CEELI INSTITUTE

ADVANCING THE RULE OF LAW

SPEAKING UP

Protecting Whistleblowers in Central and Eastern Europe

SPEAKING UP

Protecting Whistleblowers in Central and Eastern Europe

Kieran Pender
Principal Author

Christopher Lehmann
Halya Senyk
Editors

Prague, September 2021

ABOUT THE CEELI INSTITUTE

The CEELI Institute is a Czech public-benefit (not-for-profit) organization based in Prague, dedicated to the development and training of an international network of legal and judicial professionals committed to advancing the rule of law. Through innovative training programs and other activities, the Institute works with judges, lawyers, and civil society actors to build laws-based societies. The CEELI Institute prides itself on the diversity and quality of the programs it has developed, the peer-to-peer exchanges it fosters, the innovative nature of its programming, and its legacy of contributing to the advancement of the rule of law in vulnerable countries. Our efforts are focused on creating independent, transparent, and effective judiciaries, strengthening democratic institutions, fostering efforts to combat corruption, bridging difficult conflicts, promoting human rights, and supporting lawyers and civil society actors in repressive environments. The CEELI Institute is based at the Villa Grébovka, in Prague, a historic nineteenth century building now renovated into a state-of-the-art residence and conference center.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This report was produced as part of a larger CEELI Institute project to combat fraud and corruption in the health care sector in Central and Eastern Europe. The project was funded by the U.S. Department of State, Bureau of Democracy, Human Rights and Labor (DRL).

The principal author of the report is Kieran Pender, Honorary Lecturer, ANU College of Law, The Australian National University, Canberra. Substantial contributions to this report were prepared and received from our partner organizations in this project, the Expert Forum (Romania); Transparency International (Slovakia); the Bulgarian Institute for Legal Initiatives (BILI)(Bulgaria); and the NGO, K-Monitor (Hungary).

Thanks also to Halya Senyk, Senior Program Advisor at the CEELI Institute and Maggie Utecht, CEELI Institute Legal Intern (William & Mary Law School) for their valuable contributions in developing this Report

EXECUTIVE SUMMARY

A. By 17 December 2021, all European Union (EU) member states are required to have transposed into national law the *Directive 2019/1937 on the protection of persons who report breaches of Union law* **(the Directive)**. If successfully implemented, the Directive has the potential to have a transformative impact on governance, integrity and anti-corruption efforts in the EU. The Directive aims to provide world-class whistleblowing protections for those who speak up against wrongdoing.

B. To aid the transposition process in Bulgaria, Hungary, Romania and Slovakia and, particularly, to facilitate constructive engagement by civil society in each jurisdiction, this report considers how domestic law compares with the requirements of the Directive. It finds that:

   i. In Bulgaria, existing whistleblowing protections are limited, and significant legal reform is required prior to the transposition deadline;

   ii. In Hungary, the existing whistleblowing law provides a baseline of protections, but some reform will be required to ensure alignment with the Directive;

   iii. In Romania, a draft law to transpose the Directive is very promising but would benefit from further revision; and

   iv. In Slovakia, a relatively new whistleblowing law is broadly consistent with the Directive and will only require minor technical amendments to ensure compliance.

C. The report concludes with several recommendations. These include:

   i. A holistic, 'horizontal' approach to the transposition of the Directive is critical – limiting the material scope of new laws to only wrongdoing covered by EU competency would have an extremely negative effect;

   ii. Member states must be cautious to avoid reducing the protections already afforded to whistleblowers in the name of implementing the Directive (something prohibited by the Directive's non-regression clause);

   iii. Maximum possible flexibility for speaking up is necessary – some existing limitations around public reporting and the lack of explicit protection for anonymous whistleblowers whose identity is subsequently revealed will require amendment to laws in each country to ensure alignment with the

Directive. Jurisdictions should also be extremely careful with the standards required for whistleblowers to make reports and avoid the whistleblower's motive being a relevant factor (except in cases of bad-faith, false information reporting);

iv. Comparative experience indicates that the mechanisms around retaliation claims are critical to the effective utilisation of whistleblower protections. Member states should prioritise making remedies accessible and not unduly technical. Legal assistance and other support should be provided to whistleblowers;

v. In other jurisdictions, whistleblowing laws have often proven ineffective in practice and difficult to scrutinise. To mitigate this risk, each jurisdiction should ensure transparency, data collection and ongoing review are at the heart of their schemes;

vi. Member states should adequately fund a designated whistleblowing authority (as required by the Directive) and support – through funding and other means – civil society and other stakeholders to contribute to the design, implementation and ongoing promotion of the law. The experience in other jurisdictions has been that civil society plays a major role in the ultimate success of effective whistleblowing laws.

