WHITE PAPER

New rules on whistleblowers and breach notifications

Peter Craddock
Head of Data, Cybersecurity & IT Law,
NautaDutilh

INTERSENTIA

GoComply
Whistleblowing

Table of contents

The European "Whistleblower Directive" of 23 October 2019 (EU Directive 2019/1937) contains rules for the protection of persons who report breaches of EU law. This directive must be implemented in each EU Member State by 17 December 2021.

Compliance with these rules will be crucial for organisations, to ensure good practice and avoid the risk of fines for non-compliance.

We examine below the most important questions regarding these new rules. Belgian legislation will be integrated into this guide as soon as it becomes available.

1. "Whistleblowers" and "reports of breaches": what does it cover?

Persons working for an organisation or who are in (close) professional contact with it are often the first to be aware of existing or imminent breaches of legal obligations by the organisation itself or by (one of) its personnel. Because of the fear of retaliation, however, reporting such breaches is not always the obvious way forward.

This Whistleblower Directive aims to provide a framework to lower the threshold for making such reports, by offering the reporting person (often called a "whistleblower" in practice) the necessary protection.

However, this Directive is limited to reports of breaches of EU law, i.e. acts or omissions that are unlawful or defeat the object or the purpose of the relevant EU rules. For instance, infringements of EU competition law or laws regarding product safety, consumer protection or data protection fall within the scope of the Directive; this will not be the case for infringements of national legislation in matters that do not fall within the EU's competence (e.g. many rules of labour law, such as the special regime in Belgium on the prevention of psychosocial stress at work, which notably covers sexual harassment). (Art. 2 Directive)

In other words, the Directive is there to allow people to report many (but not *all*) kinds of breaches without fear of retaliation. With other kinds of breaches, there may already be a mechanism for reporting improper acts or unlawful behaviour. Communicate clearly regarding which system is relevant for which breaches.

2. Reporting without fear: what protection should your organisation offer to reporting persons?

A reporting person will enjoy protection against retaliation if two conditions are met: (Art. 6 Directive)

1. The reporting person had reasonable grounds to believe that the information on breaches reported (the allegations) was true at the time of reporting and that such information fell within the scope of the Directive (see question 1); and
2. The reporting person transmitted the information through one of the channels provided for in the Directive (see question 3).

Besides (and in addition to) a confidentiality obligation for the persons handling the report, the reporting person benefits from two kinds of protection, even after the reporting procedure has ended:

1. There is a **prohibition of retaliation** against the reporting person. More specifically, this means that there must be no negative consequences for the reporting person for making a report which, in the opinion of the reporting person, was true and lawful at the time. The Directive mentions several examples: suspension, dismissal, a negative performance assessment, unfair treatment, a financial penalty, harm to reputation, etc. (Art. 9 Directive)
2. The reporting person has the right to access **support measures** "as appropriate". These measures include "comprehensive and independent information and advice" regarding these protections and procedures as well as (if provided by the Belgian legislator) financial assistance in the framework of legal proceedings. In principle, this assistance is covered by the Member State (e.g. through an information centre) and not by the organisation itself. (Art. 20 Directive)

This protection **also applies to third persons** (natural persons but also legal entities) **connected with the reporting persons** and who could suffer retaliation in a work-related context (e.g. colleagues or relatives of the reporting persons, management companies of the reporting persons, employer of the reporting person in case of an external organisation, etc.). (Art. 4(4) Directive)

In other words: ensure that reporting persons are protected, and that potential reporting persons know that they are free to report – as long as the information is correct.

Note: The person making the report will only exceptionally be able to benefit from this protection if the report is not made through the intended channels (e.g. publication online and not through the internal reporting channel). Therefore, it is better to encourage individuals to use only the official internal or external reporting channels.

3. Does your organisation have to establish a procedure for internal reporting of such breaches, and which channels can be used to do so?

All legal entities in the private sector with 50 or more workers are required to establish internal reporting channels (often called "whistleblowing hotlines"). Similar rules exist in principle for legal entities in the public sector, but Member States such as Belgium may provide for certain exceptions. (Art. 8 Directive)

Such internal reporting channels must allow the report to be made in writing (e.g. online, by post) or orally (e.g. by telephone or voice message systems, or through a physical meeting). (Art. 9.2 Directive)

> **TIP: How to build and provide an online internal reporting channel?** The Directive does not mention the actual operation, but often a **specific link** on the organisation's website will be used (external website *and* intranet, to allow employees and third parties to use it). It is important to make this **accessible** and **visible** enough. Hiding this link in general terms and conditions will probably not be accepted.

Besides such internal reporting channels, it is also possible for reporting persons to follow other procedures (e.g. via an external authority or through public disclosures). However, the European legislator prefers the use of internal reporting channels. (Art. 7 Directive)

In other words: try to make internal reporting channels the standard procedure, but still allow other channels as an alternative and adequately inform your employees and external parties about both channels.

4. Within what timeframe does an internal report have to be handled?

Upon receipt of a report (e.g. via an online tool or via other channels such as by phone), the organisation must acknowledge receipt **within 7 days**.

Afterwards, an "impartial person or department" must follow up on the report and provide feedback **within 3 months** of the acknowledgement of receipt.

Failure to meet these deadlines gives the reporting person the possibility to benefit from protection as a reporting person (see question 2) even if they make their complaint public. It is therefore important to strictly observe the time limits.

Did you know that... some internal reporting tools make it possible to create reminders, or tasks with a specific due date? This makes it easier to ensure that deadlines are not missed.

5. Who can be appointed as manager of an internal reporting channel?

The aforementioned "impartial person or department" handling the complaint will often be someone with a compliance-related role. However, the company should be mindful of the identity and function(s) of this person, given possible conflicts of interest.

