7

1. The purpose of processing personal data in the whistleblower system

The purpose of processing personal data in the whistleblower system is to uncover knowledge of serious matters, including suspicion or knowledge of any illegal, unethical or irregular conduct to prevent, limit and follow up on such matters in the entire organization.



Routine employment matters (such as dissatisfaction with salary conditions, benefits, performance appraisals, cooperation difficulties, etc.) should not be reported via the whistleblower channel.

Nortal AS is the data controller of the personal data processed in the whistleblower system. The data is collected from the data subjects identified as Whistleblowers under the Nortal Whistleblower policy.

2. Categories of personal data that is processed

2.1. Information about the reporter

We will process different categories of personal data depending on how you chose to make a disclosure. All disclosures are documented. As a starting point, we will only process the personal data that you chose to provide. This may include your name, contact information, role, department and other data that you chose to include in your disclosure, e.g. voice recordings, photos and special categories of personal data (personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning sex life or sexual orientation).

You may always choose to make a disclosure anonymously. If you choose to be anonymous, we will not process any personal data about you and only register the report itself. There is no log made as to the IP address or machine ID of the computer on which the report is made. Be aware that if you choose to give such information when submitting the report from which you can reasonably likely be identified either directly or indirectly, the organization will also process this information when handling the case. This also applies if you have chosen to remain anonymous.

Please note that it may be more difficult to investigate disclosures made anonymously since this will limit our possibility to communicate with you and ask you follow-up questions.

2.2. Information about the reported person

If you are the subject of a disclosure, we will process any personal data about you that is included in such disclosure and/or that comes to our attention during an ensuing investigation, if applicable. This may include photos and special categories of personal data (personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning sex life or sexual orientation).

All personal data collected through the system will be treated as confidential to the maximum extent possible. Nortal guarantees that your personal data protection rights will be respected with certain limitations and will only be used as described above. Your right to know about a disclosure concerning you is subject to your rights under the GDPR and complementing national legislation.

3. Basis of processing

We have a legal obligation under the Whistleblowing legislation to provide a whistleblowing channel. Hence, our processing of your personal data will rely on this legal obligation (GDPR, article 6.1(c)). This includes any processing of data relating to criminal convictions and offences. Any processing of special categories of personal data is necessary for reasons of substantial interest on the basis GDPR, article 9(2)(g).

4. Making available and disclosing personal data

The reporting system is hosted by Nortal AS. Nortal has taken the necessary technical and organizational measures to prevent personal data from being accidentally or unlawfully destroyed, lost or damaged and to prevent breaches of confidentiality, unauthorized disclosure or misuse of the personal data.

Only the Compliance Team will have access to the report and any personal data included therein. The members of the Compliance Team will carry out the initial screening of disclosures made and take appropriate measures in regard to the information provided in your report.

The information registered in the system is generally not transferred to a third party outside of Nortal Group. However, in the following circumstances, the information may be transferred onward on a case by case basis:

- Transfer to an external attorney or auditor in connection with the case processing of the report.
- If the report results in legal action.
- If the law so requires (e.g. report to authorities).

5. Deletion of registered data

Registered data may only be retained for as long as there is a need for it. When there no longer is a need for retaining the registered information, the information is deleted. Personal data will be kept for 3 years after an investigation has been completed unless longer retention is provided or necessary for the fulfilment of rights and obligations under the Whistleblower Protection legislations or other regulations, or for the preparation, presentation, or defense of a legal claim.

6. Data subjects rights

6.1. The right of access

You have the right to receive information about the personal data we process and why we do it. You also have the right to receive a copy of all personal data we have about you. This right may be restricted in the event, and only to the extent, it is necessary and proportionate to verifying the accuracy of the report made and protecting the identity of the Whistleblower, as provided under national laws.

6.2. The right to rectification

If the data we hold about you is incorrect, you have the right to have it corrected. You also have the right to supplement incomplete information with additional information that may be needed for the information to be correct. Once we have corrected your data, or it has been supplemented, we will inform those we have shared your data with about the update, provided that it is possible. If you request to have data corrected, you also have the right to request that we limit our processing during the time we investigate the matter.

6.3. The right to erasure/be forgotten

In some cases, you have the right to have your data deleted. You have the right to have your data deleted if:

6.3.1. The data is no longer needed for the purposes for which we collected it,

6.3.2. You oppose use that is based on our legitimate grounds and we cannot show compelling grounds that outweigh your interests,

6.3.3. The personal data has been used illegally, or

6.3.4. Deletion is required to fulfill a legal obligation.

6.3.5. If we delete data following your request, we will also inform those we have transferred your data to in accordance with this policy, provided that it is possible.

6.4. The right to object

You have the right to object to processing that is based on our legitimate grounds. If you object to the use, we will, based on your particular situation, evaluate if our grounds for processing the data outweigh your interests in the data not being used for that purpose. If we are unable to provide compelling legitimate grounds that outweigh yours, we will stop using the data you object to - provided we do not have to use the data to establish, exercise or defend legal claims.

6.5. Right to request restriction

Restriction means that the data is marked so that it may only be used for certain limited purposes. The right to restriction applies, unless provided otherwise under national laws:

6.5.1. When you believe the data are incorrect and you have requested correction. If so, you can also request that we limit our use while we investigate if the data are correct or not.

6.5.2. If the use is illegal but you do not want the data to be deleted.

6.5.3. When we no longer need the data for the purposes for which we collected it, but you need it to be able to establish, assert or defend legal claims.

6.5.4. If you object to the use. If so, you can request that we limit our use while we investigate if our interest in processing your data outweighs your interests.

Even if you have requested that we restrict our use of your data, we have the right to use it for storage, if we have obtained your consent to use it, to assert or defend legal claims or to protect someone's rights. We may also use the information for reasons relating to an important public interest.

If we limit our use of your data, we will also inform those we have shared your data with, provided that it is possible.

6.6. The right to object

If you exercise your rights and they are not met, we will tell you why. Please let us know if you do not agree with the way we are processing your personal data. You may also submit complaints to a supervisory authority, in particular in the Member State of your habitual residence, place of work or where the alleged infringement of the GDPR took place.

7. Contact details for questions

If you have any questions regarding personal data protection, you may contact Nortal by e-mail: privacy@nortal.com.

Nortal is data controller for the processing of the personal data that you report and can be contacted through the ordinary communication channels. Likewise, the Nortal´s data protection officer can be contacted through the ordinary communication channels (privacy@nortal.com) if you have questions about the processing of the information.

Document control

Title	Nortal privacy policy for whistleblowing system
Applies to	Nortal Group, except Nortal LLC (USA)
Date prepared	17.12.2023
Valid for	Until updated

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.1	17.12.2023	Tanja Bäthge, Kadri Riisalu, Veli Sinda	Introduction of privacy policy