

□

Whistleblower Policy for ATG Netherlands B.V.

Public document

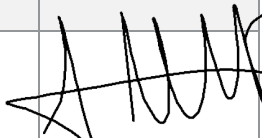
Prepared by: Ellemiek Westhoek, HR Director



DOCUMENT OWNER

The HR Director is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ATG Quality Management System (QMS) and Information Security Management System (ISMS) and the applicable legislation.

DOCUMENT CHANGE LOG APPROVAL & AUTHORIZATION

Issue Revision	Date of Issue DD-MM-YYYY	Change Description	Pages Affected	Approved by date	Approved by date	Authorized by date
1.0	08-03-2024	First issue	All pages	Works Council NL	Ellemiek Westhoek, HR Director	Gian Carlo Coletta, CEO
1.1	19-08-2024	Minor updates	Page 8, 10	n/a		

DISTRIBUTION

Name	Job Title/Organization
All employees of ATG Netherlands	

APPLICABLE DOCUMENTS

Title of document	Reference
QMS	
ISMS	
Employee Disciplinary Procedure for NL	ATG-IMS-DOC-07-ATG
Disciplinary Procedure for Security Incidents	ATG-ISMS-DOC-A6-4-1
Whistleblower Privacy Notice	ATG-ISMS-DOC-A05-34-9

Table of Contents

1.	Introduction & Scope	5
1.1	A (danger of) violation of a statutory regulation or internal rules of an employer	5
1.2	A risk to public health	5
1.3	A risk to the safety of persons	5
1.4	A risk of environmental degradation	6
1.5	A risk to the proper functioning of the Company as a result of improper actions or negligence	6
1.6	A violation of European Union law.	6
1.6.1	Public Procurement	6
1.6.2	Financial services, products and markets, prevention of money laundering and terrorist financing.....	6
1.6.3	Product safety and product compliance	6
1.6.4	Transport safety.....	6
1.6.5	Environmental protection	6
1.6.6	Radiation protection and nuclear safety	6
1.6.7	Food and feed safety, animal health and welfare.....	6
1.6.8	Public health	7
1.6.9	Consumer protection.....	7
1.6.10	Protection of privacy and personal data and security of network and information systems	7
1.6.11	Breaches affecting the financial interests of the EU	7
1.6.12	Infringements related to the internal market of the EU	7
2.	Responsibilities.....	7
3.	Definitions	8
4.	General Principles.....	8
4.1	Key Principles	8
4.1.1	Confidentiality safeguards.....	8
4.1.2	Protection against retaliation	9
4.1.3	Anonymous reporting.....	9
4.1.4	The investigation process	9
5.	Reporting Process.....	9
5.1	Accessing the Reporting Tool.....	10
5.2	Anonymous Reporting Option	10
5.3	Other means of reporting	10
5.4	Submission of Report	10
5.5	Confidentiality and Security	11
5.6	Confirmation of Receipt	11
5.7	Tracking and Follow-Up.....	11
6.	Investigation Process.....	11
6.1	Objectives.....	11
6.2	Relevant Documents	12
6.3	Other Sources of Information	12



6.4	Engagement of external experts	12
6.5	Findings	12
7.	Follow up and resolution.....	12
7.1	Review and Approval	12
7.2	Decision-Making.....	12
7.3	Implementation of Corrective Actions.....	12
7.4	Follow-Up and Monitoring.....	12
7.5	Communication.....	13
7.6	Documentation and Recordkeeping	13
8.	Reporting to an external channel.....	13
9.	Compliance.....	13
Annex 1	14
Annex 2	15

1. Introduction & Scope

The purpose of this policy is to establish a framework that encourages employees and other stakeholders to come forward with information on any potential wrongdoing, misconduct, or unethical behavior within ATG Netherlands B.V. (hereafter referred to as ATG Netherlands, ATG or the Company). By providing a secure and confidential channel for reporting, we aim to identify and address issues promptly, protecting the well-being of the company and its employees. This policy is fully compliant with EU Whistleblower Directive (EU)2019/1937 and adheres to the provisions outlined in the Dutch Whistleblowers Protection Act (*Wet bescherming klokkenluiders*).

This policy applies to anyone who, in the context of their work, reports a suspicion of wrongdoing within ATG Netherlands B.V. It is designed to encourage the reporting of concerns in good faith without fear of retaliation.

