Whistleblower Policy

---

1 Purpose

Group PSA consisting of the following entities:

- PSA Antwerp - Napelsstraat 79, 2000 Antwerp - 0442.652.075
- PSA Finance Europe - Napelsstraat 79, 2000 Antwerp - 0882.346.048
- MPET - Napelsstraat 79, 2000 Antwerp - 0552.527.539
- ATS - Napelsstraat 79, 2000 Antwerp - 0506.666.137
- PSA Breakbulk - Napelsstraat 79, 2000 Antwerp - 0689.746.214
- PSA Zeebrugge - Caxtonweg Q140-143, 8380 Zeebrugge - 0808.254.478
- PSA Baltics - Napelsstraat 79, 2000 Antwerp - 0715.850.397
- PSA Supply Chain Solutions - Napelsstraat 79, 2000 Antwerp - 0776.990.091
- PSA Investments - Napelsstraat 79, 2000 Antwerp - 0671.672.441
- PSA Genoa Investments - Napelsstraat 79, 2000 Antwerp - 0751.776.823

hereinafter referred to as "the Companies" want to act with integrity and ethics in their activities and therefore they want to ensure that their employees have the opportunity, in accordance with the terms and conditions set out below, to report identified or suspected violations of the provisions to the legal and regulatory standards, referred to in point 2.2 of this policy, within the Companies, in the most serene and confidential manner.

It is often their own employees who are the first to know about threats or breaches occurring within a company. However, they might become reluctant to raise concerns or suspicions for fear of backlash or reprisals.

This potential fear could ultimately result in the Companies being kept in the dark about possible breaches and unable to take the necessary steps to address them. As a result, this could constrain the interests of the Companies, which are committed to high standards of good governance and professional ethics.

The purpose of this policy is to prevent this situation by strongly encouraging all employees and other persons, who have a contractual relationship with the Companies, to report any breach, illegal, unethical or fraudulent activity, related to the Companies' business, without fear of sanctions or other measures.

This policy has been established in accordance with the Law of 28 November 2022 on the protection of reporters of breaches of the Union law or the national law, established within a legal entity in the private sector, transposing the European Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of the Union law, hereinafter referred to as "the Law".

This policy aims to:

- enable the confidential reporting of information about possible or actual infringements, anonymous or not.
- offer protection to persons reporting an infringement or assisting the reporter.
- lay down the procedure to be followed by the reporter of an infringement.

This policy is available on the Companies' intranet (Be Connect), and may be amended from time to time. This policy is a supplement to the 'Code of Conduct' and specifically in elaboration of the Belgian legislation on whistleblowers (see above).

Of course, this policy in no way excludes the direct dialogue and the communication of information, outside the reporting procedure. The Companies wish to emphasize that employees with concerns or suspicions can turn to their immediate supervisors, to HR or to the Compliance department (Legal), at any time.

2 Scope of application

2.1 Who does this policy apply to?

This policy applies to the following persons:

- current and former employees who are, or were, associated with the Companies under an employment contract;
- candidates who are, or were, involved in a recruitment procedure in the Companies;
- persons who work, or have worked, on an independent basis with the Companies, and the candidates for independent cooperation in the context of pre-contractual negotiations;
- volunteers and trainees (paid or unpaid);
- shareholders and members of the administrative, management or supervisory body of the Companies (including non-executive members);
- any person who works, or has worked, under the supervision and direction of contractors, subcontractors, and/or suppliers of the Companies;
- anyone who has information about infringements in the Company's financial services, products and markets, even outside of a work-related context

2.2 Which breaches can be reported?

Only breaches that relate to any of the following areas as defined in the Law can be reported:

- Public procurement;
- Financial services, products and markets, prevention of money laundering and terrorist financing;
- Product safety and product compliance;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and animal welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, and security of network and information systems;
- Combating tax fraud;
- Social fraud prevention.

In addition, infringements that may harm the financial interests of the European Union can be reported, as well as infringements related to the European internal market, including Union rules on competition and state aid.

Infringement means the act or omission that is unlawful or contrary to the purpose or application of the rules in the above-mentioned areas. It refers to any infringement of the legal or regulatory provisions on the matter, or the provisions taken in implementation of the provisions mentioned above.

