DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE *PROTECTION OF PERSONS WHO REPORT BREACHES OF UNION LAW*

Contributors:
Lawyer Dobrina Pavlova.
•
Jurisconsult Alexander Leshev
•
Petya Stankova

With the adoption of ***Directive (EU) 2019/1937*** of the European Parliament and of the Council of 23.10.2019 on the protection of persons who report breaches of Union law (the "**Directive**"), the European legislator has taken steps to unify the rules for protection of persons who submit information for violations - the so-called "Whistleblowers".

The key points in the **Directive** are summarised by the team of Georgiev, Todorov & Co. Law Offices.

CONTACTS

Address:
27 Petar Parchevich Str., Sofia 1000, Bulgaria

Telephone:
(+359 2) 937 65 00 / 01 / 02

E-mail: office@georg-tod.com

I. Overview and objectives of the Directive

The purpose of the ***Directive*** is to set common minimum standards to ensure a high level of protection for those who report breaches of EU law. While drafting it, the European Parliament and the European Council take into account the key role of these individuals in the effective detection, investigation and prosecution of breaches of EU law, which undoubtedly helps to strengthen transparency and accountability.

The European legislator has concluded that persons who work for a public or private organisation or are in contact with such an organisation in the context of their work-related activities are often the first to know about threats or harm to the public interest, which arise in that context. However, potential "whistleblowers" are often discouraged from reporting their concerns or suspicions for fear of retaliation. Therefore, the ***Directive*** aims to provide balanced and effective whistleblower protection, taking into account the need to improve law enforcement by introducing effective, confidential and secure reporting channels and ensuring the protection of individuals against revenge actions.

II. What kind of breaches does the Directive apply to?

The protection provided for in the **Directive** applies to those who report the following breaches of EU law:

1. **Breaches** falling within the scope of EU acts **affecting the following sectors:**

- *public procurement;*
- *financial services, products and markets and the prevention of money laundering and terrorist financing;*
- *product safety and compliance;*
- *transport safety;*
- *environmental protection;*
- *radiation protection and nuclear safety;*
- *food and feed safety, animal health and animal welfare;*
- *public health;*
- *consumer protection;*
- *protection of privacy and personal data and security of networks and information systems.*

2. **Infringements** affecting the financial interests of the EU referred to in Art. 325 of the TFEU **(anti-fraud)** and further specified in the relevant EU measures.

3. **Breaches related to the internal market**, including of **EU competition and State aid rules**, as well as breaches of **corporate tax law** and arrangements of which the purpose is to obtain a tax advantage and to evade legal obligations, thereby receiving a tax advantage, which defeats the object or purpose of the applicable corporate tax law.

III. Which persons are protected?

Protection is provided to reporting persons, who have "*reasonable grounds to believe, in light of the circumstances and the information available to them at the time of reporting, that the matters reported by them are true*".

The ***Directive*** seeks to avoid malicious, frivolous or abusive reporting, as it ensures that those who, at the time of the reporting, deliberately and knowingly reported wrong or misleading information do not enjoy

protection. Reporting incorrect information due to an unintentional error does not deprive the person of the protection of the ***Directive***.

The protection extends both to **(i)** employees and to **(ii)** partners and shareholders, **(iii)** persons involved in management bodies, **(iv)** self-employed persons, **(v)** contractors, **(vi)** subcontractors, **(vii)** suppliers, **(viii)** employees of infringer counterparties, etc. In addition, **(ix)** persons whose employment has ended, as well as **(x)** job seekers and **(xi)** persons wishing to provide services to an organization, who receive information about violations during of the selection or other stage of the pre-contractual relationship which may be retaliated against. It also provides for the protection of **(xii)** volunteers, paid and unpaid trainees.

The ***Directive*** provides protection against retaliation against the whistleblowers themselves (suspension, harassment, demotion, disciplinary action, etc.), but does not end there. It also provides protection against indirect responses, namely against assistants, colleagues, relatives of the whistleblower, who are also linked through work with the whistleblower's employer, client or recipient of services.

IV. Is it necessary that the offense being reported has already been committed?

No, protection is granted to persons who provide information necessary to reveal breaches which have already taken place, breaches which have not yet materialised, but are very likely to take place, acts or omissions which the reporting person has reasonable grounds to consider as breaches, as well as attempts to conceal breaches. In order for a person to benefit from these rules, protection is justified also for persons who do not provide positive evidence but "*raise reasonable concerns or suspicions*".
At the same time, protection should not apply to persons who report information which is already fully available in the public domain or unsubstantiated rumours and hearsay.

V. How should a breach be reported so that the whistleblower can enjoy protection?

The information should be transmitted in the manner provided for in the ***Directive*** - through an internal channel for reporting breaches to the undertaking or establishment or externally - to a public authority.

Protection is also provided to persons who make this information public through online platforms or social media or to the media, elected officials, civil society organizations, trade unions or professional and business organizations.

VI. Obligation to create internal reporting channels

All enterprises having 50 or more workers should be subject to the obligation to establish internal reporting channels, irrespective of the nature of their activities. Internal channels can take the form of internal units or be outsourced to external third parties (external reporting platform providers, external advisers, auditors, trade union representatives or employee representatives).

The reporting channels should enable persons to report in writing and submit reports by post, by physical complaint box(es), or through an online platform, whether it be on an intranet or internet platform, or to report orally, by telephone hotline or other voice messaging system, or both. Upon request by the reporting person, such channels should also enable reporting by means of physical meetings, within a reasonable timeframe.

The reporting person should be informed within a reasonable timeframe about the action envisaged or taken as follow-up to the report and the grounds for the choice of that follow-up. A reasonable timeframe for informing a reporting person should not exceed three months. The persons to whom the internal channel is assigned should take the necessary actions to investigate and put an end to the breach.

VII. Obligation to create appropriate channels for external reporting

The ***Directive*** imposes a clear obligation on competent authorities to establish appropriate external reporting channels, to diligently follow up on the reports received, and, within a reasonable timeframe, give feedback to the reporting persons.

It should be for the Member States to designate the authorities competent to receive information on breaches falling within the scope of this ***Directive*** and give appropriate follow-up to the reports. Staff members of the competent authorities who are responsible for handling reports should be professionally trained, including on applicable data protection rules, in order to handle reports and to ensure communication with the reporting person, as well as to follow up on the report in a suitable manner.

VIII. Penalties

Member States are required to impose penalties for:

- obstructing or attempting to obstruct the signaling;
- taking measures to retaliate against whistleblowers;
- initiation of malicious proceedings against whistleblowers;
- breach of the obligation to maintain the confidentiality of the personal data of the whistleblowers.
- a whistleblower who has knowingly submitted or disclosed publicly false information (for this violation a right to compensation for the person, who has suffered the damage should also be provided).

IX. In what time frame should Bulgaria adopt national rules in implementation of the Directive?

Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by the 17th of December 2021.

As regards **legal entities in the private sector with 50 to 249 workers**, Member States shall by the **17th of December 2023** bring into force the laws, regulations and administrative provisions necessary to comply with the **obligation** to establish internal reporting channels.

This text does not constitute a legal advice and should not be taken into account in resolving legal disputes, but only to inform readers.

The team of Georgiev, Todorov & Co. Law Offices remains available for assistance and additional information related to the implementation of the Directive.