A wrongdoing is considered to be in the public interest when it affects interests beyond those of individuals involved and extends beyond personal conflicts or individual issues. This means that the nature and scope of the issues or conflicts must go beyond mere individual interests. Additionally, the wrongdoing must either demonstrate a pattern or structural nature, or it must be sufficiently serious or extensive to impact the public interest.

The Whistleblower must have a working relationship with the Company to which the suspicion is related. This is typically an employee, i.e. a person with an employment contract, but that is not necessary. A Whistleblower can therefore also be a self-employed person (e.g. a consultant, freelancer, contractor, or supplier), director, shareholder, intern, employee of a business partner etc. What matters is that the Whistleblower is going to perform, is performing or has performed activities for ATG Netherlands. A former employee or another person whose working relationship has ended but also job applicants and other people whose working relationship has yet to start are then included under this concept.

In accordance with Dutch law, these persons may blow the whistle if they have reason to believe there is a wrongdoing within ATG or one of ATG's business partners:

1.1 A (danger of) violation of a statutory regulation or internal rules of an employer

Any suspicion of a (potential) violation of statutory regulations or internal rules of the employer should be reported. This includes instances where employees observe or suspect actions that contravene established laws or company policies.

1.2 A risk to public health

Suspected breaches posing risks to public health. This includes situations where activities or conditions may endanger the health and well-being of the public.

1.3 A risk to the safety of persons

Any perceived threats to the safety of individuals, whether employees, customers, or the general public. This encompasses hazards or conditions that may cause harm or injury to persons.

1.4 A risk of environmental degradation

Suspicious activities or practices that could lead to environmental degradation, pollution, or harm to natural ecosystems. This includes incidents that may result in adverse impacts on air, water, soil, or biodiversity.

1.5 A risk to the proper functioning of the Company as a result of improper actions or negligence

Suspected improper actions or negligence jeopardizing the proper functioning of the Company. This encompasses behaviors or decisions that may undermine the Company's integrity, reputation, or operational effectiveness.

1.6 A violation of European Union law.

1.6.1 Public Procurement

Suspected irregularities or fraudulent activities related to contracts funded by the EU fall within this category. Any indications of corruption, bribery, or favoritism in the awarding or execution of EU-funded contracts.

1.6.2 Financial services, products and markets, prevention of money laundering and terrorist financing

Suspicious activities, non-compliance, or fraudulent activities within financial services, products, and markets regulated by EU directives. This includes breaches related to banking, insurance, investment services, securities markets, and the prevention of money laundering and terrorist financing.

1.6.3 Product safety and product compliance

Any concerns regarding the safety, quality, or compliance of products with EU regulations. This includes suspicions of defective or non-compliant products that pose risks to consumers' health or safety.

1.6.4 Transport safety

Suspected violations or risks to traffic safety, including non-compliance with EU regulations on vehicle standards, road infrastructure, transportation services, and road safety measures.

1.6.5 Environmental protection

Suspicious activities or practices that violate EU environmental regulations or pose risks to environmental conservation and sustainability. This includes incidents of pollution, improper waste management, habitat destruction, or biodiversity loss.

1.6.6 Radiation protection and nuclear safety

Suspected breaches of EU regulations on radiation protection and nuclear safety, including incidents involving nuclear facilities, radioactive materials, and radiation-emitting devices.

1.6.7 Food and feed safety, animal health and welfare

Concerns regarding food safety, feed safety, and the health and welfare of animals within the EU's agri-food sector.

1.6.8 Public health

Suspicious of threats to public health arising from breaches of EU regulations on healthcare, pharmaceuticals, medical devices, disease control, or health standards.

1.6.9 Consumer protection

Suspected violations of EU consumer protection laws, including unfair commercial practices, misleading advertising, product labeling discrepancies, or breaches of consumer rights.

1.6.10 Protection of privacy and personal data and security of network and information systems

Concerns related to breaches of EU data protection laws, privacy violations, unauthorized access to personal data, or inadequate cybersecurity measures.

1.6.11 Breaches affecting the financial interests of the EU

Suspected irregularities, fraud, or misuse of EU funds, subsidies, grants, or resources that impact the financial interests of the EU.

1.6.12 Infringements related to the internal market of the EU

Suspected violations of EU rules governing the internal market, including competition law, free movement of goods, services, capital, and persons.

These reasons provide guidance to employees on the types of concerns they can report under the Whistleblower policy, ensuring alignment with Dutch legal requirements and EU Law, and promoting accountability and integrity within the Company. The suspicion must be based on reasonable grounds, which arise from the knowledge that the Whistleblower has acquired from the Company as an employee or arise from the knowledge that they have acquired through their work at or with another Company (ATG business partner).

