

# Whistleblowing policy

## for reporting dangerous, immoral or illegal practices



At Van de Velde we do our utmost to exclude any form of misconduct or irregularity within the company. But despite all our efforts, misconduct can still occur.

- Our open door policy enables colleagues to discuss such matters face to face with a manager, confidential counsellor or contact person at our HR department.
- There is also a **reporting procedure** at Van de Velde<sup>1</sup>, which is set out in this policy (“Whistleblowing policy”).

The purpose of the reporting procedure is to report breaches (or suspected breaches) while keeping the **identity** of the **reporting person** confidential. Here ‘breach’ means dangerous, immoral or illegal practices for which the employer is responsible. That means the reporting procedure is not meant for issues affecting individuals, such as a conflict between an employee and the employee’s manager.

In this regard, Van de Velde will comply with the applicable privacy laws.

### Article 1 – Legal framework

A European Union directive<sup>2</sup> regarding protection for whistle-blowers was adopted in 2019. This directive provides a **high level of protection for persons who report breaches** and encourages the reporting of any breach anyone is aware of.

Under this directive a reporting procedure for whistle-blowers is only mandatory for the following entities of the Van de Velde group: Van de Velde NV (Belgium) and Van de Velde Nederland BV (Netherlands). The subsidiaries of Van de Velde NV in France and Sweden are covered by the reporting procedure of Van de Velde NV.



- Belgium has enacted the directive into Belgian law<sup>3</sup>.
- In the Netherlands the national law was not yet effective when this policy was rolled out.

To promote transparency and integrity, Van de Velde has decided to **open the inhouse reporting procedure (Article 7) to all entities of the Van de Velde group within the EU.**

<sup>1</sup> Van de Velde NV and its subsidiaries within the European Union.

<sup>2</sup> European Union directive 2019/1937 on the protection of persons who report breaches of Union law.

<sup>3</sup> Law of 28 November 2022 regarding the protection of persons reporting breaches of Union or national law established within a legal entity in the private sector.

This whistleblowing policy protects not only the reporting person but Van de Velde too. Van de Velde collects information that can be useful for eliminating dangerous, immoral and illegal practices. As a consequence, Van de Velde can respond quickly and avoid economic losses.

## Article 2 – Protection of the reporting person

Every person that reports a breach as provided for in Article 4 under the conditions of this policy is protected.

- First and foremost, this protection consists in a **ban on retaliation**. Van de Velde cannot take any actions or refrain from taking any actions with regard to the reporting person if this would be detrimental to the reporting person.
- In addition, **support measures** are in place to help the reporting person during the whistle-blowing procedure.
- Lastly, **protection** is also provided **against retaliation**.

These protective measures are set out in Article 6 of this policy.

As well as the reporting person, the following persons also benefit from the same protection:

- Facilitators: persons who assist the reporting person during the reporting process (such as trade union officials, colleagues and managers);
- Third parties who are connected with the reporting person and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting person;
- Legal entities that the reporting person owns, works for or is otherwise connected with in a work-related context.

## Article 3 – Conditions for protection

To enjoy protection, a reporting person must fulfil all conditions set out below. The **reporting person** will enjoy protection subject to having:

- **reasonable grounds** to believe that the reported information about the breach was true at the time of the report. This is assessed on the basis of the principle of due care.
- **reasonable grounds** to believe that the reported information falls **within the scope of the law**, particularly the breaches stated in Article 4;
- used the **proper reporting channel**, i.e. the internal reporting channel, the external reporting channel or public disclosures.

**Facilitators and third parties connected with the reporting person** also enjoy protection, provided that they had reasonable grounds to believe that the reporting person falls within the scope of this law.

### What about reports that prove to be untrue?

#### 3.1 Report in good faith

The person who reports a breach that is untrue or for which there are no reasonable grounds **in good faith** continues to enjoy protection. Furthermore, it is important for the reporting person to know that:

- a report or public disclosure does not entail gross negligence, fraud or simple negligence for which the reporting person could incur civil liability;

- the reporting person is also not liable for the acquisition of or access to information that is reported or disclosed unless the acquisition or access is in itself punishable.

