Newsletter:
Whistleblowers

DECEMBER 2022

Dear reader,

On 25 October, a bill was passed in the House of Representatives to transpose Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report violations of Union law.

The purpose of the Directive is to set minimum standards for better protection of persons who report violations of EU law ("whistleblowers").

The Belgian law, published yesterday in the Belgian State Gazette, transposes the obligations imposed by the Directive on private sector enterprises into Belgian law.

In this Newsletter, we set out the new obligations imposed on enterprises on this basis.

We hope you enjoy the read!

CONTENTS TABLE

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

1 What can an alert be issued about?

1.1 Substantive scope

The law is **applicable** in those areas:

1) violations that concern the following areas: (a) public procurement; (b) financial services, products and markets and the prevention of money laundering and terrorist financing; (c) product safety and conformity; (d) transport safety; (e) environmental protection; (f) radiation protection and nuclear safety; (g) food and feed safety, animal health and welfare; (h) public health; (i) consumer protection; (j) protection of privacy and personal data, and the security of networks and information systems; (k) the fight against tax fraud; and (l) the fight against social fraud;

2) breaches affecting the **financial interests of the Union**;

3) breaches relating to the **internal market**, in particular breaches of the rules on competition and State aid.

1.2 Exceptions

The law is **not applicable** to:

1) **national security** area;

2) **classified information**;

3) information covered by **medical confidentiality** and the **professional confidentiality of attorneys**;

4) information covered by the **confidentiality of judicial deliberations**.

2 Who falls within the scope of the law?

2.1 Personal scope

The law applies to:

- To whistleblowers working in the **private sector** who have obtained information about violations in a professional context, including at least:
    - Persons with **employee** status, including **civil servants**. Workers as well as employees, workers on fixed-term or indefinite contracts, etc. are covered;
    - Persons with the status of **self-employed**;
    - **Shareholders** and **members** of the administrative, management or supervisory body of a company, including **non-executive members**.
    - **Volunteers** and paid or unpaid **trainees**;

  - Any person working under the supervision and direction of contractors, subcontractors, and suppliers.

- To whistleblowers whose **employment relationship has ended** since disclosure;
- To whistleblowers whose **employment relationship has not yet started** (in case information on violations was obtained during the recruitment process or pre-contractual negotiations);
- To:
  - **Facilitators**
  - **Third parties** who are **connected** to the whistleblowers and who are at risk of retaliation in a professional context (i.e., colleagues or relatives);
  - **Legal entities owned by** or **connected** to the whistleblowers in a **professional context**;
- To whistleblowers who pass on information **obtained outside a professional context**, when reporting a violation in the field of **financial services, products and markets** and violations in the field of prevention of **money laundering** and **terrorist financing;**
- Any organisation, whether or not it has legal personality, which comes under the jurisdiction of the Federated Entities insofar as a matter is not regulated by the legislation of the regions and communities and comes under the jurisdiction of the Federal State, subject to the application of more favourable protection measures for the whistleblower.

2.2 Exceptions

There are two categories of persons who fall outside the scope of the Directive:

- Persons who report violations to law enforcement authorities **in return for a reward or compensation** if they have been **listed**, based on their informed consent, as **informants** or registered as such in databases managed by the authorities at national level. However, they can be covered by the protection provisions to the extent that they are more favourable.
- Persons who report or make a public disclosure **based on an obligation under one of the sectoral acts of the Union** listed in Part II of the Annex to the Directive.

2.3 Lexicon

*What is a **violation**?* A violation is an act or omission that: a) is **unlawful** and relates to the areas of substantive application of the law; b) is **contrary to the object or purpose of the rules** in the areas of substantive application of the law.

*What is a **whistleblower**?* A whistleblower is someone who **reports or publicly discloses** information about violations.

*What does **reporting** mean?* The oral or written communication of information about violations.

*What is **public disclosure**?* Making information about violations available in the **public sphere** (e.g., in the press).

*What is a **professional context**?* Past or present professional activities in the private sector through which, regardless of the nature of those activities, individuals obtain information about violations and in which those individuals could be subject to reprisals if they report such information.

*What is a **facilitator**?* A natural person who assists a whistleblower in the reporting process and whose assistance should be confidential.

*What is a **private sector legal entity**?* It is any organisation with or without legal personality which carries out one or more specific activities, except for organisations or activities which are covered by other specific laws relating to the protection of whistleblowers.