Each report will have to be assessed on whether there is wrongdoing within the meaning of the law. The public interest is at stake, as required, if the act or omission does not merely affect personal interests and there is either a pattern or structural character or the act or omission is serious or extensive.

2. Responsibilities

Title	Responsibilities <i>(In addition to tasks & responsibilities described in the job description)</i>
<ul style="list-style-type: none">HR Director	Owner of this document, responsible for ensuring that this procedure and related actions are conducted as described, responsible for updating of the procedure and related actions, in

Title	Responsibilities <i>(In addition to tasks & responsibilities described in the job description)</i>
	order to reflect the changes and requirements within the Company or as a result of external factors.
<ul style="list-style-type: none"> Whistleblowing Case Manager for ATG Netherlands B.V. 	Bertilla Sinka, Quality and Information Manager. Responsible for following procedures and related instructions as well as for providing feedback on current ways of working.
<ul style="list-style-type: none"> Legal & Contract Manager 	Provides legal advice to the Whistleblowing Case-Manager during the whole process

3. Definitions

Title	Description
Whistleblower	Any individual who reports concerns about misconduct, illegal activities, or violations of company policies
Protected Disclosure	Information provided by a Whistleblower in good faith and with a reasonable belief that it is accurate
Retaliation	Any adverse action taken against a Whistleblower in response to their disclosure
Whistleblower tool	Secure online reporting tool https://atg.integrityline.com

4. General Principles

4.1 Key Principles

The Whistleblowing policy is based upon the following key principles:

- confidentiality safeguards
- protection against retaliation
- anonymous reporting
- objective investigation of reports

4.1.1 Confidentiality safeguards

The Company is committed to maintaining the confidentiality of whistleblowers to the extent possible, in compliance with applicable law, including the General Data Protection Regulation (GDPR), and the need to conduct a thorough investigation.

The Whistleblowing Privacy Notice, ref. ATG-ISMS-DOC-A05-34-9 can be found On Stargate in the ATG Knowledge Base, but also on the ATG Website at <https://www.atg-europe.com/privacy-statement/>.

4.1.2 Protection against retaliation

The Company strictly prohibits retaliation against whistleblowers in accordance with the EU Whistleblower Directive and the Dutch Whistleblower Protection Act. Retaliation shall not take place in any form, including but not limited to suspension, dismissal, demotion, withholding promotion, a negative review, a written reprimand, reduction of wages, change of work location, refusal to provide a reference, libel or slander, bullying, harassment, and exclusion. This also applies to natural persons and legal persons supporting a Whistleblower.

Even if the Whistleblower has violated rules or obligations, they are not held accountable if they reasonably believed it was essential to contravene those rules to expose a breach and had reasonable grounds to believe the accuracy of the information provided. The burden of proof rests with the Company to demonstrate otherwise.

Whistleblowers, involved parties, and individuals assisting a Whistleblower are entitled to legal aid. The Dutch Legal Aid Act (*Wet op de rechtsbijstand*) provides a system of subsidized legal assistance for individuals or legal entities with insufficient financial means.

4.1.3 Anonymous reporting

Anonymous reporting can be done online via [ATG - Home \(integrityline.com\)](https://www.atg-europe.com/integrityline.com), ensuring confidentiality and direct communication with designated Whistleblowing Case Manager responsible for handling reports. This communication can occur without revealing the reporter's identity.

4.1.4 The investigation process

Upon receiving a report through the web-based reporting tool. The Whistleblowing Case Manager will initiate an internal investigation. The investigation will focus on identifying and addressing reported concerns, ensuring compliance with company policies and legal requirements in accordance with the procedures outlined in the Dutch Whistleblower Protection Act.

5. Reporting Process

Employees, contractors, consultants, suppliers, and other stakeholders are encouraged to report concerns about unlawful activities, unethical behavior, fraud, or any other wrongdoing within ATG, using the designated online reporting tool. This reporting procedure ensures confidentiality, security, and transparency in handling reported concerns. The Whistleblower has the possibility to consult the ATG Confidant (*vertrouwenspersoon*, at the moment of writing Barbara Emmigje van Marle) in confidence about a suspected misconduct. They can also consult an external advisor (e.g. a lawyer) for advice and support.