### 3.2 Report in bad faith



The reporting person who **knowingly** reports **false information** does so **in bad faith** and is not protected. In that case, Van de Velde may impose appropriate disciplinary measures, as provided for in the employee handbook and providing false attestations or documents or making false statements, for example, constitutes urgent cause justifying the immediate dismissal of the employee.

Furthermore, the reporting person can commit the crime of slander or libel for which criminal law sets appropriate sanctions. Victims of such reports or public disclosures in bad faith may also claim compensation.

## Article 4 – What can be reported?

Reporting persons can enjoy protection when reporting the following breaches or a reasonable suspicion of such breaches:

- Any breach of legal, regulatory or directly applicable European provisions (including implementing provisions).
- Breaches that concern the following areas:

<ul style="list-style-type: none"> <li>✓ Consumer protection</li> <li>✓ Public health</li> <li>✓ Transport safety</li> <li>✓ Protection of the environment</li> <li>✓ Product safety and compliance</li> <li>✓ Protection of privacy and personal data and security of networks and information systems</li> <li>✓ Safety of food and feed, animal health and welfare</li> <li>✓ Public procurement</li> </ul>	<ul style="list-style-type: none"> <li>✓ The fight against social fraud </li> <li>✓ Financial services, products and markets, prevention of money laundering and terrorist financing</li> <li>✓ The fight against tax fraud </li> <li>✓ Acts contrary to the financial interests of the Union</li> <li>✓ Breaches relating to the internal market (competition and state aid)</li> <li>✓ Radiation protection and nuclear safety</li> </ul>
--	---

Breaches that concern the following areas cannot be reported:

<ul style="list-style-type: none"> <li>✗ National security (except in the event of a breach of the rules for public defence and security procurements)</li> <li>✗ Classified information</li> </ul>	<ul style="list-style-type: none"> <li>✗ Information protected by legal and medical professional privilege</li> <li>✗ Information protected by the secrecy of judicial deliberations</li> </ul>
---	---

These matters may be reported while they are occurring, after they have occurred or if they will occur in the future.

It is requested that the reporting person **always** reports this type of breach (or suspicion of such breaches). Breaches (or suspicion of such breaches) relating to members of the Board of Directors, members of the Management Team or other managers must be reported.

What about information that is a trade secret of Van de Velde? A reporting person can report such information insofar as the conditions of the Belgian Whistleblowing law are fulfilled.

**Article 5 – Who can report a breach?**

Everyone who has received information **in a work-related context** about a breach at Van de Velde can report a breach.

The reporting procedure is not open only to people who currently work for Van de Velde, but also to former employees and all persons who come into contact with Van de Velde in the course of their duties.

The following persons may make use of this reporting procedure:

Employees (including civil servants)	Self-employed people	Employers
Former employees	Shareholders	Persons that are members of an administrative, managerial or supervisory body
Contractors, subcontractors and suppliers (and their staff)	(Paid and unpaid) interns	Applicants
Job students	Volunteers	

If a breach is reported in the area of financial services, products and markets, and in the area of prevention of money laundering and terrorist financing, the reporting person can also enjoy protection if this information was acquired **outside a work-related context**.

**Article 6 – Protective measures**

**6.1. Ban on retaliation**

Van de Velde undertakes a **complete ban** on any form of retaliation against the reporting person or any other person involved in the matter. As well as the taking of actual retaliation, threats and attempts to take retaliation are prohibited. Among other things, this means dismissal, bullying and detrimental treatment. For a full list of banned forms of retaliation see **Annex 1** to this Whistleblowing Policy.

**6.2. Support measures**



- The Federal Institute for Human Rights (FIRM/IFDH) is the **central point of information** in Belgium regarding the protection of reporting persons. FIRM/IFDH’s remit is to implement support measures and supervise the application of support measures. Furthermore, FIRM/IFDH’s members will notify the public prosecutor in the event of a crime.

These support measures comprise: provision of full impartial information and advice, technical advice, legal aid, technical, psychological, media-related and social support and financial assistance (as part of legal proceedings).



The relevant competent authorities listed in **Annex 2** can be contacted for support measures relating to the entities in the Netherlands, Denmark, Finland, Germany and Spain.

