3.22 Whistleblowing

1. Policy

This Policy seeks to ensure that adequate tools, procedures and safeguards are in place for FedEx Team Members and Third Parties to report information on actual or potential breaches that fall within the material scope of Dutch Law, as recently amended in order to implement the EU Directive on the protection of persons who report breaches of Union law ('the EU Whistleblowing Directive'). It does not limit the responsibility of FedEx Team Members to speak up and report other types of suspected breaches as referred to in the FedEx Code of Conduct and the FedEx Global Policy on Reporting Concerns. In the event of any contradiction or conflict between the terms of this Policy and the provisions of the applicable local law and regulation, the latter shall prevail.

Scope

This Policy applies to FedEx Team Members and Third Parties as defined below.

2. Definitions

- **Breach (in Dutch: "*Misstand*")**: a former, actual or potential breach of EU law, or another act or omission that falls within the material scope of Dutch Law:
  - A former, actual or potential breach of national law, or internal procedures that impose an obligation to act for FedEx and that are established to implement a statutory requirement, insofar it puts the public interest at risk; or
  - A malpractice threatening public health, safety of persons, the environment, the good functioning of the public service or of the organization, insofar it puts the public interest at risk.
- **Central Case Administrator**: a person in the Europe Legal Department authorized to receive reports, acknowledge their receipt and initiate or perform diligent follow-up action.
- **Corporate Integrity and Compliance**: the department that ensures that the FedEx Alert Line and surrounding processes are fit for purpose from a functionality and legal / privacy perspective.
- **Dutch Law**: the Act on the Protection of Whistleblowers dated 25 January 2023.
- **Investigative Function**: the department that is authorized and considered best placed to investigate a report.
- **Local Case Administrator**: a person of the Legal or Human Resources Department authorized to receive reports at local entity level, acknowledge their receipt and initiate or perform diligent follow-up action.
- **Regional Case Administrator**: a person in the Regional (i.e. Benelux) Legal Department authorized to receive reports, acknowledge their receipt and initiate or perform diligent follow-up action.
- **Report:** the oral or written communication of information on a Suspicion of Breach in scope of this policy.
- **Reporting Person:** a natural person who reports or publicly discloses information on a Suspicion of Breach acquired in the context of his or her work-related activities.
- **Suspicion of Breach (in Dutch: "*Vermoeden van een misstand*"):** a reasonable suspicion, insofar based on the knowledge of the Reporting Person acquired at work or in a work-related context, of a Breach at the organization where the Reporting Person works, has worked, or at another organization in which the Reporting Person was involved in the work-related context.
- **Team Member**: every officer, director, manager and employee of FedEx.

- **Third Party**: any individual, including former team members, who acquired information on a Suspicion of Breach. This includes former, current or future: agents; temporary agency staff; job candidates; contractors; consultants; freelance workers; service providers; subcontractors; suppliers; distributors; business partners; shareholders; persons in administrative, management or supervisory bodies; volunteers; (paid or unpaid) trainees; any persons working under the supervision and direction / management of a contractor, subcontractor or supplier; or any other person with whom FedEx did, does or may do business.

3. Guidelines

3.1. Types of breaches in scope of this Policy

This Policy applies to the reporting of information on a Suspicion of Breach as defined above.

These include, for example, breaches of EU Law (e.g. breaches in relation to a tender issued by a public authority, money laundering and terrorist financing, protection of the environment, public health or food safety); breaches affecting the financial interests of the EU (e.g. fraud, corruption and any other illegal activities affecting the financial interests of the European Union); breaches relating to the EU internal market (e.g. competition law infringements); and a variety of other matters.

A Report for the purpose of protecting purely private interests is excluded from the scope of this Policy.

3.2. Channels for internal reporting

A suspicion of Breach governed by this Policy can be reported in writing, orally, or both. Reports can be made through one of the following channels:

4.2.1.The FedEx Alert Line

The FedEx Alert Line is a service that FedEx contracts for through an independent vendor at FedEx group level. Reports to this service may be made by calling a toll-free telephone number or by completing an online questionnaire. Both the telephone hotline and online reporting tool are available 24-hours a day for use by FedEx Team Members and Third Parties.

Contact details:

Phone:	0800-023-4237
Online:	fedexalertline.com

4.2.2.Your Local Reporting Channel

A Reporting Person may also choose to reach out directly to the local reporting channel established at legal entity level:

For FedEx Express Netherlands B.V.:

Voice mail:	0031 88 393 9191
E-mail:	NL.whistleblowing@fedex.com
Face-to-face:	By sending a request by voice mail or e-mail

For FedEx Express International B.V.:
Voice mail: 0031 23 7994692
E-mail: NL2.whistleblowing@fedex.com
Face-to-face: By sending a request by voice mail or e-mail

For FedEx Supply Chain Services Netherlands B.V.
Voice mail: 0031 23 7994693
E-mail: NL3.whistleblowing@fedex.com
Face-to-face: By sending a request by voice mail or e-mail

FedEx provides Reporting Persons with the opportunity to reach out to the internal reporting channel of their choice (i.e., to the FedEx Alert Line at group level or to the local reporting channel at legal entity level). If there is reason to believe that a member of the entity's leadership or a member of the entity's Legal, Human Resources or Security department may be involved in a Breach or may not be impartial, the Reporting Person is advised to make a Report through the FedEx Alert Line and explain the potential conflict of interest or risk of partiality (or vice versa).

The Reporting Person is free to consult an advisor about a Suspicion of Breach.

4.3. Anonymous Reports

All reporting channels allow for anonymous reporting. FedEx strictly prohibits any attempt to discover the identity of Reporting Persons who request to remain anonymous. However, we encourage Reporting Persons to reveal their identity as it is often difficult to investigate certain anonymous Reports. Providing contact information also allows us to communicate with (and provide updates to) the Reporting Person.