INTRODUCTION

1. In 2020, the CEELI Institute received funding from the U.S. Department of State, Bureau of Democracy, Human Rights and Labor to undertake an initiative to address corruption in the healthcare sectors in Bulgaria, Hungary, Romania and Slovakia. One element of the initiative is focused on whistleblower protection legislation in each jurisdiction, with a view to developing practical recommendations to aid the implementation of the EU Directive in each jurisdiction (collectively the Project). The CEELI Institute appointed Mr Kieran Pender as an independent expert to prepare a report. Mr Pender's expertise is outlined at Appendix 1.

2. To undertake the Project, the CEELI Institute partnered with civil society organisations in each jurisdiction: the Bulgarian Institute of Legal Initiatives (BILI), K-Monitor (Hungary) (KM), Expert Forum (Romania) (EFR) and Transparency International Slovakia (TIS) (collectively the Partner Organisations). The Partner Organisations provided the CEELI Institute with detailed information on existing whistleblowing protections in each jurisdiction, to enable comparison with the requirements of the EU Directive. The ultimate purpose of this research is to enable the Partner Organisations, with the CEELI Institute's support, to effectively advocate during the transposition process.

I. THE EU WHISTLEBLOWER DIRECTIVE

3. It is instructive to begin by briefly providing some context to the development of the Directive. The concept of whistleblowing dates back to Ancient Greece; the first laws to encourage and incentivise whistleblowing were introduced in England during the early Middle Ages. However, the phrase 'whistleblowing' did not enter the English lexicon until the 1970s. Although the United States pioneered early modern whistleblower protection laws in the 1980s, it would take several decades for standalone protections to reach the legislative agenda in Europe.[1]

4. In different ways and to different extents, any purported whistleblower protections law seeks to do one or more of three things:

    a. Protect whistleblowers;

    b. Reward whistleblowers; and/or

    c. Empower whistleblowers.

5. In the late 2000s, the Parliamentary Assembly of the Council of Europe began to consider the issue of whistleblower protections in Europe. In 2010, the Assembly encouraged European countries to review what protections, if any, they provided. In the early 2010s, a number of European countries began to develop and ultimately implement comprehensive whistleblower protection laws.

6. The case of LuxLeaks and Mr Antoine Deltour provided considerable impetus. Mr Deltour leaked documents relating to favourable tax treatment of large multinationals by Luxembourg; the leaks gave momentum to tax reform in the EU, and Mr Deltour was awarded the European Parliament Citizen's Prize. Simultaneously, he was prosecuted and convicted in Luxembourg's courts (although the convictions were ultimately overturned). This dissonance highlighted to many in the EU that robust, EU-wide whistleblower protections were required. In 2017, the European Commission began consultation on a possible EU directive.

7. The subsequent process saw considerable evolution of a draft directive and much negotiation and compromise between the European Commission, European Parliament and Council of the EU. Civil society played a major role in securing robust rights for whistleblowers.

[1] For a brief history, see Kieran Pender, Sofya Cherkasova and Anna Yamaoka-Enkerlin, 'Compliance and Whistleblowing: How Technology will Replace, Empower and Change Whistleblowers' in Jelena Madir (ed), *FinTech: Law and Regulation* (Edward Elgar, 2019).

8. Broadly speaking, the Directive represents international best-practice. There are some shortcomings and a number of innovative features that are yet to be tested in practice. Nevertheless, the Directive is a landmark step for the protection of whistleblowers globally. It will improve existing whistleblower protections in every EU member state; in many, extant protections are limited or non-existent.

9. Transposition of the Directive into national law is an important and challenging next step. The Directive provides only limited detail and guidance; the operative text contains just 29 articles. If transposition is undertaken effectively, holistically and with fidelity to the Directive's underlying intent, whistleblowers across the EU will benefit. However, there are many examples of whistleblower protection laws in other jurisdictions that mirror best-practice on paper and have negligible impact in reality. The transposition process is an important first step, but it is just that. Effectively protecting whistleblowers requires ongoing cultural and societal change.

II. EXISTING NATIONAL LAWS

10. Three of the four jurisdictions considered in the Project have existing laws which provide some standalone protections to whistleblowers:

    Bulgaria: N/A

    Hungary: *Act CLXV/2013 on Complaints and Public Disclosures*

    Romania: *Public Servants Disclosure Protection Act (571/2004)*

    Slovakia: *Act No. 54/2019 Coll., on the Protection of Whistleblowers*

11. As an initial step, it is helpful to consider each jurisdiction's existing frameworks against the requirements of the EU Directive. Partner Organisations were asked to provide answers in relation to the questions about national law (the full list of questions is at Appendix 2).