3 The notification

3.1 Purpose of the notification

Any breach relating to the areas referred to in point 2.2, as well as any information about such breaches, including any reasonable suspicion of actual or potential breaches, that have taken place or are highly likely to take place within the Companies, and attempts to conceal such breaches within the Companies, can be notified in writing or verbally through one of the channels referred to in point 4.

3.2 Conditions for notification and protection

The report must be made in good faith and must not be based on mere rumor or gossip, nor must the report be intended to harm the Companies.

The reporter must have reasonable grounds to believe that the information about the violations was true at the time the report was made.

If the report contains false, unsubstantiated, or opportunistic allegations, or is made with the sole purpose of harming or damaging others, the Companies may take appropriate disciplinary and/or judicial action against the reporter, including the imposition of sanctions in accordance with the Companies' employment regulations.

4 Reporting channels

Any person, covered by this policy, who has information about actual or suspected breaches, referred to in point 2.2, is encouraged to report it to the Companies as soon as possible, in good faith, and in accordance with the principles set out in point 3.2. Before using the specific reporting channels below, it is preferable for the employee to initially report to the immediate supervisor, to the head of department, to HR or to the legal department.

4.1 Internal reporting channels

4.1.1 Who can use the internal reporting channel?

All employees or other persons, covered by this policy, are allowed to use the internal reporting channels, provided by the Companies.

4.1.2 Which channels are available?

If an employee or other person cannot, or does not wish, to report to the direct supervisor, to the department head, to HR or to the Legal Department, the specific channels below can be used:

- psaantwerp.sdwhistle.com
- psa.sdwhistle.com
- mpet.sdwhistle.com
- ats.sdwhistle.com

Or:

- By post to the following address: HR, Napelsstraat 79, 2000 Antwerp
- By phone or email to the known confidential advisers within the Companies

The notification should preferably be made in Dutch, French or English. Any notification, made in another language, will have to be translated first, as this may affect the accuracy of the content of the notification.

These reporting channels are always accessible, 24/7.

It is also possible to request a face-to-face meeting with the reporting manager, as mentioned below in point **4.1.4** of this policy.

Each of the above channels is managed in a confidential and secure manner to ensure the confidentiality of the identity of the reporter and any third parties, named in the report. Access to the channels is strictly limited to employees who have access to them, based on responsibilities and/or powers.

4.1.3 How does the notification proceed?

A notification shall include a brief description of the reasonable suspicions about a committed or possible breach of any of the domains listed in Article 2.2, that has occurred or is highly likely to occur, as well as any attempts to conceal or disguise such breaches.

At the discretion of the reporter, the report can be made anonymously, or not, on the channels mentioned in Article 4.1.2.

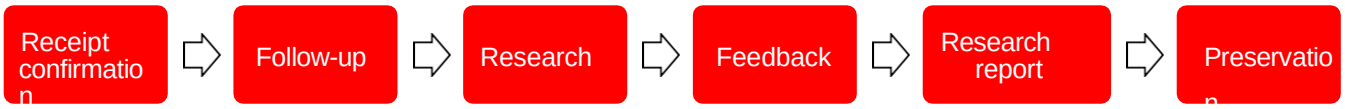
The Companies do not encourage reporting in an anonymous manner, as this prevents the Companies from properly investigating and dealing with the notification. However, if the reporter would still not feel comfortable, the reporter can of course choose to remain anonymous. The Companies will of course respect this choice of the reporter and an anonymous report will be taken as seriously as a non-anonymous report.

The notification should be sufficiently detailed and documented and should include the following details (when the relevant information is known):

- A detailed description of the incident, and how it came to the attention of the reporter;

- the date and place of the incident;
- the names and functions of the persons concerned, or information enabling their identification;
- the names of other persons, if any, who can confirm the reported facts;
- when making a report, the name of the reporter (this information is not requested when an anonymous report can be made); and
- any other information or elements that may help the investigation team to verify the facts.

4.1.4 What happens after the notification?



1- Receipt confirmation

The author of the notification will receive an acknowledgement of receipt within 7 days of notification.

