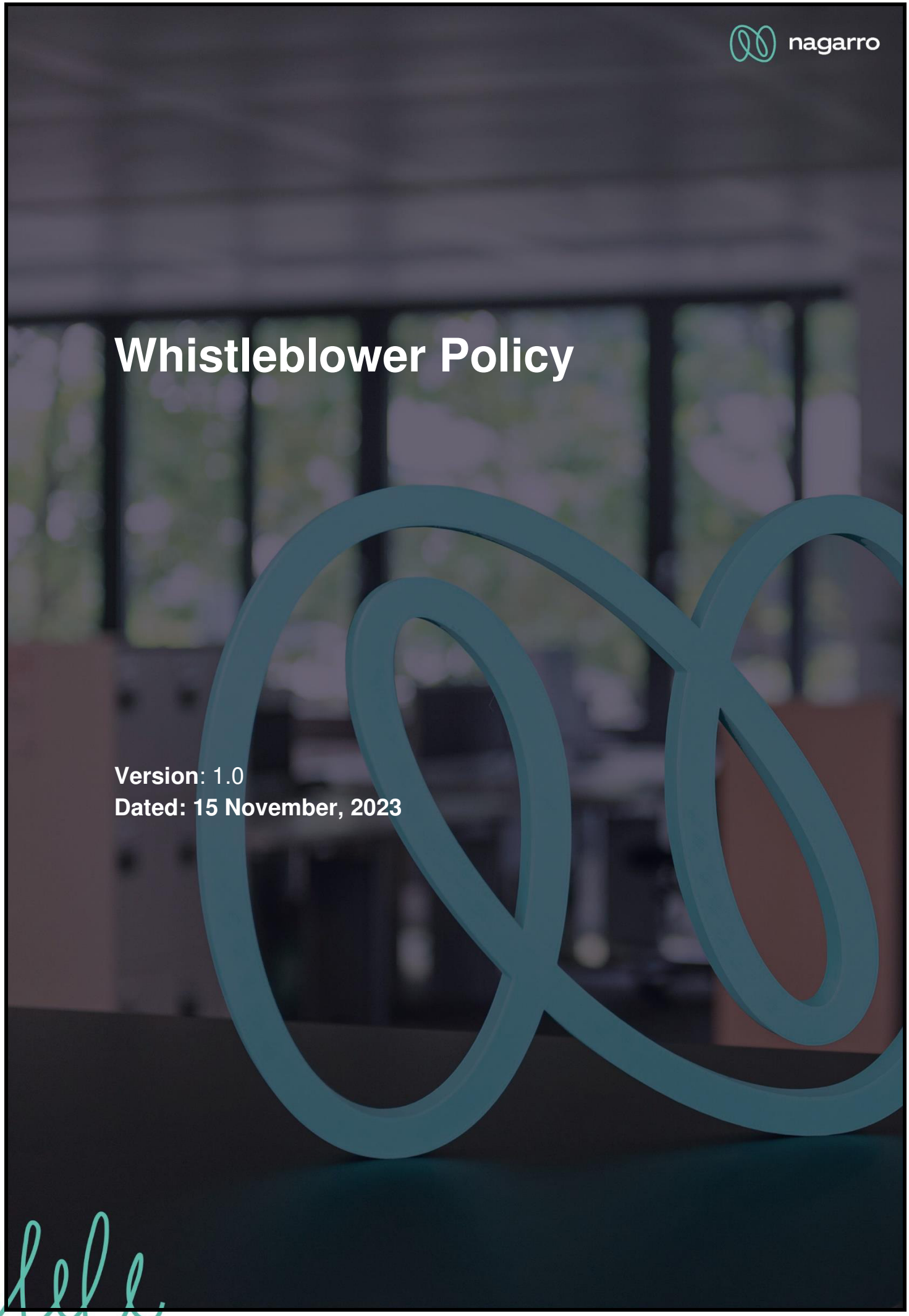
nagarro

# Whistleblower Policy



**Version**: 1.0
**Dated: 15 November, 2023**

Table of Contents

# 1. Introduction

Nagarro is committed to promoting transparency, accountability, and ethical behavior in the workplace. This policy provides reporting persons with a mechanism to report suspected breaches, as defined below, within Nagarro group ("**Nagarro**") and ensures that Nagarro takes appropriate action to address such reports. It provides access to mechanisms to report such incidents within and outside of Nagarro without fear of retaliation, promotes transparency and accountability, and ensures compliance with the relevant laws and regulations, in accordance with, *inter alia*, the 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 corresponding national laws applicable to Nagarro entities.