A. BULGARIA

12. While Bulgaria does not currently have a standalone whistleblower protections law, protections do exist for speaking up against wrongdoing in limited circumstances. As BILI explained in its research memorandum:

    > *The foundations of the whistleblowing protection in Bulgaria were laid with the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act (articles 48-51), adopted in 2018. The concept of whistleblowing and its protection is relatively new for the Bulgarian society. As a consequence, whistleblowing as a construction still opens some interesting debates, provoked by the communist past…*

13. Additionally, Bulgarian labour law provides some protections for employees who are dismissed for reporting on illegal conduct, and sectoral whistleblowing laws exist in certain sectors.

Scope

14. The existing whistleblower protections in Bulgaria are extremely limited in material scope, confined effectively to high-level corruption. Accordingly, to comply with the Directive, Bulgaria will be required to implement a new law with expanded material scope. Encouragingly, BILI reported that there was initial consensus at a preliminary working group in relation to the *Directive* that 'reporting for violation of the internal law should have the same level of protection like those reporting for violation of the EU legislation.'

15. However, in relation to personal scope, BILI indicated that existing domestic law does not differentiate between public and private sector employees, nor is it limited to current employees (and thereby might include contractors, former employees, interns, etc). Such broader personal scope will be necessarily incorporated in the transposition of the Directive.

Conditions for Reporting

16. In cases covered by the *Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act,* reporting protocols are provided. At a more general level, the *Administrative Procedure Act* (Article 111, (4)) provides that reports concerning violation of law are not accepted and processed if they relate to conduct taking place more than two years prior.

17. Anonymous reporting is not permitted under the *Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act;* anonymous reports are not accepted or processed. However, there are other avenues for anonymous reporting in Bulgaria. BILI explained:

> *At the same time, most of the institutions' offices (ministries, agencies, local departments, municipalities, police, etc.) are equipped with boxes for collection of anonymous signals from citizens for the need of their internal anticorruption control procedures (Inspectorates). The efficiency of this tool, however, is zero or very close to zero for all institutions, according to a research BILI had done in 2017.*

Internal Reporting

18. Bulgarian law regulates, to some extent, the collection and coordination of reports by public sector agencies. The *State Administration Act* (Article 46) requires all the ministries to have internal Inspectorates with a broad spectrum of powers, including some actions for internal reporting. However, it has been BILI's experience that, with some notable exceptions, these internal procedures remain rudimental and inefficient. Local legislation does not require private sector organisations to develop internal channels for reporting, albeit recently-introduced money laundering laws do impose some reporting requirements in that narrow sphere.

External Reporting

19. Under Bulgarian law, internal reporting is not a prerequisite for reporting to relevant state authorities. There are some protocols for receiving and investigating reports, and the Commission for Combating Corruption and Confiscation of Illegally Acquired Property is required to report annually to the National Assembly.

Public Reporting

20. At present, Bulgarian law provides no regulation in relation to public whistleblowing, such as to the media. Protections will be required for such whistleblowing, in appropriate circumstances, to ensure alignment with the Directive.

Confidentiality and Record-Keeping

21. Bulgarian law provides for confidentiality in relation to whistleblowing to state authorities. It does not provide such confidentiality in relation to internal, private sector whistleblowing – and hence new obligations will be required in line with the Directive.

Retaliation

22. There are limited protections from retaliation for Bulgarian whistleblowers. The *Administrative Procedural Code* (article 108 (1)) provides that no one could be prosecuted and suffer retaliation because they submitted a report against wrongdoing. Whistleblowers covered by the *Corruption and Unlawfully Acquired Assets Forfeiture Act* are entitled to relatively robust protection. Additionally, protections are available in labour law, albeit BILI described this protection as only constituting a prohibition in relation to extreme forms of retaliation.

23. Whistleblowers are not entitled to immunity from civil or criminal liability, except in the context of money laundering, where whistleblowing does not constitute a breach of secrecy, confidentiality or data protection provisions under contract or law. These protections will need to be replicated for all whistleblowers to comply with the Directive.

Burden and Remedies

24. Bulgarian law presently does not provide for reverse burden of proof (as is required by the Directive) in either whistleblowing proceedings or in comparable areas of law. Interim orders are also not available. However, under the (limited) protections in the *Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act,* whistleblowers are able to claim compensation for economic and non-economic loss in the case of retaliation, and courts have the ability to order reinstatement for dismissed employees.

Rights of Persons Concerned

25. The rights of those accused by a whistleblower have robust protection in Bulgarian law. As BILI explained:

The presumption of innocence is a constitutional norm in Bulgaria, and on no account could it be sidestepped by any other legislative acts, including those regulating the numerous aspects of whistleblowing.