5.1 Accessing the Reporting Tool

Whistleblowers can access the online reporting tool via a designated tool weblink [ATG - Home \(integrityline.com\)](https://integrityline.com). ATG encourages all interested persons to use this tool for whistleblowing purposes to ensure the correct record-keeping.

5.2 Anonymous Reporting Option

The online reporting tool includes an option for anonymous communication via an encrypted connection. When using the tool, the IP address and current location of the Whistleblower are not stored at any time. After sending a report the Whistleblower receives login details to access the tool's inbox so that they can continue to communicate with the Case Manager in a secure and anonymous way.

5.3 Other means of reporting

Reporting made by telephone or in an on-site conversation or through a video conferencing tool is captured by recording the conversation in a durable and retrievable form (with prior consent of the notifier) or by providing a complete and accurate written account of the conversation, subject to approval by the Whistleblower.

The report should then be kept confidential and immediately transferred to the relevant Whistleblowing Case Manager, who will record it appropriately in the tool. This also applies to reports presented to the wrong person or submitted to the wrong Whistleblowing channel. The report must be transferred within seven days of its receipt to the correct Case Manager, giving simultaneous notice of the transmission to the Whistleblower.

5.4 Submission of Report

Whistleblowers are required to fill out the necessary fields in the reporting tool with details of their concerns. This includes providing a description of the incident, relevant dates, the affected department, relevant dates, names of individuals involved (if known), and any supporting evidence or documents. The report may be either in writing or in the form of a voice message recorded in the tool. In case anonymity is selected, the tool will automatically change the voice in the recording so that it is unrecognizable.

The Whistleblower is strongly encouraged to avoid including unnecessary personal data that is not directly relevant or needed for the reporting. While providing relevant information is crucial for the investigation process, the Whistleblower should refrain from disclosing personal data beyond what is essential for the investigation and resolution of the reported concern.

The Whistleblower also has the right to ask for an in-person or videoconference meeting in the tool. ATG will arrange the meeting within a reasonable time. However, in this case it is of course impossible to report anonymously. In such a case, the relevant Whistleblowing Case Manager will make notes of the meeting, which the Whistleblower may comment on and, once ready, confirm with their signature.

The report will be received and handled by the relevant Whistleblowing Case Manager (or in their absence by another Whistleblowing Case Manager within ATG).

5.5 Confidentiality and Security

ATG is committed to maintaining the confidentiality and security of the information submitted through the reporting tool. Measures are in place to protect the whistleblower's identity, ensuring that their confidentiality is respected throughout the investigation process. The Company takes measures to ensure that every person who received confidential information in relation to a report maintains secrecy.

Confidential information includes e.g. the identity of the Whistleblower, the identity of persons named in the report and trade secrets. Personal data which are manifestly not useful for processing of a specific report are not collected, or if collected accidentally, are immediately deleted.

In cases where an investigation into the reported wrongdoing is initiated, it may be necessary to disclose the identities of individuals identified as wrongdoers or witnesses in the report. This disclosure is essential for conducting a thorough investigation and may be required for disciplinary proceedings or other corrective actions. Such disclosure will be handled with the utmost confidentiality and discretion, limited only to those individuals directly involved in the investigation process.

5.6 Confirmation of Receipt

Whistleblowers will receive acknowledgment of receipt within seven days of submitting their report. This acknowledgment confirms that the concern has been received and will be investigated accordingly.

5.7 Tracking and Follow-Up

Whistleblowers can track the status of their report through the online reporting tool. They are encouraged to provide any additional information or updates related to their concerns, either proactively or upon request of the Whistleblowing Case Manager. The Whistleblower shall get information on the evaluation of their report, including steps (to be) taken as a result, as soon as possible but at the latest within three months from confirmation of receipt of the report. Even if no further follow-up is given to the report, the Whistleblower will be informed of this and the reasons for this decision will be given.

6. Investigation Process

For the purpose of ensuring thoroughness and clarity throughout the investigation process, an investigation plan will be drafted. The investigation plan encompasses the following steps:

6.1 Objectives

- Determine the facts surrounding the reported concerns. Identify individuals involved in the reported concerns.
- Assess the impact of the reported concerns on the Company.
- Recommend corrective actions to prevent recurrence and mitigate risks.

6.2 Relevant Documents

- Review documents, records, or other sources of information that may provide evidence or context related to the reported concerns.

6.3 Other Sources of Information

- Consider additional sources of information that may be relevant to the investigation, such as surveillance footage or system logs.

6.4 Engagement of external experts

- Engage forensic experts if necessary to conduct specialized examinations.