2- Follow-up

Follow-up refers to any action taken by the recipient of a report to verify the accuracy of the allegations, made in the report, and to address the reported breach, if necessary, including through measures, such as an internal preliminary investigation, an investigation, a prosecution, a recovery of funds, or the termination of the proceedings.

The reporting manager follows up on reports, maintains communication with the reporter, requests additional information, if necessary, links back to the reporter and takes in any new reports.

3- Research

The reporting manager can decide whether to investigate a report, or not, after consulting with the management within the organization.

Reports will be investigated promptly and carefully in accordance with this policy. All investigations will be conducted thoroughly with due regard to the principles of confidentiality, impartiality and fairness to all persons involved. The reporting manager will establish an investigation team, if necessary.

Persons involved in the breaches or potential breaches, reported by the reporter, will be excluded from the investigation team, nor are they allowed to participate in the assessment of the report or the determination of the actions to be taken regarding the report.

Conflicts of interest are reported to the board of directors if the management/executive board is targeted in the report. If the board of directors appears to be involved, the general meeting of the Companies will be notified.

4- Feedback

The reporting manager will provide appropriate feedback to the reporter within a reasonable time, and at most within three months from the date of the acknowledgement of receipt of the report. This feedback contains information for the reporter on the measures planned and/or taken and the reasons for these measures. He/she informs the reporter through the chosen internal reporting channel.

5- Research report

Upon completion of the investigation, the investigation team will prepare a summary report, describing the investigative actions taken. A redacted, non-confidential and anonymized version of this overview

report may be shared, on a need-to-know basis only, outside the investigation team with the local or executive management to reach a final decision.

A member of the investigation team prepares a final report describing the facts and the final decision:

i. If the (potential) breach is proven, relevant actions are identified with a view to countering the (potential) breach and protecting the Company; or
ii. In case the investigation shows that there is insufficient or no evidence of the (potential) breach, no further action will be taken.

The reporter will be informed of the closure of the report and the decision taken via the internal reporting channel chosen by them.

4.1.5 The notification manager

The known confidential advisers within the Companies will be designated as notification managers of the Companies.

The reporting managers perform their duties independently and without any conflict of interest. They are subject to a duty of confidentiality.

4.1.6 Registration of notifications

The Companies keep a record of all reports received, in accordance with the confidentiality measures set out in section 5.1 of this policy.

These reports and the related information are kept for as long as the contractual relationship between the reporter and the Companies continues and for a maximum period of five years.

Where, with the consent of the reporting person, the report is made using a recorded telephone line, or other recorded voice messaging system, the Companies will record the oral report as follows:

- by a recording of the conversation in a durable and retrievable form; or
- by a full and accurate written statement of the conversation, prepared by the reporting managers. The reporter will be given the opportunity to check, correct and sign this written statement for approval.

If a telephone line without call recording or other voice message system without call recording is used for reporting, the Companies will record the verbal report in the form of an accurate record of the conversation, prepared by the handling of the staff member responsible for the report. The reporter will be given the opportunity to check, correct and sign this report for approval.

In case a face-to-face meeting takes place with a reporting manager, provided the reporter agrees, a complete and accurate record of the interview will be kept in a durable and retrievable form. The Companies have the right to record the interview as follows:

- by a call recording in a durable and retrievable form;
- by an accurate record of the interview. The reporter will be given the opportunity to check this report, correct it and sign it for approval.

4.2 External reporting channels

1-
Reporters can use an external reporting channel after reporting through the internal channels or directly through the external reporting channels, if they consider it more appropriate.

2-
The Federal Coordinator is charged by the Belgian legislature with coordinating notifications, introduced through external channels.

He/she is responsible for receiving external reports, for checking their admissibility, and for forwarding them to the competent authority for investigation, which will be different depending on the subject of the report.

This authority could be, for example, the FPS Policy & Support (in the field of public procurement), the Financial Services and Markets Authority (FSMA), the National Bank of Belgium (NBB) or the College of Supervision of Auditors (in the field of financial services, products and markets), the FPS Economy (in the field of consumer protection), the Data Protection Authority (in the field of privacy and personal data protection), etc.

In exceptional cases, the Federal Coordinator may also conduct the substantive investigation.