3 What protection is provided?

3.1 Prohibition of retaliation

Reporters are protected from sanctions or action as a result of a report (so-called reprisals). The law provides an illustrative list of types of retaliation that are prohibited, including:

(1) suspension, layoff, termination or equivalent action; (2) demotion or denial of promotion; (3) transfer of duties, change of work location, reduction in pay, change in work schedule; (4) suspension of training; (5) negative performance evaluation or certification; (6) discipline imposed or administered, reprimand or other penalty, including financial penalty; (7) coercion, intimidation, harassment or exclusion; (8) discrimination, disadvantageous or unfair treatment; (9) failure to convert a temporary employment contract into a permanent contract, where the employee had a legitimate expectation of being offered permanent employment; (10) non-renewal or early termination of a temporary employment contract; (11) damage, including damage to the person's reputation, in particular on social media, or financial loss, including loss of business and loss of income [...]

3.2 Measures to protect against retaliation

To prevent retaliation from occurring, various protective measures are provided:

- It is possible for the employee to make a reasoned complaint to the Federal Coordinator, who will then initiate an extrajudicial protection procedure;
- The whistleblower is immune from liability for reporting or publicly disclosing information that he or she has obtained or had access to, whether lawful or not, if he or she had reasonable grounds to believe that the reporting or disclosure was necessary to reveal the violation;
- The employee can appeal to the Labour Court if he or she is subject to retaliation, if necessary, as a summary procedure. If the employee claims to have suffered harm, then it is presumed that this harm arises from the retaliation;
- The employee's disclosure of trade secrets will not be considered unlawful if the reporting or public disclosure falls within the scope of the law;
- The identity of the employee who is being challenged is protected during the investigation. The rules protecting the identity of the whistleblower (see below) also apply to him/her.

In the case of retaliation, if the victim is an employee, the law provides for the granting of a **lump-sum compensation**, the **amount of which will vary from 18 to 26 weeks' remuneration** (this compensation cannot be cumulated with compensation for manifestly unreasonable dismissal granted

on the basis of CLA No. 109). If the victim is another person, the compensation corresponds to the prejudice actually suffered, the victim having to provide proof of its extent.

A whistleblower who reports a violation in **financial services, products and markets** and suffers retaliation may request compensation, either a lump sum of **6 months' gross salary**, or the actual damage suffered. In these sectors, the whistleblower may also request reinstatement or the respect of his/her working conditions if he/she is an employee who has been dismissed or whose working conditions have been changed by the employer.

4 What are the conditions for protection?

To benefit from the protection mechanism established by the law, the whistleblower must:

1. have had reasonable grounds to believe that the reported **information** on violations was **true** at the time of reporting and that the information fell within the **scope of the law** (by comparison with a person in a similar situation with comparable knowledge); and

2. have made an **internal** or **external whistleblowing** or **public disclosure** in accordance with the law.

The first criterion is assessed in relation to a person in a similar situation with comparable knowledge.

The author of the alert does not lose the benefit of protection simply because the alert made in good faith has proved to be inaccurate or unfounded.

If the protection is enjoyed by a facilitator, third party or legal entity (see point 2.1 above), they must have had reasonable grounds to believe that the whistleblower fell within the scope of protection of the law.

5 Internal reporting channels

5.1 Obligation to establish internal reporting channels

Which companies must set up internal channels?

Private sector legal entities must establish channels and procedures for internal reporting and for the follow up of reports. This obligation does not apply to legal entities which employ fewer than 50 employees (unless a Royal Decree provides otherwise); this threshold is calculated in relation to the average number of employees in the legal entity.

Legal entities that offer financial products or services and/or are subject to terrorist financing and money laundering legislation must provide internal reporting channels regardless of the number of employees.

Under what terms?

These channels and procedures should be set up **after consultation with the social partners**, i.e., the works council, or failing that, the trade union delegation, or in their absence, the Committee for prevention and protection at work, or in the absence of all of these, the employees directly.

Who should be able to use the internal channels?

The internal reporting channels and procedures in place in companies should **at least be accessible to employees of the entity**. However, companies may choose to open these channels to others (such as freelancers, employees of co-contractors, etc.).

5.2 Whistleblowing officer

Internal reporting channels may be managed internally by a whistleblowing officer or outsourced to a third party, who must offer sufficient guarantees.

In both cases, the private sector legal entity is considered responsible for the processing of personal data.