Penalties

26. Bulgarian law does not presently provide penalties against individuals or organisations who obstruct whistleblowing. Penalties for retaliation are limited to those available at general law. Penalties are available, under general breach of confidentiality obligations, if an official leaked information which breached a whistleblower's confidentiality entitlement. These penalty provisions will need to be strengthened during the transposition process.

Other

27. To comply with the Directive, the transposed Bulgarian law will also be required to provide ongoing review and data collection requirements and prohibit employees from being able to waive their whistleblowing rights.

Summary

28. While Bulgaria has some protections for whistleblowers, the absence of a standalone, comprehensive national whistleblowing law means that considerable legislative reform will be required to comply with the *Directive.* Most importantly, a robust, three-tier reporting framework, comprehensive protections for whistleblowers and the procedural tools required for these to be accessible will all be needed in Bulgarian law by the end of 2021.

B. HUNGARY

29. There has been limited progress in Hungary towards transposition of the Directive, largely, it appears, as a result of a belief that the existing whistleblowing law – *Act CLXV/2013 on Complaints and Public Disclosures* – is broadly sufficient.

Scope

30. The material scope of *Act CLXV/2013* is expansive: 'a public interest disclosure calls attention to a circumstance the remedying or discontinuation of which is in the interest of the community or the whole society.' The personal scope is more limited: the protections and requirements it provides are mandatory among public sector employers but optional among private sector employers, where it is, in any event, restricted to breaches of rules of conduct. This scope will need to be expanded to align with the Directive.

Conditions for Reporting

31. Protection is not available where a whistleblower discloses in bad faith by providing false or deceptive information and (a) there is evidence of criminal offence or (b) there are reasonable grounds to believe the whistleblower caused unlawful damage.

32. Anonymous reporting is not permitted, albeit there are provisions for identified whistleblowers to request anonymity during regulatory processes.

Internal Reporting

33. *Act CLXV/2013* imposes some requirements in relation to internal reporting systems, although its protocols are limited. The law also establishes a 'lawyer for the protection of whistleblowers' to aid private organisations in implementing internal reporting systems.

34. *Act CLXV/2013* specifies timeframes for investigation – 30 days, with extensions in special circumstances, in the public sector and maximum three months in the private sector.

External Reporting

35. The Commissioner for Fundamental Rights is the designated external reporting recipient authority.

Public Reporting

36. The Hungarian law provides no explicit protection or authorisation for public reporting by whistleblowers. This will need to be addressed to ensure alignment with the Directive.

Confidentiality and Record-Keeping

37. *Act CLXV/2013* provides some confidentiality and record-keeping requirements, albeit these are not comprehensive and will require amendment to comply with the Directive.

Retaliation

38. While *Act CLXV/2013* prohibits retaliation – 'any action taken as a result of a public interest disclosure which may cause disadvantage to the whistleblower shall be unlawful even if it would otherwise be lawful' – the relevant clause is otherwise vaguely worded. The only support available is via the Commissioner for Fundamental Rights or the lawyer for the protection of whistleblowers (where the service is provided by the private sector employer). Legal aid is available

as generally provided, but there is no specific provision for support for whistleblowers. More robust protections will be required to ensure alignment with the Directive.

39. The law does not provide immunity from civil or criminal liability for whistleblowers. Such immunity will need to be added to Hungarian law.

Burden and Remedies

40. No reverse burden is provided, although a comparable mechanism is available in law on equal treatment. That mechanism should be implemented in the whistleblowing context to ensure alignment with the Directive.

Rights of Persons Concerned

41. Fundamental law provides basic rights to fair procedures to all Hungarian citizens, and the *Act CLXV/2013* outlines specific procedural safeguards.

Penalties

42. There are minimal penalties available for wrongdoing under *Act CLXV/2013.* Retaliation is only regarded as a misdemeanour, where prosecuted.

Other

43 The Commissioner for Fundamental Rights has ongoing review and data collection obligations.

Summary

44. While Hungary already has an established whistleblower protection framework, *Act CLXV/2013* does not satisfy the requirements of the *Directive.* To ensure alignment, the law will be required to be amended in several respects, including:

    a. Providing clarity around internal reporting obligations, including for private companies;

    b. Creating more robust protections, including through the inclusion of a reverse burden provision, stronger penalties and immunity from criminal or civil suit in relation to the disclosure;

    c. Protection in relation to public reporting in certain circumstances; and

    d. Greater systems of support for whistleblowers.

C. ROMANIA

45. Romania has an existing law, *Public Servants Disclosure Protection Act* (571/2004), albeit it only applies to public sector employees. Additionally, there are some sectoral protections. In March 2021, the Romanian Ministry of Justice released a draft bill for public consultation. The draft law is broadly faithful to the requirements of the Directive and will apply not only in areas of EU competency, but in relation to all wrongdoing. The draft law will require all public authorities and private organisations with at least 50 employees to set up internal reporting channels. However, companies that employ between 50 and 249 employees will have a longer time period before compliance is expected. These are both positive indications that Romania intends to take a holistic approach and go beyond the mandatory requirements of the Directive. A revised draft law was circulated in mid-May 2021.