### 6.3. Protective measures against retaliation



If a person protected by this policy becomes a victim of or is threatened with retaliation, that person can file a motivated complaint in Belgium with the **federal ombudsman** ([www.federaalombudsman.be](http://www.federaalombudsman.be)). The federal ombudsman will launch an **extrajudicial protection procedure** and verify the existence of a reasonable suspicion of retaliation. Van de Velde will in that case have to prove that there is no question of retaliation.

Persons who report breaches **do not incur liability** for the report if there were reasonable grounds to believe that the information had to be reported to disclose the breach.

A person who enjoys protection under this legislation against whom retaliation is taken has a right to **compensation**.

- If the victim of the retaliation is an employee, this compensation is in an amount equivalent to between 18 and 26 weeks' pay.
- If the victim is not an employee, the amount will be calculated on the basis of the actual damage suffered, which the victim will have to prove. If a person has reported a breach in the area of financial services, products and markets or in the area of money laundering and terrorist financing, the victim may opt for a fixed amount equal to 6 months' gross pay (including all perks) or an amount equal to the actual damage suffered, which the victim will have to prove.

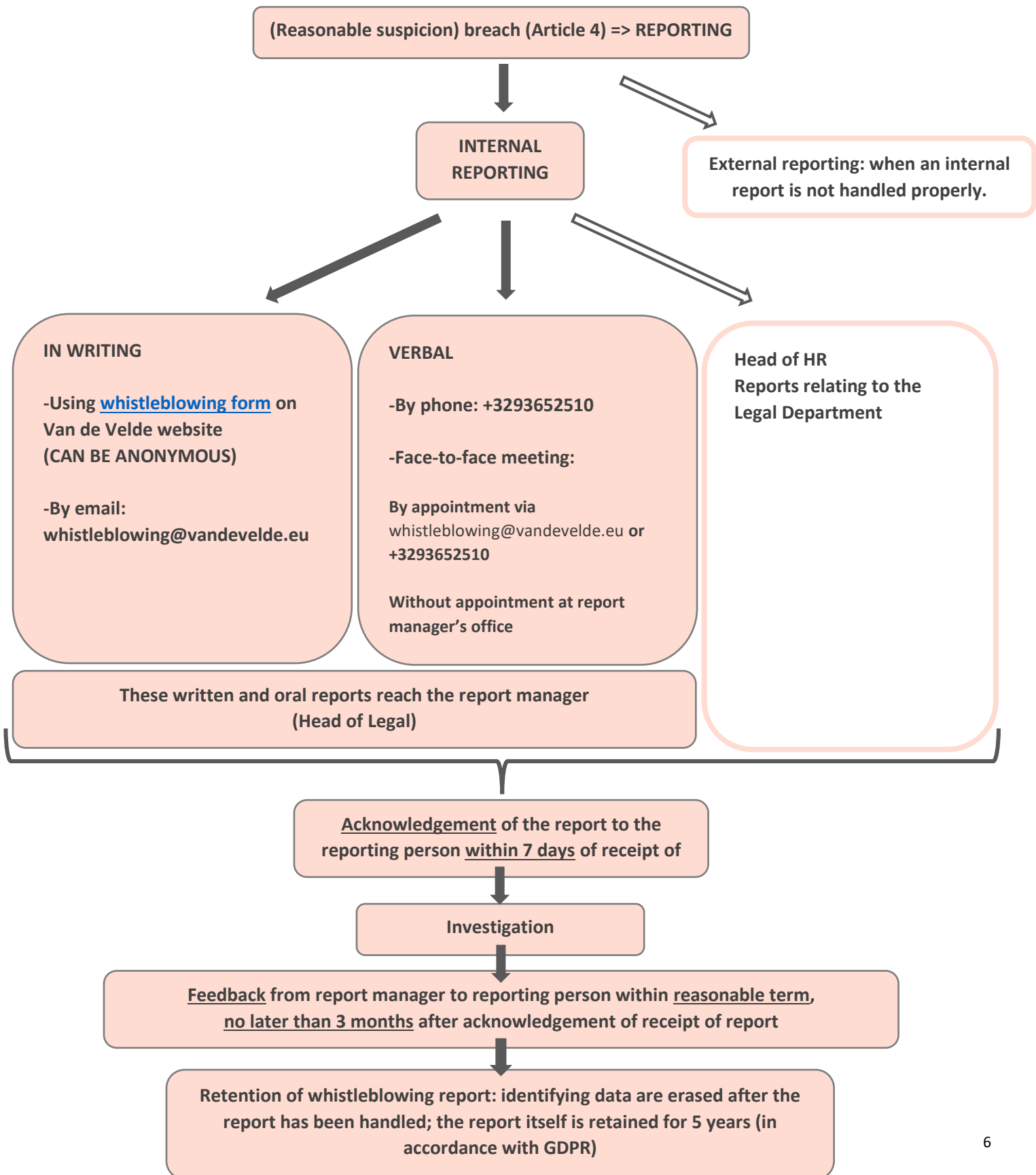
If a person is dismissed or working conditions are unilaterally changed as a consequence of reporting a breach, the employee (or the trade union) can ask to be **re-employed under the same conditions**. This request must be sent by registered mail and received within 30 days of the date of notification of the dismissal/change. The employer must respond to this within 30 days. If the response is negative, the employee retains the right to claim compensation.