The choice of the most appropriate persons or departments to designate as competent for receiving and monitoring reports depends on the entity's structure.

The reporting manager will be responsible for receiving reports and for following up on the reports. He/she is the point of contact for the whistleblower and should keep him/her informed of the progress of the procedure.

The reporting manager must be independent and must not have any conflicts of interest. He/she should not receive instructions from the management of a specific case and should be able to report directly to the highest level of management on risks or (potential) obstacles to the performance of his/her duties.

Private sector legal entities with fewer than 250 employees may share resources in relation to the receipt of reports and possible investigations.

5.3 Internal reporting procedures and follow-up

The internal reporting and monitoring procedures include the following elements:

1° A channel/channels for receiving reports. Through the internal reporting channel, it should be possible to report breaches in writing or orally (e.g. by phone or voice message). At the request of the reporter, it should also be possible to report a breach through a physical meeting, which should take place within a reasonable time.

In legal entities with 250 or more employees, reports should also be able to be made **anonymously**.

2° an **acknowledgment of receipt** of the report must be sent to the reporting person within seven days following the receipt of the report;

3° the appointment of a reporting manager (see below, point 5.2);

4° a **diligent follow-up** by the reporting manager, including for anonymous reports;

5° a reasonable period of time to **provide feedback** (on the measures considered or taken as a follow-up and on the reasons for such follow-up), not exceeding three months from the acknowledgment of receipt of the report (or, in the absence of an acknowledgment of receipt sent to the author of the report, three months from the expiry of the seven-day period following the report);

6° the provision of clear and easily accessible information on external reporting procedures (see below, point 6).

The law does not provide according to which form these rules should be implemented. It can therefore be done, at the choice of the legal entity, through labour regulations, a collective labour agreement or a policy of the legal entity. The latter form offers the most flexibility.

5.4 Duty of confidentiality et security measures

Companies should set up measures to secure internal channels (both in their design, implementation and management) to ensure the confidentiality of the identity of the reporting person and any third party mentioned in the report, and to prevent access by unauthorised staff members.

The identity of the reporting person may under no circumstances be disclosed without the express and free consent of the reporting person, to any person other than authorised staff members competent to receive or follow up on reports. This also applies to any other information from which the identity of the reporting person may be directly or indirectly deduced.

5.5 Processing of personal data

Any processing of personal data must be carried out in accordance with Regulation (EU) 2016/679 ("GDPR"), as well as the legal provisions relating to the protection of individuals with regard to the processing of their personal data.

Personal data which are clearly not relevant for the processing of a specific report shall not be collected (in accordance with the data minimisation principle) or, if collected accidentally, shall be deleted without undue delay.

The name, function and contact details of the reporting person and of any person to whom the protection and support measures apply, as well as of the person implicated, shall be safeguarded until such time as the reported violation is prescribed.

5.6 Archiving of reports

All received reports should be recorded, respecting confidentiality requirements.

To this end, companies must keep a **specific register**, containing all received reports.

Reports must be kept for the duration of the reporting person's employment relationship.

The way in which the report is kept depends on the channel set up/used:

- Where a **recorded telephone line** (or other recorded voice-mail system) is used for reporting, the company may, with the consent of the reporting person, record the oral report in one of the following forms:

  1° by making a recording of the conversation in a durable and retrievable form; or

  2° by a full and accurate transcript of the conversation made by the member of staff dealing with the report. The reporting person shall always have the opportunity to check, rectify and approve the transcript of the call by signing it.

- Where an **unrecorded telephone line** (or other unrecorded voicemail system) is used for reporting, private sector legal entities may record the oral report in the form of an accurate record of the conversation made by the member of staff handling the report. The company

should then give the reporting person the opportunity to check, rectify and approve the transcript of the conversation by signing it.

- If the report is made **during a face-to-face meeting**, the company shall ensure, with the consent of the reporting person, that a full and accurate report of the meeting is kept in a durable and retrievable form through a recording of the conversation or through a report of the meeting made by the authorised staff member. Here again, the reporting person should always have the opportunity to check, correct and sign the report of the meeting for approval.

6 External reporting channels

The law also establishes **external reporting channels**.

Whistleblowers can use an external reporting channel either after having made a report through the internal channels, or by directly using an external reporting channel if they consider it more appropriate.

The **Federal Ombudsman** has been designated by the Belgian legislator as the person responsible for coordinating alerts submitted through external channels.