46. Given the broad alignment between the latest draft law and the Directive, it is not necessary to consider the draft law step by step. Instead, the following commentary is offered as to areas for improvement required in the draft law to ensure it meets the standards of the Directive:

    a. Arguably the most significant limitation of the draft law is its limitations in relation to public reporting. Romania's existing protections provide greater empowerment to whistleblowers. As EFR explained in a recent policy brief, 'the law currently in force gives the whistleblower the possibility to choose among various reporting channels freely.'[2] Regrettably, by implementing the Directive's narrower public reporting clause, this freedom has been diminished. In this way, it is arguable that the draft law contravenes the Directive's non-regression clause. The existing protections for public reporting should be retained;

    b. Greater legislative clarity is required around internal reporting processes and frameworks, including deadlines for investigations;

    c. The 'National Agency for Integrity' is given a central role in the external reporting scheme. While this is not inherently bad, there is risk by focusing reporting through one avenue, rather than a disaggregated approach where whistleblowers can approach any agency with relevant competency, that the designated agency will become overwhelmed unless sufficiently resourced. This could in turn lead to greater public reporting;

    d. Greater clarity would be helpful in relation to the conditions for protection and what constitutes vexatious or false reporting. Currently, the draft

[2] Expert Forum Romania, 'Draft Law on the Protection of Whistleblowers – EFOR's Comments and Position (Policy Brief No 113, April 2021) 2.

law requires 'good reason to believe that the information relating to the reported breaches was true at the time of reporting.' While this is broadly consistent with the Directive, which requires 'reasonable grounds' to believe, it must also be considered in the context of the significant financial penalty imposed on 'reporting information on violations of the law, knowing they are unreal,' which is a misdemeanour. More detail in the draft bill on this standard would be helpful; and

e. The draft law includes a provision prohibiting employment conditions that seek to waive the Directive rights. This is a positive development and complies with article 24 of the Directive. However, greater detail is needed about the scope of the prohibition, particularly given the number of different forms of employment-related confidentiality obligations; and

f. The draft law needs to clearly implement the reverse burden in cases of retaliation – whereby the Directive provides that it must be presumed the retaliation was taken in bad faith. The draft law seeks to do this in clause 23, but the wording could be improved for clarity.

D. SLOVAKIA

47. In Slovakia, whistleblowers are protected by *Act No. 54/2019 Coll. on the protection of whistleblowers notifying activities undermining the functioning of civil society and the amendment of certain other Acts of 30 January 2019* ***(Act No. 54/2019).*** At the time of writing, to the best of the authors' knowledge, minimal work had been undertaken in relation to transposition in Slovakia.[3] However, only limited work may be required to comply with the Directive. As TIS explained:

> *Most of the provisions of the Directive have already been transposed (in substance). Protection granted under the Act is in some respects even broader than under EU Directive.*

Scope

48. The material scope of Slovakia's whistleblower protections is not confined; the law covers 'all activities undermining the functioning of civil society.' The personal scope is broad, applying to both public and private sector employees, albeit the definition of employee is narrow – limited to employees and closely-linked individuals who work for the same employer. *Act No. 54/2019* also provides protection to whistleblowers who acted prior to the enactment of the law.

[3] Transparency International and Whistleblowing International Network, *Are EU Governments Taking Whistleblower Protection Seriously? A Progress Report on Transposition of the EU Directive* (2021) 29.

Conditions for Reporting

49. The Slovakian whistleblowing law establishes a system of protections for whistleblowers. It is predicated on the whistleblower having reasonable grounds for their reporting (notification) and the whistleblowing being in good faith. Anonymous whistleblowing is permitted, albeit only identified whistleblowers are entitled to claim protection (albeit they can seek identity protection when making their notification).

Internal Reporting

50. *Act No. 54/2019* requires public bodies of more than 5 employees and private bodies of more than 50 employees to establish internal reporting channels. Organisations are required to nominate a 'responsible person' for the receipt of whistleblowing reports and have 90 days – with the possibility of a 30 day extension – to investigate a disclosure. Once the investigation concludes, the whistleblower must be notified within 10 days.

External Reporting

51. The law also empowers whistleblowers to notify the public prosecutor, administrative bodies or, in any case, the Whistleblowing Office of the Slovak Republic (which was recently established and is not, at the time of writing, operational).

Public Reporting

52. Protection for public reporting may be available upon the order of the Office, provided the individual believed the notification to relevant authorities would not lead to proper investigation or would lead to retaliation.