The victim of retaliation can also file an **appeal with the employment tribunal**. The president of the employment tribunal can impose redress measures against the retaliation in preliminary proceedings, such as provisional measures in anticipation of the settlement of the legal proceedings.



The relevant competent authorities listed in **Annex 2** can be contacted for protective measures relating to the entities in the Netherlands, Denmark, Finland, Germany and Spain.

Article 7 - Internal reporting



The above flowchart shows the internal procedure at Van de Velde.

- Van de Velde provides four ways for a person to file a (written/verbal) report. The reporting person may do so anonymously.
- The report is received and managed by the report manager. This is the head of the Legal Department. After receiving the report, the report manager is responsible for responding to the report with due care and conducting an investigation.
- The report manager has sole access to the **identity of the reporting person** and will keep this **secret**. The report manager can share confidential information (not including the reporting person's personal data) to safeguard feedback.

We do not ask for proof when a breach is reported, but we do need the claim to be backed up, so the procedure can advance more quickly.

After the report manager has received the report, the report is included in a report register. If the reporting person has reported a breach verbally by phone or in a face-to-face meeting, an accurate written account of the verbal report will be drawn up. This account will be made available to the reporting person to allow the reporting person to check it, make any corrections and sign it before it is included in the report register.

This report procedure does not affect any other report procedures that are provided for under specific legislation.

Custodial sentences, criminal penalties and/or administrative fines can be imposed on Van de Velde NV, its employees or agents, if Van de Velde fails to fulfil its obligations regarding internal reporting under the Belgian Whistleblowing Law.



As stated in Article 1, Van de Velde opens its internal report procedure to all Van de Velde entities in the EU (Belgium, the Netherlands, Denmark, Finland, Germany and Spain).


### Article 8 - External reporting

We ask you to always submit reports internally. We ask you to only report the matter externally if the internal report is not dealt with properly. This reporting procedure does not impose any ban on reporting a situation under this policy externally.



- The authorities competent to receive and handle an external report for Belgium are listed in **Annex 2**. Furthermore, as coordinator the **federal ombudsman** will be responsible for referring an external report to the competent authority ([www.federaalombudsman.be](http://www.federaalombudsman.be)). Independent and autonomous reporting channels are set up to receive and handle verbal and written reports of breaches. The competent authority/federal ombudsman must send an acknowledgement of receipt to the reporting person within 7 days, unless the reporting person requests otherwise. The competent authority/federal ombudsman provides feedback about the report within a reasonable term of no more than 3 months (in justifiable cases this can be 6 months). The competent authority/federal ombudsman will include the procedural rules for receiving and handling external reports in a

regulation or circulaire. These are binding and will be published on the website of the competent authority/federal ombudsman.

-  ▪ The relevant competent authorities listed in **Annex 2** can be contacted for external reports relating to the entities in the Netherlands, Denmark, Finland, Germany and Spain.
- If a person reports a breach to the competent institutions, bodies or agencies of the **European Union**, the reporting person can enjoy protection in the same way as a person who reports a breach externally. This also applies to a reporting person who reports a breach to a **judicial authority** insofar as these protective measures are more favourable for the reporting person.