For example, the usual external lawyer or a consultant may not always be the best choice, as reports may involve the instructing officer of the lawyer or consultant. Moreover, this will give the external lawyer access to information that may become important in the context of a future dispute.

6. How should your organisation handle the processing of personal data in the context of a report?

The Directive stresses that any processing of personal data under the Directive, "including the exchange or transmission of personal data by the competent authorities", must be carried out in accordance with the General Data Protection Regulation (GDPR).

Moreover, the Directive contains a specific obligation that seems to be based on the principles of "data minimisation" (Art. 5(1)(c) GDPR) and "storage limitation" (Art. 5(1)(e) GDPR): "Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay". The Directive also contains several references to confidentiality *(see question 7)*, which is in line with the principle of "integrity and confidentiality" (Art. 5(1)(f) GDPR). (Art. 17 Directive)

The recitals of the Directive also contain important considerations regarding compliance with the other obligations under the GDPR. For example, the Directive refers to the fact that the procedures relating to the follow-up of reports "serve an importance objective of general public interest" and to the importance of the principle of data protection by design and by default ("data protection by design and by default"; Art. 25 GDPR).

It is therefore crucial to consider the processing activities related to the handling of reports as separate and new processing activities – and to take the necessary steps to comply with the GDPR in this respect as well.

In addition, your company should take due care in handling e.g. requests for access or deletion originating from persons named or associated with a report ("persons concerned" in the sense of the Directive). In this regard, the Directive states that Member States must "ensure that this Directive is effective, including, where necessary, by restricting, by legislative measures, the exercise of certain data protection rights of persons concerned".

Did you know that... the former Article 29 Working Party (predecessor of the European Data Protection Board, composed of data protection authorities of the different Member States) had published an opinion on reporting systems/whistleblowing systems in 2006 that can still serve as inspiration with regard to compliance with data protection principles?

In Belgium, the former Privacy Commission (predecessor of the Belgian Data Protection Authority) had also published a recommendation on this subject (Dutch / French), and the Belgian Data Protection Authority now also has a webpage on such systems (Dutch / French).

7. Should the identity of the reporting person and the persons concerned remain confidential, and are there any limits to this?

Confidentiality is not only an obligation under the GDPR *(see question 6)* but also a fundamental requirement for a reporting system: without a guarantee of confidentiality, a reporting person will probably not submit a report.

The Directive stresses the importance of protecting the reporting person's identity. For example, **without his or her explicit consent, the reporting person's identity cannot be disclosed** to anyone beyond the (authorised) persons handling the report. This applies not only to the name of the reporting person, but also "to any other information from which the identity of the reporting person may be directly or indirectly deduced". (Art. 16.1 Directive)

There is one exception to this, namely the mandatory disclosure of the reporting person's identity in the context of "investigations by national authorities or judicial proceedings". In such a case, the organisation is required to inform the reporting person thereof, unless doing so would "jeopardise" the investigations or judicial proceedings (e.g. risk of destruction of evidence). (Art. 16.2 and 16.3 Directive)

What about anonymous reports? The Directive provides that Member States have the power to decide whether anonymous reports should be accepted and handled. In the absence of national provisions in this respect, nothing prevents an organisation from accepting anonymous reports, provided there is a proper assessment of the reliability of the report (so as not to affect the rights of defence – *see question 8)*.

The Directive also provides for confidentiality concerning the **identity of the persons concerned**, but to a more limited extent (obligation for authorities and for persons receiving or handling a report through an external reporting channel). In any case, the principle of integrity and confidentiality under the GDPR remains applicable, and this requires organisations to be cautious about revealing the identity of the data subject during an investigation. (Art. 22.2 and 22.3 Directive)

In other words: ensure that confidentiality becomes the norm at every level, and be cautious in internal and external communications regarding an investigation.

8. How are the rights of defence safeguarded and what measures are in place to protect against malicious or dishonest reporting?

The Directive regularly mentions data subjects' rights of defence, because reports can be harmful on their own. Member States must take measures to safeguard these rights –including the presumption of innocence, the right to a fair trial, the right to access the file, the right to be heard and the right to an effective remedy against a decision concerning the person concerned. (Article 22.1 Directive)

The Directive also emphasises that persons concerned should have the right to compensation "where it is established that [the reporting persons] knowingly reported or publicly disclosed false information", but this should again be provided for by Member States. (Art. 23.3 Directive)

In other words: do not forget that persons concerned also enjoy a certain degree of protection by way of the rights of defence.

9. By when should your organisation implement this?

Does your organisation have 250 or more workers, or does it belong to the public sector? Then your organisation must implement all rules **by the end of 2021**.

If your (private sector) organisation has less than 250 workers, you must:

- Make internal reporting channels available by the end of 2023;
- Comply with all other provisions (confidentiality, data protection, possibility to use external reporting channels, etc.) by the end of 2021.

In other words: it is high time to think about how your organisation will deal with such reports.

10. CHECKLIST FOR IMPLEMENTATION OF REPORTING/WHISTLEBLOWING RULES

☐ Choose internal reporting channels

☐ Include a link to the internal reporting channels on the organisation's website(s) and digital environment(s) (public website, intranet, applications etc.)

☐ Provide information on these channels (external versus internal and in areas for which this is relevant) to:

- Employees
- Third parties

☐ Embed data protection safeguards and limit access to personal data

☐ Monitor deadlines

☐ Regularly evaluate (including whether the person handling reports is following up correctly and remains impartial)

The content is updated to 18 February 2021.

INTERSENTIA

GoComply
Whistleblowing