6.5 Findings

Prepare investigation findings detailing the findings, conclusions, and recommendations upon completion of the investigation.

7. Follow up and resolution

After the investigation findings are drafted, ATG will take the following steps to address the reported concerns.

7.1 Review and Approval

The investigation findings will be submitted to the HRM Director to assess the findings, conclusions, and recommendations and to decide on further action. The Legal & Contract Manager will support the HRM Director.

7.2 Decision-Making

Based on the findings and recommendations outlined in the final report, decisions will be made regarding any necessary corrective actions. If the outcome of the investigation determines that disciplinary measures are justified, the Company's Employee Disciplinary Procedure (ATG-IMS-DOC-07-ATG) or the Disciplinary Procedure for Security Incidents (ATG-ISMS-DOC-A6-4-1) will be applied, as appropriate. The initial investigation already performed under this procedure may then form part of the investigation under the Disciplinary Procedure.

7.3 Implementation of Corrective Actions

Appropriate corrective actions will be implemented to address any identified issues or deficiencies, which may involve updating policies and procedures, improving internal controls, or making organizational changes.

7.4 Follow-Up and Monitoring

ATG will follow up on the implementation of corrective actions to ensure they are effectively addressing the reported concerns, with regular monitoring and review processes established to track progress and identify any ongoing risks or issues.

7.5 Communication

The outcome of the investigation and any actions taken as a result will be communicated to relevant stakeholders, including the Whistleblower (if known) and other employees who may have been impacted by the reported concerns. Additionally, in cases where legal violations or criminal activities are identified, the Company may need to liaise with law enforcement authorities for further investigation and potential legal action.

Furthermore, external stakeholders, such as regulatory bodies, government agencies, or legal advisors, may also be informed as necessary to ensure compliance with legal obligations and facilitate cooperation in resolving issues.

7.6 Documentation and Recordkeeping

Detailed documentation of the investigation process, including the final report and any actions taken, will be maintained in accordance with the Company's recordkeeping policies and any applicable legal requirements.

8. Reporting to an external channel

Whistleblowers are encouraged to first report any suspicion of wrongdoing to the Company. In doing so, the Company has the opportunity to address the report immediately and stop any misconduct as quickly as possible, while also implementing measures to prevent future wrongdoing. However, it is not mandatory to report internally first. If, for any reason, the Whistleblower prefers to report directly to an external reporting point, they may do so. They can report their concerns to an authority with jurisdiction over the subject of the suspected wrongdoing, such as an inspection service or regulatory body. If they choose to report externally, they are entitled to the same protection as with an internal report. Please see Annex 2 with the list of the competent authorities to receive reports.

Note: The main authority for receiving reports externally is the House for Whistleblowers (*Huis voor klokkenluiders*). The procedure for reporting to the House for Whistleblowers may involve additional steps or requirements, which should be followed as per their guidelines <https://www.huisvoorklokkenluiders.nl/> and [Dutch Whistleblower Protection Act | Wet bescherming klokkenluiders](#) (English). The House for Whistleblowers may forward the report to another authority. This will be the case if that other authority is competent in the policy area of the report. If no other authority is competent, the Whistleblowers Authority will handle the report itself.

