Whistleblowing Directive Published

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

On 26 November 2019, Directive 2019/1937 "on the protection of persons who report breaches of Union law" was published in the Official Journal (L 305, p. 17). The European Parliament and the Council already agreed on the content of the Directive in April 2019. For the compromise reached on this directive, nicknamed "Whistleblower Directive," see eucrim 1/2019, p. 27 (with further references on the legislative process, which was closely monitored in eucrim).

The *material scope* of the Directive is limited to specific areas of Union law, where the Union legislator believes in enhancing enforcement if breaches of law are reported. Still, the areas covered by the Directive are broad, including, e.g., public procurement, financial services, product and transport safety, protection of the environment, etc. Union acts that may be breached are set out in the annex to the Directive. The Directive expressly states that protection of the Union's financial interests is a core area of the Directive's scope, which is related to the fight against fraud, corruption, and any other illegal activity affecting Union expenditure, and the collection of Union revenues and funds or Union assets.

AUTHOR

Thomas Wahl

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2019, Vol. 14(4) eucrim pp 238 – 239
ISSN: 1862-6947
https://eucrim.eu

Legislation in the field of whistleblowing entails a number of legal problems regarding the *relationship with existing reporting mechanisms and conflicting areas*, e.g., the protection of classified information, the protection of legal/medical professional privilege, the secrecy of judicial deliberations, and rules of criminal procedure. The relationships in this regard are set out by the Directive. It also stresses that the Directive's provisions do not affect the Member State's responsibility to ensure *national security*. In particular, it shall not apply to reports of breaches of the procurement rules involving defence or security aspects unless they are covered by the relevant acts of the Union.

Regarding the Directive's *personal scope*, it broadly applies "to reporting persons working in the private or public sector who acquired information on breaches in a work-related context." The Directive lists a number of persons who must be included in the protection scheme at least, e.g.:

- Persons having the status of workers in the sense of Union law (including civil servants);
- Persons having self-employed status;
- Shareholders;
- Members of the administrative, management, or supervisory bodies of an undertaking, including non-executive members;
- Volunteers and trainees;
- Any persons working under the supervision and direction of contractors, subcontractors, or suppliers;

- Persons whose work-based relationship has since ended or is yet to begin (e.g., cases in which the information on breaches was obtained during the recruitment process or other pre-contractual negotiations);
- Facilitators and third persons who are connected with the reporting person (such as colleagues or relatives) and the legal entities owned by, or otherwise connected to, the reporting person in a work-related context.

However, persons may benefit from the protection under the Directive only if

(1) They 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 Directive; and

(2) They reported either internally in accordance with Article 7 or externally in accordance with Article 10, or made a public disclosure in accordance with Article 15.

The latter refers to the *reporting system* established by the Directive. The provisions mainly follow the flexible approach pushed through by the European Parliament. Accordingly, Member States shall "encourage" reporting through *internal* reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation. However, a whistleblower may also choose to *directly report* breaches to competent authorities. The Directive sets out the obligations, the necessary framework, the procedure, and the follow-up for both the internal and external reporting channels. This includes the obligation for companies with at least fifty workers to establish such channels and procedures for internal reporting and for follow-up.

Public disclosure (i.e., making information on breaches available in the public domain) – the third form of reporting – is protected by the Directive under the following conditions:

(1) The person first reported internally and externally, or directly externally, but no appropriate action was taken in response to the report within the timeframe referred to in the Directive; or (!)

(2) The person had reasonable grounds to believe that:

(i) the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or

(ii) 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.

Member States have the duty to ensure that the *identity* of the reporting person is *not disclosed* to anyone beyond the authorised staff members competent to receive/follow up on reports, without the explicit consent of that person. By way of derogation, the identity of the reporting person may be disclosed if this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including those with a view to safeguarding the rights of defence of the person concerned. In these cases, safeguards also apply to the reporting persons, e.g., he/she must be informed before his/her identity is disclosed, and he/she must receive a written explanation of the reasons for the disclosure.

Another key element of the Directive involves *protection measures against retaliation*. This includes obligations for Member States to prohibit any form of retaliation against whistleblowers. In this context, the Directive provides a non-exhaustive list of prohibited retaliatory acts. It includes not only work-related

measures, e.g., suspension/ dismissal, demotion, or withholding of promotion, but also acts harming the whistleblower's reputation, blacklisting, and psychiatric or medical referrals.

Beyond the prohibitions, Member States are obliged to proactively take the necessary measures to ensure that the whistleblower is protected from retaliation. Such measures include the following:

- Persons who report breaches or publicly disclose them shall not be considered to have breached any restriction on disclosure of information and shall not incur liability of any kind in respect of such a report or public disclosure, provided that they had reasonable grounds to believe that the reporting or public disclosure of such information was necessary to reveal a breach pursuant to this Directive;
- Reporting persons shall not incur liability in respect of the acquisition of or access to the information reported or publicly disclosed, provided that such acquisition or access did not constitute a self-standing criminal offence;
- If whistleblowers suffered a detriment, it shall be presumed that the detriment occurred in retaliation for the report or public disclosure (inversion of the onus of proof);
- Provided that they had reasonable grounds to believe that the reporting or public disclosure was necessary to reveal a breach, reporting persons can seek dismissal of legal proceedings, including those for defamation, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or for compensation claims based on private, public, or on collective labour law;
- If information includes trade secrets, but the reporting person meets the conditions of the Directive, such reporting or public disclosure shall be considered lawful.

Furthermore, the Directive requires Member States to make available a number of support measures to whistleblowers, e.g.:

- Comprehensive and independent information and advice on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned;
- Effective assistance from competent authorities;
- Access to legal aid in accordance with EU law (i.e., Directive (EU) 2016/1919 and Directive 2008/52/EC applicable in criminal and in cross-border civil proceedings) and national law.

Ultimately, Directive 2019/1937 obliges Member States to provide for "effective, proportionate and dissuasive *penalties*" applicable to natural or legal persons who hinder or attempt to hinder reporting; retaliate or bring vexatious proceedings against whistleblowers; or breach the duty of maintaining the confidentiality of their identity. In addition to compensating damages, effective, proportionate and dissuasive penalties must also be put in place against reporting persons who knowingly reported or publicly disclosed false information.

The Directive only establishes minimum rules, i.e., Member States can introduce or retain more favourable rules on whistleblowers protection. They may also extend protection as regards areas or acts not covered by the Directive (see above for the material scope). Member States must implement the Directive by 17 December 2021. Regarding the obligation for legal entities in the private sector with 50 to 249 workers to establish internal reporting mechanisms, Member States have time until 17 December 2023.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.

All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union