# 2. Purpose and Scope

The purpose of this policy is to encourage persons with knowledge about suspected breaches, as defined below, within Nagarro to speak up and report it through whistleblower@nagarro.com as the designated reporting channel, to protect reporting persons as well as persons who are subject of a report and other persons affected by a report against retaliation and to promote public interest.

This policy is essential to Nagarro's commitment to ethical behavior, transparency, and accountability. Nagarro encourages to report any breaches and expects all employees to comply with this policy by reporting suspected breaches promptly.

This policy does not cover complaints against personal work-related grievances which do not constitute breaches, as defined below. Such complaints should be addressed to the person's Operational Guide or People Enablement.

# 3. Definitions

**Reporting person** or **whistleblower** means a natural person who reports or publicly discloses information on breaches acquired in the context of their work-related activities.

**Breaches** means acts or omissions that constitute a violation of law, e.g. laws protecting against fraud, corruption, money laundering, crimimal assault or other criminal offences, laws protecting rights of employees and employee representatives, consumers, fair competition, public procurement, product safety and compliance, the environment, public health, privacy and personal data, and security of networks and information systems.

**Information on breaches** means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches.

**Retaliation** means any act or omission occurring in a work-related context, which is prompted by a report or public disclosure and causes them unjustified detriment.

**Work-related context** means current or past work activities within or with Nagarro through which, irrespective of the nature of those activities, reporting persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information.

## 4. Applicability

This policy applies to all current and former employees of Nagarro, including temporary employees, contractors, trainees, interns, applicants, suppliers and business partners, who have obtained information about breaches, as defined below, in connection with their professional activities or in advance of professional activities and report or disclose such information as described in this policy.

The protection provided under this policy also applies to persons who are the subject of a report or disclosure and other persons affected by a report or disclosure.

This policy covers all reports of breaches, as defined below,provided that the reporting person had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of this policy.

## 5. Nagarro's commitment

Nagarro is committed to:

- providing an internal reporting channel (whistleblower@nagarro.com) to report suspected breaches within Nagarro;
- protecting the identity of reporting persons and ensuring confidentiality of submitted reports;
- protecting reporting persons as well as persons who are subject or a report or disclosure or other persons affected by a report or disclosure from retaliation;
- thoroughly examine each submitted report and investigate any reported breaches in a timely manner, and provide a response about the outcome to the reporting person;
- keep all records of reports and their investigations carefully and securely.

# 6. Protection from retaliation

Everyone with knowledge about suspected breaches in a work-related context has the right, and is highly encouraged to report such breaches, without fear of retaliation.

Nagarro will not retaliate or tolerate any form of retaliation against reporting persons, persons who are the subject of a report or disclosure and other persons affected by a report or disclosure and will take appropriate measures to protect them.

# 7. Operation

### 7.1 Internal reporting

Any suspected breaches can be reported by sending an email to whistleblower@nagarro.com from any email address.

All submitted reports should be in English.

At the request of the reporting person, a personal meeting with a member of the internal reporting office or a person designated by the internal reporting office shall be made possible within a reasonable time period. With the consent of the reporting person, the meeting may also take place by means of video and audio transmission.

Nagarro's internal reporting channel is designed, established and operated in a secure manner ensuring that confidentiality of the report and the identity of the reporting person and any other person mentioned in the report are protected, and preventing access thereto by non-authorised persons.

Employees can choose to remain anonymous by using an anonymous or disposable email account. Nagarro will make every effort to protect the identity of the Whistleblower.

### 7.2 Internal reporting office

Nagarro has established an internal reporting office with a limited number of independent, trained and impartial recipients of reports submitted through the internal reporting channel. Access to such reports is restricted to:

- Custodian of Regulatory Compliance & Management Board member,
- Director Data Privacy,
- Director Legal & Compliance.

The internal reporting office will conduct an initial review of each report and, depending on the subject matter of the report, involve additional people, e.g. the responsible Service Region Custodian, persons with knowledge of or a connection to the reported breaches or independent,

external legal counsel to the extent necessary to properly investigate the matter, while maintaining confidentiality (sec. 7.4) and conduct an effective investigation.

Only members of the internal reporting office will respond to reports and maintain communication with the reporting person and, where necessary, ask for further information from and provide feedback to the reporting person.