Confidentiality and Record-Keeping

53. The law provides for confidentiality for whistleblowers and provides protocols, record-keeping and data protection.

Retaliation

54. Retaliation against whistleblowers is prohibited by *Act No. 54/2019.* The scheme deployed is somewhat atypical. TIS explained:

> *The public prosecutor (in criminal proceedings) or administrative body (in the administrative proceeding) is obliged to grant protection to any person who submits a notification on serious anti-social activity which is a criminal*

> *or administrative offense (so called qualified notification), and who requests protection … In case the employer undertakes any action towards a person who submitted a notification on anti-social activity but who has not yet been granted protection, such employee is entitled to request that the Office suspend the effectiveness of such action. The Office is required to suspend the effectiveness unless the employer proves that his/her action towards the whistleblower has no causation with the notification submitted by the whistleblower. … If there was granted protection by the Office, the employer may undertake any actions only with the prior consent of the Office.*

55. The anti-retaliation protections are broadly defined. The Office is required to assist whistleblowers. Whistleblowers are also entitled to free legal services. The law also provides a reward system.

56. The law also provides immunity from confidentiality obligations. TIS explained:

> *Notification of activities undermining the functioning of civil society is considered to be neither a breach of contractual duty of confidentiality nor a breach of confidentiality duty according to individual legal Acts if this duty follows from employment, profession, standing, or function and it is not a duty of confidentiality connected to the protection of secret matters, postal confidentiality, business confidentiality, bank confidentiality, telecommunications confidentiality or tax confidentiality. Protection of confidential statistical data is not considered a duty of confidentiality in connection to the provision of health documentation data, the confidentiality duty of news service members or the confidentiality duty related to the provision of legal services.*

Burden and Remedies

57. *Act No. 54/2019* contains a reverse burden of proof and the ability for interim relief.

Rights of Persons Concerned

58. The rights of the person concerned are robustly protected via the constitution, and information relating to the identity of the accused is protected by criminal and administrative procedures.

Penalties

59. Slovakia's whistleblowing law contains a range of penalties for failing to comply with the law, including taking retaliation action, breaching a whistleblower's confidentiality or failing to set up internal reporting channels. TIS considered that the potential quantum of the penalties was sufficiently serious to be dissuasive.

Other

60. An annual review requirement is imposed on the Office.

Summary

61. On paper, Slovakia's whistleblower protections are extremely robust. However, compliance with the Directive may require a few minor amendments – the good faith standard in *Act No. 54/2019* is contrary to the Directive (which is limited to 'reasonable belief'), and the personal scope of the law may need to be revised to encompass the Directive's wider application. The conditions for seeking protection for public reporting may also require minor technical amendment to ensure alignment with the Directive.

III. RECOMMENDATIONS

62. The foregoing analysis of whistleblower protections in each jurisdiction reveals that none is entirely consistent with the requirements of the Directive. Relevantly:

    a. Bulgaria has the weakest protections for whistleblowers, and substantial legislative reform will be required to ensure compliance with the Directive;

    b. Hungary's existing domestic law will require moderate reform to ensure alignment;

    c. Romania's draft law is very robust and faithful to the requirements of the Directive, but will benefit from a number of revisions before being enacted; and

    d. Slovakia's law is broadly compliant with the Directive and, in some cases, is even more generous. However, a number of technical amendments will be required before December 2021 to ensure complete alignment.

63. A number of general comments can also be made that will assist the effective transposition and implementation of the Directive.

64. Firstly, it is essential that the transposition does not limit the protections in the Directive to those speaking up in relation to wrongdoing with an EU nexus. The prospect of inconsistent protections between those speaking up about breaches of local law with no EU nexus and those covered by the Directive is extremely troubling. While the Romanian draft law and Slovakian existing law are comprehensive, it is important that the ongoing transposition in Bulgaria and Hungary adopt a holistic approach.

65. Secondly, there is a risk that, in transposing the Directive into national law, more beneficial existing domestic law will be replaced. The Directive explicitly provides, in article 25, that member states may introduce or retain provisions more favourable to whistleblowers than the Directive and 'the implementation of this Directive shall under no circumstances constitute grounds for a reduction in the level of protection already afforded by Member States in the areas covered by this Directive.' Initial transposition discussions and drafts in the jurisdictions covered by this Report suggest there is a real risk of regression in certain limited contexts. This must be avoided.