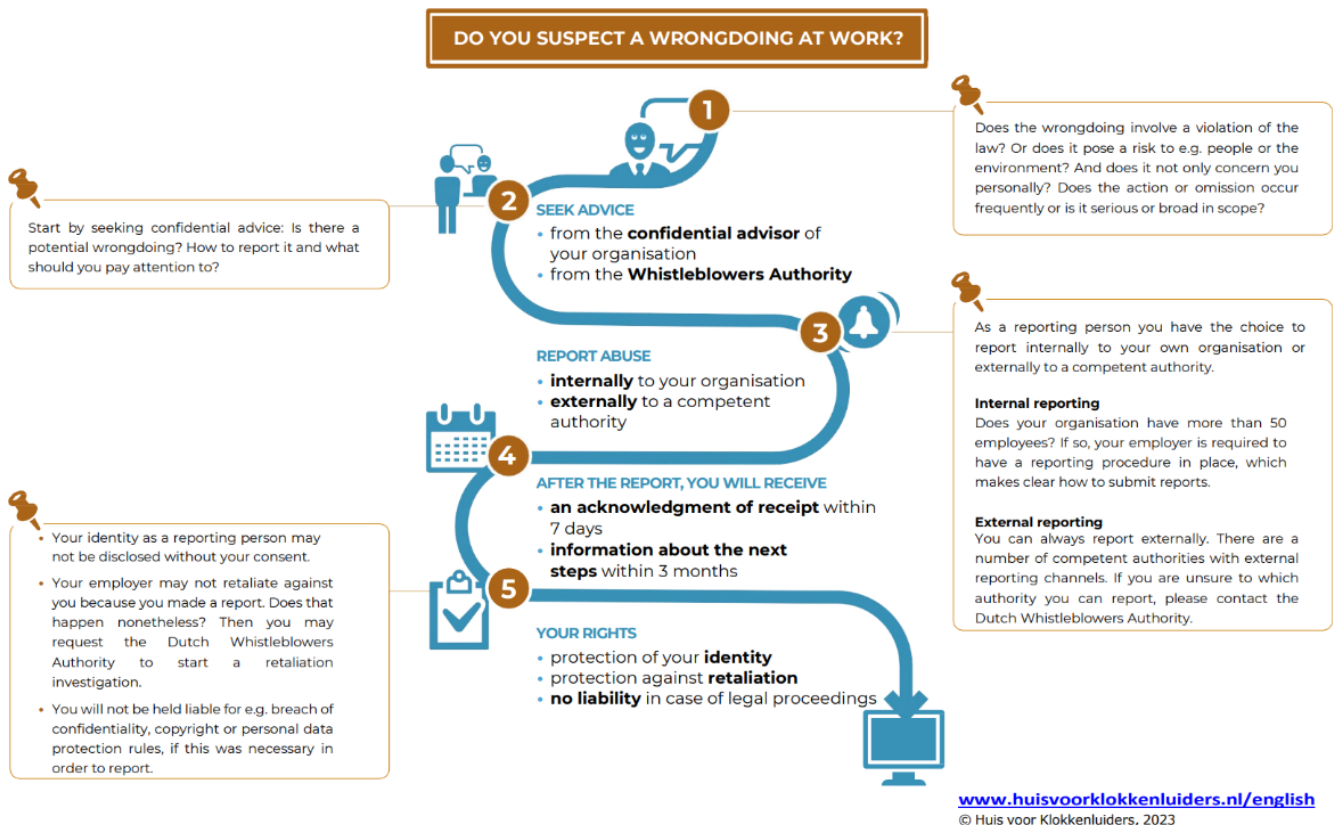
See Annex 1

9. Compliance

The Quality management Team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits.

Annex 1

HOW DO I REPORT A WRONGDOING IN ACCORDANCE WITH THE DUTCH WHISTLEBLOWER PROTECTION ACT?



Annex 2

For the external reporting of a suspicion of wrongdoing, you can contact the following competent authorities:

- het Huis voor klokkenluiders (HvK):
[Ik vermoed een misstand | Huisvoorklokkenluiders.](#);
- de Autoriteit Consument en Markt (ACM):
[Bescherming klokkenluiders | ACM.nl](#);
- de Autoriteit Financiële Markten (AFM):
[Bescherming klokkenluiders \(afm.nl\)](#);
- de Nederlandsche Bank N.V. (DNB):
[Contact en veelgestelde vragen \(dnb.nl\)](#);
- de Inspectie gezondheidszorg en jeugd (IGJ):
[Melden over uw werkgever \(klokkenluidersmelding\) | Inspectie Gezondheidszorg en Jeugd \(igj.nl\)](#);
- de Nederlandse Zorgautoriteit (NZa):
[Meldpunt misstanden bij zorgaanbieders of zorgverzekeraars \(klokkenluiders\) | Contact | Nederlandse Zorgautoriteit \(nza.nl\)](#);
- de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS):
[Overtreding of misstand melden | Autoriteit NVS](#);
- de Autoriteit persoonsgegevens (AP):
[Autoriteit Persoonsgegevens |](#)
- de Inspectie Leefomgeving en Transport (ILT):
[Home | Inspectie Leefomgeving en Transport \(ILT\) \(ilent.nl\)](#);
- de Nederlandse Arbeidsinspectie (NLA):
[Home | Nederlandse Arbeidsinspectie \(nlarbeidsinspectie.nl\)](#);
- de Nederlandse Voedsel- en Warenautoriteit (NVWA):
[Home | NVWA.](#)

The aforementioned authorities all have their own areas in which they are authorized to investigate the report. If there is no specific regulatory authority with jurisdiction, then the House for Whistleblowers is permitted to conduct an investigation into a report.