### 7.3 Response time

The internal reporting office will acknowledge receipt of a report to the Whistleblower within seven days of its receipt, and provide feedback within a reasonable time frame which may vary depending on the type of reported misconduct, but which shall not exceed three months from the acknowledgment of receipt of a report.

### 7.4 Confidentiality

The internal reporting office maintains the identity of:

- the reporting person, provided that the information reported relates to offences falling within the scope of this policy or the reporting person had reasonable grounds to believe that this was the case at the time the report was made,
- the persons who are the subject of a report, and
- other persons named in a report

strictly confidential.

The identity of the persons referred to above may only be disclosed to members of the internal reporting office, people entrusted with investigating reported breaches or taking follow-up actions and to the persons assisting them in the performance of these tasks.

### 7.5 Documentation

The internal reporting office documents all incoming reports in a permanently retrievable manner and in compliance with the confidentiality requirements according to sec. 7.4.

The records of a report shall be deleted three years after the review process has been completed. Records may be kept longer to meet legal requirements for as long as necessary and proportionate.

### 7.6 External reporting

Nagarro prefers and encourages the use of its internal reporting channel since Nagarro believes that any breaches can be most effectively addressed internally and no person reporting suspected breaches has to fear any retaliation.

A reporting person may nevertheless also contact an external reporting office established by the authorities where the concerned Nagarro entity is located. A list with the competent external reporting offices is included as **Annex** to this policy and updated frequently.

### 7.7 Public disclosure

The protection provided by this policy extends to individuals who publicly disclose information about suspected breaches to the media or through other means, under certain conditions.

Therefore, this policy only applies to persons who publicly disclose suspected breaches if:

- the person first reported internally or externally in accordance with sec. 7.1 and 7.6, but no appropriate action was taken in response to the report within three months or six months in justified cases,

  or

- the person has reasonable grounds to believe that:
  - the breaches may pose an immediate or obvious threat to public interest because of an emergency, risk of irreversible damage or comparable circumstances,
  - in case of internal or external reporting, there is a risk of retaliation or it is unlikely that the reported breach are being remedied effectively, due to the particular circumstances of the case, e.g. if evidence could be suppressed or destroyed or where a public authority could be in collusion with the perpetrator of the breaches or involved in the breaches.

The disclosure of knowingly false information on breaches is prohibited and not protected by this policy or applicalble whistleblower protection laws.

## 8. Policy access

Nagarro will communicate this policy to all employees and will make it accessible on its internal platform and website.

Nagarro will review and update this policy as necessary to ensure its continued effectiveness.

## 9. **Annex:** List of external reporting channels in EU member states

| Country | External reporting office | Contact or additional information |
|---|---|---|
| **Austria** | Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (Federal Office for the Prevention of and Fight against Corruption) | https://www.bak.gv.at/601/ |
| **Denmark** | Den Nationale Whistleblowerordning (National Whistleblower Scheme) | https://whistleblower.dk/ |
| **Finland** | Valtioneuvoston Oikeuskansleri (Chancellor of Justice) | https://oikeuskansleri.fi/en/whistleblower-protection |
| **France** | Défenseur des droits (Defender of rights) | https://www.service-public.fr/particuliers/vosdroits/F32031 |
| **Germany** | Bundesamt für Justiz (Federal Office of Justice) | https://www.bundesjustizamt.de/hinweisgeberstelle |
| | Bundesamt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority) | https://www.bafin.de/DE/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node.html |
| | Bundeskartellamt (Federal Cartel Office) | https://www.bundeskartellamt.de/DE/Kartellverbot/Hinweise_auf_Verstoesse/Hinweise_node.html |
| **Portugal** | Multiple authorities | See Art. 12 of Lei n.º 93/2021 (https://files.dre.pt/1s/2021/12/24400/0000300015.pdf) |
| **Romania** | Agentia Nationala de Integritate (National Integrity Agency) | https://avertizori.integritate.eu/ |
| **Spain** | Autoridad Independiente de Protección del Informante (Independent Authority for the Protection of the Informant) | As of November 2023, the competent authority has not yet been officially established by the Spanish government. |
| **Sweden** | Multiple authorities | See Annex to Ordinance on the Protection of Persons Reporting Irregularities (SFS 2021:949): https://www.government.se/government-policy/labour-law-and-work-environment/2021890-act-on-the-protection-of-persons-reporting-irregularities-2021890/ |