66. Maximum possible flexibility for speaking up is necessary for effective whistleblower protections. Bulgaria and Hungary both need to provide protection for public reporting in appropriate circumstances, and the Slovakian provisions may require minor amendment to ensure alignment with the Directive. None of the current or proposed schemes across the four countries considered

actively authorise anonymous reporting, although there are some provisions for seeking confidentiality and protections for anonymous whistleblowers who are subsequently identified. Recognising the important role that can be played by anonymous reports and incorporating that into whistleblowing law, as is permitted (although not required) by the Directive, would be a helpful step. Jurisdictions should also be wary of the standards they impose upon whistleblowers in speaking up. Good faith was considered and explicitly rejected as a standard for protection during the development of the Directive; it is important that a good faith does not 'sneak in the backdoor' of transposed law via other such standards. Whistleblowers should be judged based on the public interest in what they disclose, their motives should not be put on trial.

67. Making the protections real in practice and not merely 'paper rights' requires that they be accessible. That means making the provisions as straightforward as possible, ensuring they are claimant-friendly (including via the Directive-required reverse burden of proof), that judges and court staff are trained on the intricacies of whistleblowing law and that whistleblowers can assist legal assistance and other support. While good legislation is important in this respect, translating law into practice most significantly requires funding for training, awareness and support.

68. In most countries with whistleblowing laws, the laws remain relatively novel and, too often, underutilised. Among 37 countries studied in a joint report by the International Bar Association and Government Accountability Project, 33 had fewer than 15 publicly reported whistleblowing cases for the entirety of each law's enactment.[4] When whistleblowers do take advantage of these laws, often they experience challenges that were not foreseen by the drafters of the law. To enable proper monitoring of these laws once the Directive has been transposed and ensure they remain up to date and effective, the transposition process should ensure robust transparency, data collection and ongoing review requirements. While the Directive itself mandates some data collection, more expansive requirements can and should be inserted into laws during transposition to ensure maximum impact.

69. The Directive requires member states to designate one or more competent authorities to receive external disclosures. It also requires a competent authority to provide support and assistance to whistleblowers. This authority or authorities must be adequately funded to ensure the can play their role – both in receipt of disclosures and in support of whistleblowers more broadly.

70. Similarly, civil society can and should play a major role in making whistleblower protection provisions work in practice. Governments should provide funding and support to that end. The lived experienced in other jurisdictions is that effective civil society engagement with whistleblowing laws – for example,

4 IBA and GAP, 'Are Whistleblowing Laws Working? A Global Study of Whistleblower Protection Litigation' (2021) 11.

providing pro bono legal support to whistleblowers – makes a major difference to the ultimate success of the law. Such civil society services should be funded accordingly. Finally, other stakeholders, including trade unions, professional associations and employer groups, can also contribute to the transposition and effective implementation of the Directive.

IV. CONCLUSIONS

Upon promulgation, the EU Directive represented a landmark development in global efforts to protect whistleblowers. In 1978, not a single country had a standalone national law dedicated to protecting those who spoke up about wrongdoing. Once all EU member states transpose the Directive, at least 62 countries globally will have such laws – representing about one-third of all nations. The Directive is broadly consistent with what has emerged as international best-practice for protecting whistleblowers. The transposition will apply those robust protections, on paper at least, to almost a billion Europeans. That is a laudable development.

Yet the transposition process is not proceeding smoothly. Despite the Covid-19 pandemic highlighting the importance of whistleblowing, the subsequent health and economic crises have been used to justify delay and inaction. Despite the transposition deadline rapidly approaching (in December 2021), a February 2021 report by Transparency International and Whistleblowing International Network found that two-thirds of EU member states had not started or had only made minimal progress on the transposition. The report observed: 'It is uncertain whether any EU country will transpose the Directive by the December deadline. This lack of urgency from EU member states is concerning.'[5] This observation was consistent with the research undertaken by each Partner Organisation for this report. One Partner Organisation, for example, wrote:

> *There isn't still a real discussion about the Directive in [the jurisdiction]. Some of the interested parties are still unaware of the process of its transposition (for example, the trade unions, which are supposed to have an important role in the implementation of the Directive's requirements concerning the private sector, were informed by the [Partner Organisation] that such a process has begun.*

It is hoped that this report will assist Partner Organisations and other interested civil society organisations in constructively engaging with their respective governments in ensuring the Directive is transposed in a robust, compliant manner. As this research has indicated, in not one of the four countries considered is the whistleblower law entirely aligned with the Directive, although the draft law in Romania and the existing law in Slovakia come very close. All four countries require legislative reform and – as experience from other jurisdictions highlights – cultural change to ensure the Directive is effective in practice. The EU Directive is a momentous global occasion; if properly transposed, it will provide robust, world-class protections to whistleblowers across the region, including in Bulgaria, Hungary, Romania and Slovakia. To ensure whistleblowers in these and other jurisdictions can speak up tomorrow, civil society must speak up today and insist upon proper, consultative and holistic transposition of the Directive.

