UNALOME LEGAL

NEWSletter

WHISTLEBLOWING SPECIAL SERIES – N°3
Designing an internal whistleblowing scheme

The new law transposing Directive (EU) 2019/1937 on the protection of persons who report breaches of EU law (the "Whistleblower Protection Act") is now in force!

It has a significant impact on Luxembourg companies, even for those which may already have a whistleblowing scheme in place at local or group level.

To assist companies in implementing the Whistleblower Protection Act, we have identified 4 main topics and the necessary practical steps that should be undertaken to ensure compliance. We will present each of these topics through a dedicated newsletter to be published every week.

In this third edition, we will review the minimum legal requirements that internal whistleblowing channels and procedures must comply with and provide a list of key items to be decided upon when designing such whistleblowing scheme.

Minimum requirements for an internal whistleblowing scheme

Setting up internal whistleblowing channels and procedures implies for the company to make available to its employees some tools/means and processes allowing them to report breaches of the law in a confidential and secure manner.

The law leaves a large freedom to companies to design their internal whistleblowing scheme taking into account their size, organisation and governance, but sets key principles that must be complied with:

In a nutshell

- ✓ Security of the channel(s) is key: select reporting tools that guarantee full confidentiality
- ✓ Service in charge: appoint person(s) having relevant skills and time to deal with reports and being impartial, or outsource the process, wholly or partially
- ✓ Scope of the whistleblowing scheme: decide whether to open it to third parties in professional contact with the company
- ✓ Reporting modalities and process: determine whether to accept anonymous reports or not
- ✓ Ensure due compliance with mandatory deadlines through robust case management process

- Fully secure channel(s) which guarantee that the identity of the reporting person and of persons concerned by the report remains confidential and prevent access by non-authorized persons.
- The possibility to report orally and/or in writing, in any of the 3 national languages and/or in any other language accepted by the company.
- An acknowledgement of receipt of the report within 7 days.
- A competent and impartial service or person(s) in charge of receiving reports, ensuring their follow-up, maintaining communication with and giving feedback to the reporting person.
- Follow up measures to assess the reality of the reported facts and remedy the breach (if any).
- Information to the reporting person on the follow-up measures envisaged or taken, within 3 months as of the acknowledgement of receipt
- Clear and accessible information on the use of the internal channels and on the external reporting procedures to the authorities.

Unalome Legal S.à r.l.
119, rue de Reckenthal
L-2410 Strassen

T +352 27 40 52 20
info@unalome-legal.lu
www.unalome-legal.lu

N° RCS : B263140
Capital social : 12.500€
N° TVA : LU33633088

Société d'avocats inscrite
au Barreau de Luxembourg

UNALOME LEGAL

Main points to be decided upon when designing the internal whistleblowing scheme

Scope of the whistleblowing scheme

Personal scope:

As per the Whistleblower Protection Act, the internal whistleblowing channel(s) shall be available to employees of the company. An option is to open the internal channel(s) to third parties who are or have been in professional contact with the company, such as freelance workers, board members, employees of suppliers and contractors, as well as candidates and former employees. The advantage is that third parties could opt for an internal reporting instead of directly filing their report to the competent authorities.

Material scope:

Although the Luxembourg legislator has opted for a very wide scope of application (any illegal act or omission or abusive practices, which goes against the object or purpose of the law), companies may wish to also encourage reporting of breaches of their own ethical standards embedded in a code of conduct or compliance manual (such as rules on gifts and favours, on conflicts of interests, …).

Tools and means for the receipt of reports

As a principle, the company can decide to implement one or several of the following channels:
- In-person meeting
- Dedicated hotline / voice messaging system *
- E-mail box
- Dedicated web platform / software.

The key considerations when selecting the appropriate channel are data security and GDPR compliance (as per the legal requirements stated above). For instance, an e-mail box, even if accessible to limited persons, may have security vulnerabilities, and will never prevent recipient errors, which may have major consequences (penalty for data breach under the GDPR, penalty under the Whistleblower Protection Act for breach of confidentiality, …). In this context, it is recommended to involve the IT department as well as the data protection officer in the selection process.

* Specific legal requirements apply for the recording and conservation of vocal messages and phone conversations. Where oral reporting is offered, it should also offer the possibility for an in-person meeting within a reasonable delay

Person(s) / service in charge of the receipt and follow up of the reports

Following options are available as per the law:

- Internal management: Whistleblowing channels can be managed internally, provided the company has resources (generally within the Legal or Compliance department) having the necessary skills, impartiality… and time to deal with the reports. No specific qualifications are required by the law.

- Outsourcing: The company may decide to outsource the process, either fully or partly (e.g. only the receipt and first assessment of the report), to an external service provider. As a reminder, outsourcing to a group entity is not permitted (see our second edition of this Whistleblowing special series). This option may notably be considered if the company lacks the necessary resources, or deems it more appropriate to ensure neutrality.

- Pooling of resources: this option is only available for companies with less than 250 employees. It consists in the sharing resources for the receipt and follow up of reports. Although the Directive and the Whistleblower Protection Act are not clear on this point, it therefore seems to be an exception to the principle of “one legal entity - one internal channel”.

Reporting modalities and follow up procedure

The Whistleblower Protection Act does not require companies to accept anonymous reports. It is therefore up to each organisation to decide whether reporting persons can remain anonymous (in which case the relevant tools allowing the preservation of anonymity shall be offered, such as specialised platforms).

Companies shall also determine in which language(s) reports can be made. This may depend notably on the language skills of the designated person or service in charge of receiving and following up on reports.

Finally, it is key to put in place a robust case management process. As indicated above, strict deadlines need to be complied with for acknowledging receipt of reports and providing feedback to the reporting person. Furthermore, it is required to follow up on reports towards the reporting person (which may include e.g. the opening of an investigation, a request for further information, the progress of the investigation, etc.). The internal process should therefore be designed in such a manner as to keep track of the milestones of each report.

Combination with grievance / harassment protection scheme ?

Considering the recent entry into force of the law on moral harassment, which notably requires companies to put in place a process for the receipt and management of harassment complaints, one may wonder whether it would be possible, and relevant, to combine the grievance and whistleblowing reporting channels and procedures.

While it may be envisaged to centralise the channels for reporting breaches of the law and individual harassment (or more generally grievance) complaints, with a common tool and the same contact person(s), it is not appropriate in our view to entirely harmonise both processes. An essential difference between both legislation lies in the confidentiality of the reporting person / complainant's identity. Indeed, it is essential in the whistleblowing management process to keep the identity of the reporting person confidential. In a harassment case, while confidentiality must be respected, the person targeted by a complaint must be heard about the reported facts and be able to defend himself/herself, and witnesses may have to be interviewed, which implies disclosing the complainant's identity. Furthermore, temporary measures may have to be taken to protect the alleged victim of harassment, often requiring the involvement of the HR department.

It is therefore recommended to state that whistleblowing procedures do not apply in the case of reports exclusively affecting individual rights of the reporting person.

In our next edition, we will discuss the content of the whistleblowing policy and the formalities for implementing the whistleblowing scheme within the company.

In the meantime, our team is at your disposal for any further information.

Contacts:

Marielle Stévenot
m.stevenot@unalomelegal.lu

Cindy Arces
c.arces@unalome-legal.lu