4.4. Departments authorized to receive Reports

Reports submitted through the FedEx Alert Line are received by a Regional and/or Central Case Administrator and handled in line with FedEx's internal policies and procedures. Reports submitted through a local reporting channel are received by a Local Case Administrator and handled by authorized functions and individuals at central level, or, if the Reporting Person explicitly objects, by authorized functions and individuals within the legal entity.

4.5. Follow-up

Following receipt of a Report, the relevant case administrator will initiate or perform the necessary follow-up activities. These may include, amongst other:

- verifying the Report to assess whether it is in scope of this Policy;
- asking the Reporting Person for further information, where needed;
- aligning internally with other case administrators, with members of the FedEx Legal Department or the FedEx Corporate Integrity and Compliance Department, or with the relevant Investigative Function;
- assigning the matter for further investigation;
- providing feedback to the Reporting Person; and/or
- closing the matter.

A Report may be assigned for further investigation to the relevant Legal, Security or Human Resources Department; the Internal Audit Department or any other internal or external party that is authorized and deemed appropriate to investigate the Report in an independent and objective manner. If the Reporting

Person is of the opinion that any of the above parties may be implicated or may not be impartial, he or she is requested to state this in his or her Report.

Subject to the approval of the Reporting Person, a Local Case Administrator receiving a Report made through a local reporting channel may share the identity details of the Reporting Person and the details of the Report with the regional or central level to handle or to assist with handling the (investigation into the) Report.

4.6. Feedback to the Reporting Person

The Reporting Person will receive a confirmation of receipt within 7 days of receipt of his/her Report. No later than 3 months following that confirmation, the Reporting Person will receive information on the measures envisaged or taken to assess the accuracy of the allegations and, where applicable, the measures taken to remedy the subject matter of the Report.

4.7. Confidentiality

It is the responsibility of all individuals involved in the receipt and/or follow-up of a Report – including those Team Members that receive updates on reported Breaches as part of their role and responsibilities within FedEx – to protect the identity of the Reporting Person and of any other party mentioned in the Report, including the person(s) targeted by the allegations.

The identity of the Reporting Person, nor any other information from which the identity may be directly or indirectly deduced, must not be disclosed to anyone beyond the individuals described above without the free and explicit consent of the Reporting Person, unless there is a necessary and proportionate obligation to disclose imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defence of the person(s) targeted by the allegations.

4.8. Processing of personal data

Individuals involved in the receipt and/or follow-up of a Report must ensure that the processing of personal data is compliant with GDPR. They must not collect personal data which is manifestly not relevant for the handling of the Report. If accidentally collected, such data must be deleted without undue delay.

4.9. Recordkeeping

FedEx will keep records of all Reports received under this Policy. Recording of personal data in these records will be kept to a minimum, and Reports will be stored for no longer than necessary.

FedEx Corporate Integrity and Compliance will take the necessary technical and organizational measures to limit the number of individuals having access to the above records, and to prevent access to these records by non-authorized individuals. It will further ensure that legally binding agreements are in place with external vendors having access to the FedEx Alert Line and related case management system to ensure that the protection mechanisms and safeguards listed in this Policy are being maintained.

4.10. Non-retaliation

FedEx prohibits retaliation, including threats or attempts of retaliation, against anyone who reports a Suspicion of Breach in good faith. Reporting in good faith means 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.

FedEx also prohibits retaliation against (1) any person who assisted a Reporting Person in the reporting process, (2) any person who assisted in an investigation into a Report, (3) third persons who are connected with the Reporting Person and who could suffer retaliation in a work-related context (e.g. colleagues or family members), and (4) legal entities that the Reporting Person owns, works for or is otherwise connected with in a work-related context.

Any Team Member who is found to have breached this non-retaliation principle, or to have threatened or attempted to do so, will be subject to discipline, up to and including termination of the employment relationship.

4.11. Procedures for external reporting

While Reporting Persons are encouraged to first use internal reporting channels, they have the option of reporting a Suspicion of Breach to Competent Authorities and, where relevant, to institutions, bodies, offices or agencies of the European Union.

In the Netherlands, the following bodies are authorized to receive external reports:

- 1° Authority for Consumers and Markets ('ACM')
- 2° Authority for the Financial Markets ('AFM')
- 3° Data Protection Authority ('Autoriteit Persoonsgegevens')
- 4° DNB ('De Nederlandsche Bank')
- 5° Whistleblowers Authority ('Huis voor klokkenluiders')
- 6° Health and Youth Care Inspectorate ('IGJ')
- 7° Healthcare Authority ('NZA')
- 8° Authority for Nuclear Safety and Radiation Protection ('ANVS')
- 9° Other bodies and/or organizations authorized by Dutch law or regulations, with tasks on one of the topics mentioned in article 2 section 1 of the EU Whistleblowing Directive.

5. Policy Related Documents

- Code of Conduct
- Global Policy on Reporting Concerns

Document History

Date of revision	Regional (R) Localised (L) Country (C)	Version	Author(s) (name and position)	Approved by (name and position)	Summary of changes
6 July 2023	C	1.0	Ilse Janssen Senior Legal Counsel I	Jihane El Farri MD Legal	Launch of new policy, including revision and rebranding of existing policy, and re-numbering from 3.31 to 3.22
28 September 2023	C	1.1	Ilse Janssen Senior Legal Counsel I	Sara Mertens MD Leadership, Talent and Employee Experience	Launch of new policy, including revision and rebranding of existing policy, and re-numbering from 3.31 to 3.22