The competent authorities designated by the legislator or, failing that, the Federal Ombudsman, are responsible for receiving external alerts.

This could be, for example, the Public Procurement Service of the FPS Chancellery (in the area of public procurement); the Financial Services and Markets Authority (FSMA), the National Belgian Bank (NBB) or the Supervisory College of Company Auditors (in the area of financial services, products and markets and the prevention of money laundering and the financing of terrorism), the FPS Economy (in the area of consumer protection), the Data Protection Authority (in the area of protection of privacy and personal data), etc.

7 Public disclosure

Public disclosure is the **making available in the public sphere of information about violations**.

Reporting violations through a disclosure will only lead to the protection of the reporter in specific circumstances.

It can be used by any author of an alert who has first issued an internal and external alert, or directly an external alert, if no appropriate action has been taken in response to the alert within the prescribed time limit (three months in the case of an internal alert – see point 5.3 above).

A person may resort directly to public disclosure as defined above where he or she has reasonable grounds to believe that:

- the breach may pose an imminent or obvious danger to the public interest; or

- in the event of external reporting, there is a risk of reprisals or there is little chance that the situation will be remedied because of the circumstances of the facts reported (risk of concealment or destruction of evidence, risk of collusion with the perpetrator of the violation or involved in the violation, etc.).

8 What are the penalties?

In addition to the lump-sum compensation (or compensation for actual damage) referred to in point 3.2 above, the law provides for several sanctions:

8.1 Social penal code

Violations of the provisions of the law relating to internal alerts and their follow-up will be punishable by a level 4 sanction on the basis of the new Article 133/1 of the Social Penal Code, i.e., a prison sentence ranging from 6 months to 3 years and/or a fine ranging from EUR 4,800 to EUR 48,000, or an administrative fine ranging from EUR 2,400 to EUR 24,000 (per employee).

These penalties apply to employers, their employees or agents who have committed an offence concerning internal alerts or the registration of alerts.

In addition, legal entities in the private sector, their staff members and any natural or legal person who commit the following offences are liable to a prison sentence ranging from 6 months and 3 years and/or a fine ranging from EUR 4,800 to EUR 48,000:

- Obstructing or attempting to obstruct reporting;
- Taking reprisals against the persons referred to in point 2.1 above;
- Taking abusive proceedings against the persons referred to in point 2.1 above;
- Breaching the obligation to keep the identity of the authors of the alert confidential.

8.2 Penal Code

Articles 443 to 450 of the Penal Code punish the author of an alert when it is established that he or she has knowingly reported or publicly disclosed false information.

8.3 (Extra-)contractual liability

If a person suffers damage because of a report or public disclosure knowingly made on the basis of false information (see point 8.2 above), he or she will be entitled to compensation in accordance with contractual or extra-contractual liability.

9 Coming into force

By 15 February 2023 at the latest

Implementation of the new legal provisions in enterprises with more than 250 employees and in financial sector companies falling within the scope of the provisions on financial services, products and markets and/or money laundering and terrorist financing.

By 17 December 2023 at the latest

Establishment of internal reporting channels for private sector enterprises with between 50 and 249 employees.

The law will come into force two months after the day of its publication in the Belgian State Gazette, i.e. on 15 February 2023

However, it is expected that **private sector enterprises with between 50 and 249 employees** will have **until 17 December 2023** to set up internal reporting channels.

Companies with more than 250 employees should be well **prepared by 15 February 2023** to comply with the new legal provisions.

For **financial sector companies** falling within the scope of the provisions on financial services, products and markets and/or money laundering and terrorist financing, the law will come into force on **15 February 2023**, regardless of the number of employees.

.

Brussels
Boulevard du Souverain 280
1160 Brussels
T 02 761 46 00

Liège
Parc d'affaires Zénobe Gramme
Square des Conduites d'Eau 7
Bat. H - 2nd floor
4020 Liège
T 04 229 80 11

Antwerp
City Link
Posthofbrug 12
2600 Antwerp
T 03 285 97 80

Ghent
Ferdinand Lousbergkaai 103
box 4-5
9000 Gent
T 09 261 50 00

Kortrijk
Ring Bedrijvenpark
Brugsesteenweg 255
8500 Kortrijk
T 056 26 08 60

Hasselt
Kuringersteenweg 172
3500 Hasselt
T 011 24 79 10

Partners with you.