### Article 9 - Public disclosure

A reporting person can opt to disclose information about a (suspected) breach by sharing it with the press, by putting it on social media and so on. A reporting person who makes use of this public disclosure option enjoys protection only if **one of the following conditions** is fulfilled:

1. The reporting person has already reported the breach internally and externally or immediately reported it externally, but no appropriate measures were implemented in response to this report within the term set. This is not the case if the competent authority does not respond in order to fulfil its confidentiality obligations.
2. There are reasonable grounds for the reporting person to believe that:
  - a. the breach may constitute an imminent or manifest danger to the public interest; or
  - b. in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

### Article 10 – Confidentiality

The identity of the reporting person will be handled confidentially by the report manager. This is not shared as part of the investigation of the report.

This confidentiality is also applied to facilitators, third parties who are connected with the reporting person and the legal entities to which the reporting person is linked.

The reporting person can also opt to report **anonymously**, in which case the report manager will not know the identity of the reporting person. Persons wishing to report breaches anonymously can do so by filling out the whistleblowing form on the Van de Velde website. The report will be handled without the reporting person receiving any response, as we must not be able to directly or indirectly infer the identity of the reporting person from any report we receive anonymously.

- ⇒ In that case we suggest that the reporting person creates an email address that gives no clues as to the reporting person's identity in order to receive a response without compromising the reporting person's anonymity.



Confidentiality is mutual, which means it also applies to the reporting person. Van de Velde expects reporting persons to remain silent about their report until they receive a fuller response.

Every effort is made to protect the identity of the persons involved for the duration of the investigation.

#### **Article 11 – Processing of personal data**

As stated above, we include certain data relating to a report in a report register. We take due care with the processing of this data in accordance with the applicable privacy legislation, particularly the General Data Protection Regulation and the Belgian Privacy Law. That means that we do not process personal data that is not relevant. If we do, this is erased immediately.

We keep only the name, position and contact details of the reporting person and any other person to whom the protective and support measures can apply and the persons/entities involved (including a business registration number). These personal data are erased once the report has been handled. The report itself is retained for 5 years in anonymous form.

#### **Article 12 – Advisor**

Potential reporting persons who are unsure whether the reporting procedure should be applied or have any other questions regarding this procedure can present any questions to the report manager by email at [whistleblowing@vandavelde.eu](mailto:whistleblowing@vandavelde.eu) or by phone on +3293652510.




The report manager at Van de Velde is the head of the Legal Department.




**Annex 1 – Selected banned forms of retaliation**

**Banned forms of retaliation**

- Suspension, temporary standing down, dismissal or similar measures;
- Demotion or denial of promotion;
- Transfer of duties, changing of location of workplace, reduction of pay, changing of working hours;
- Withholding of training;
- Negative performance review or job reference;
- Imposition or application of a disciplinary measure, reprimand or other sanction, such as a financial sanction;
- Coercion, intimidation, bullying or exclusion;
- Discrimination, detrimental or unequal treatment;
- Failure to convert a temporary contract of employment into a permanent open-ended contract of employment, if the employee had the justifiable expectation of being offered open-ended employment;
- Failure to renew or early termination of a temporary contract of employment;
- Damage, including reputational damage, including on social media, or financial disadvantage, including loss of turnover and loss of income;
- Inclusion on a blacklist based on an informal or formal agreement for a whole industry or branch, as a consequence of which the person is unable to find another job in that industry or branch;
- Early termination or notice of termination of a contract for the supply of goods or the provision of services;
- Withdrawal of a licence or permit;
- Psychiatric or medical referral.