The Federal Coordinator's contact details are as follows:

Address: Leuvenseweg 48 bus 6, 1000 Brussels
Online complaint: https://www.federaalombudsman.be/nl/klachten/dien-een-klacht-in Email: contact@federaalombudsman.be
Phone: 0800 99 961
Fax: 02 289 27 28

5 Protective measures

The Companies are committed to make every effort to provide appropriate and effective protection to the persons covered by this policy to the extent that the notification meets the conditions of the Law, in particular by taking the following measures:

5.1 Safeguarding confidentiality

The Companies guarantee to take the necessary measures so that employees and other persons, targeted by this policy, can file a report with the Companies in confidence.

The Companies undertake to provide the necessary measures so that the identity of the reporter cannot be disclosed to persons other than staff members, authorized to receive or follow up reports, without his free and express consent.

This also applies to any information from which the identity of the reporter can be directly or indirectly deduced.

In deviation from the previous paragraph, the identity of the notifier of the infringement may be disclosed, where this is necessary and proportionate under special legislation in the context of an investigation by the national authorities, or in the context of judicial proceedings, in particular to protect the rights of defense of the person concerned.

In the latter case, the reporter will be informed of the disclosure of his or her identity before it takes place, unless such information would jeopardize ongoing investigations or legal proceedings. This is the case, for example, if the reporter represents an important witness in court, or in cases of unjustified or wrongful reporting to protect the person's defense rights.

5.2 Protection against reprisals

Any form of retaliation against the persons referred to in Article 2.1, who enjoy protection under this policy, including threats of retaliation and attempted retaliation, is prohibited, particularly in the following forms:

- suspension, temporary decommissioning, dismissal, or similar measures
- degradation or refusal of promotion;
- change of job, change of workplace, reduction of wages, change of working hours;
- suspension or refusal of training
- negative performance rating or negative reference;
- imposing or applying a disciplinary measure, reprimand or other sanction, including a financial penalty;
- coercion, intimidation, harassment or exclusion;
- discrimination, adverse or unequal treatment;
- failure to convert a temporary employment contract into an open-ended employment contract, when the employee had the legitimate expectation that he would be offered an open-ended employment contract;
- non-renewal or early termination of a temporary employment contract;
- damage, including reputational damage, especially on social media, or financial loss, including loss of sales and revenue;
- blacklisting, based on an informal or formal agreement for an entire sector or industry, which prevents the reporter from finding work in the sector or industry;

- early termination or cancellation of a contract for the supply of goods or services;
- revocation of a license or permit;
- psychiatric or medical referrals.

6 Processing of personal data

In the context of the internal reporting procedure, the Companies are considered to be responsible for the processing of personal data.

Any processing of personal data under this policy will be carried out in accordance with applicable personal data protection laws, including the European General Data Protection Regulation ("GDPR").

The following personal data can be processed in the context of a report: name, position, date of employment, contact details and e-mail address of the reporter and of persons, involved in the breach, any identified or identifiable information, provided by the reporter and collected in the context of the internal investigation. This processing of data is done in the context of complying with a legal obligation and/or the legitimate interest of the Companies, to the extent that the internal reporting channel exceeds the legal objectives, in particular the detection of breaches, ensuring the security and the ethical conduct of the Companies.

Personal data, clearly irrelevant to the processing of a report, shall not be collected or, if collected, shall be deleted as soon as possible. Such data will be kept until the breach reported is time-barred and in any case for a period of five years after the report.

The identity of the reporter can only be disclosed with the reporter's consent. Other information also remains strictly confidential and is shared only on a strict need-to-know basis.

All individuals whose personal data are processed in the context of breach notifications have the right of access and the right to get a copy, the right to rectification, the right to data erasure, the right to object and the right to lodge a complaint with the supervisory authority in accordance with the applicable law. However, these rights may be limited by the rights and freedoms of others, in particular the reporter's right to confidentiality and the Companies' right to a proper follow-up on the report.

7 Entry into force

This policy takes effect on 15 February 2023 for an indefinite period.

The Companies reserve the right to amend this policy at any time, including, but not limited, to changes in relevant legislation and/or operational needs.