Annex 2 – Competent authorities for the external reporting procedure

Country	Competent authorities
<p><b>Belgium</b> </p>	<ul style="list-style-type: none"> <li>➤ The Federal Ombudsman</li> <li>➤ FPS Economy, SMEs, Middle Classes, and Energy</li> <li>➤ FPS Finance</li> <li>➤ FPS Public Health, Food Chain Safety and Environment</li> <li>➤ FPS Mobility and Transport</li> <li>➤ FPS Employment, Labour and Social Dialogue</li> <li>➤ Programmatie Overheidsdienst Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid (Federal Public Planning Service for Social Integration, Poverty Control, Social Economy and Large City Policy)</li> <li>➤ Federaal Agentschap voor Nucleaire controle (Federal Agency for Nuclear Control)</li> <li>➤ Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (Federal Agency for Medicines and Health Products)</li> <li>➤ Federaal Agentschap voor de veiligheid van de voedselketen (Federal Agency for the Safety of the Food Chain)</li> <li>➤ Belgische Mededingingsautoriteit (Belgian Competition Authority)</li> <li>➤ Gegevensbeschermingsautoriteit (Data Protection Authority)</li> <li>➤ Autoriteit voor Financiële diensten en Markten (Financial Services and Markets Authority)</li> <li>➤ Nationale Bank van België (National Bank of Belgium)</li> <li>➤ College van toezicht op de bedrijfsrevisoren (Belgian Audit Oversight Board)</li> <li>➤ The authorities stated in article 85 of the law of 18 September 2017 to prevent money laundering and terrorist financing and limiting the use of cash</li> <li>➤ Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater (National Committee for the security of the supply and distribution of drinking water)</li> <li>➤ Belgisch Instituut voor postdiensten en telecommunicatie (Belgian Institute for Postal Services and Telecommunications)</li> <li>➤ Rijksinstituut voor ziekte- en invaliditeitsverzekering (National Institute for Health and Disability Insurance)</li> <li>➤ Rijksinstituut voor de Sociale Verzekeringen der Zelfstandigen (National Institute for Social Security Insurance for the Self-employed)</li> <li>➤ Rijksdienst voor Arbeidsvoorziening (National Employment Office)</li> <li>➤ Rijksdienst voor Sociale Zekerheid (National Social Security Office)</li> <li>➤ Sociale Inlichtingen en Opsporingsdienst (Social Information and Investigation Service)</li> <li>➤ Autonome dienst Coördinatie Anti-Fraude (CAF) (Autonomous Anti-Fraud Coordination Service)</li> <li>➤ Scheepvaartcontrole (Shipping Inspectorate)</li> </ul>
<p><b>Netherlands</b> </p>	<ul style="list-style-type: none"> <li>➤ Autoriteit Consument en Markt (Netherlands Authority for Consumers and Markets)</li> <li>➤ Autoriteit Financiële Markten (Netherlands Authority for the Financial Markets)</li> <li>➤ Autoriteit persoonsgegevens (Dutch Data Protection Authority)</li> <li>➤ Nederlandse Bank N.V.</li> <li>➤ Huis (House)</li> <li>➤ Inspectie gezondheidszorg en jeugd (Health and Youth Care Inspectorate)</li> <li>➤ Nederlandse Zorgautoriteit (Dutch Healthcare Authority)</li> <li>➤ Autoriteit Nucleaire Veiligheid en Stralingsbescherming (Authority for Nuclear Safety and Radiation Protection)</li> <li>➤ appropriate organisations and management bodies that have responsibilities or powers in one of the areas stated in article 2, first paragraph of the Directive</li> </ul>
<p><b>Denmark</b> </p>	<ul style="list-style-type: none"> <li>➤ Datatilsynet (Danish Data Protection Agency)</li> <li>➤ Justitsministeriet (Ministry of Justice)</li> <li>➤ Forsvarsministeriet (Ministry of Defence)</li> </ul>

	<ul style="list-style-type: none"> <li>➤ External whistleblowing arrangements established in accordance with industry-specific EU legislation, see §2, are maintained.</li> </ul>
<b>Finland</b> 	<ul style="list-style-type: none"> <li>➤ Oikeuskanslerinviraston (Chancellor of Justice)</li> <li>➤ Finnish Financial Supervisory Authority (FIN-FSA)</li> <li>➤ Tax Administration</li> </ul>
<b>Spain</b> 	<ul style="list-style-type: none"> <li>➤ la Autoridad Independiente de Protección del Informante, A.A.I.</li> </ul>
<b>Germany</b> 	Not yet known