5 Transparency International and Whistleblowing International Network, *Are EU Governments Taking Whistleblower Protection Seriously? A Progress Report on Transposition of the EU Directive* (2021) 6.

APPENDIX I

DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 October 2019
on the protection of persons who report breaches of Union law

CHAPTER I
SCOPE, DEFINITIONS AND CONDITIONS FOR PROTECTION

Article 1
Purpose

The purpose of this Directive is to enhance the enforcement of Union law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches of Union law.

Article 2
Material scope

1. This Directive lays down common minimum standards for the protection of persons reporting the following breaches of Union law:

    (a) breaches falling within the scope of the Union acts set out in the Annex that concern the following areas:

        (i) public procurement;

        (ii) financial services, products and markets, and prevention of money laundering and terrorist financing;

        (iii) product safety and compliance;

        (iv) transport safety;

        (v) protection of the environment;

        (vi) radiation protection and nuclear safety;

        (vii) food and feed safety, animal health and welfare;

        (viii) public health;

(ix) consumer protection;

(x) protection of privacy and personal data, and security of network and information systems;

(b) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures;

(c) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

2. This Directive is without prejudice to the power of Member States to extend protection under national law as regards areas or acts not covered by paragraph 1.

Article 3
Relationship with other Union acts and national provisions

1. Where specific rules on the reporting of breaches are provided for in the sector-specific Union acts listed in Part II of the Annex, those rules shall apply. The provisions of this Directive shall be applicable to the extent that a matter is not mandatorily regulated in those sector-specific Union acts.

2. This Directive shall not affect the responsibility of Member States to ensure national security or their power to protect their essential security interests. 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.

3. This Directive shall not affect the application of Union or national law relating to any of the following:

(a) the protection of classified information;

(b) the protection of legal and medical professional privilege;

(c) the secrecy of judicial deliberations;

(d) rules on criminal procedure.

4. This Directive shall not affect national rules on the exercise by workers of their rights to consult their representatives or trade unions, and on protection against any unjustified detrimental measure prompted by such consultations as well as on the autonomy of the social partners and their right to enter into collective agreements. This is without prejudice to the level of protection granted by this Directive.

Article 4
Personal scope

1. This Directive shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context including, at least, the following:

    (a) persons having the status of worker, within the meaning of Article 45(1) TFEU, including civil servants;

    (b) persons having self-employed status, within the meaning of Article 49 TFEU;

    (c) shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees;

    (d) any persons working under the supervision and direction of contractors, subcontractors and suppliers.

2. This Directive shall also apply to reporting persons where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended.

3. This Directive shall also apply to reporting persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

4. The measures for the protection of reporting persons set out in Chapter VI shall also apply, where relevant, to:

    (a) facilitators;

    (b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and

    (c) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

Article 5
Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'breaches' means acts or omissions that:

(i) are unlawful and relate to the Union acts and areas falling within the material scope referred to in Article 2; or

(ii) defeat the object or the purpose of the rules in the Union acts and areas falling within the material scope referred to in Article 2;

(2) 'information on breaches' means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches;

(3) 'report' or 'to report' means, the oral or written communication of information on breaches;

(4) 'internal reporting' means the oral or written communication of information on breaches within a legal entity in the private or public sector;

(5) 'external reporting' means the oral or written communication of information on breaches to the competent authorities;

(6) 'public disclosure' or 'to publicly disclose' means the making of information on breaches available in the public domain;

(7) 'reporting person' means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities;

(8) 'facilitator' means a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential;

(9) 'work-related context' means current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;

(10) ‘person concerned’ means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated;

(11) ‘retaliation’ means any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;

(12) ‘follow-up’ means any action taken by the recipient of a report or any competent authority, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure;

(13) ‘feedback’ means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up;

(14) ‘competent authority’ means any national authority designated to receive reports in accordance with Chapter III and give feedback to the reporting person, and/or designated to carry out the duties provided for in this Directive, in particular as regards follow-up.

Article 6
Conditions for protection of reporting persons

1. Reporting persons shall qualify for protection under this Directive provided that:

   (a) 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

   (b) 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.

2. Without prejudice to existing obligations to provide for anonymous reporting by virtue of Union law, this Directive does not affect the power of Member States to decide whether legal entities in the private or public sector and competent authorities are required to accept and follow up on anonymous reports of breaches.

3. Persons who reported or publicly disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation, shall nonetheless qualify for the protection provided for under Chapter VI, provided that they meet the conditions laid down in paragraph 1.

4. Persons reporting to relevant institutions, bodies, offices or agencies of the Union breaches falling within the scope of this Directive shall qualify for protection as laid down in this Directive under the same conditions as persons who report externally.

CHAPTER II
INTERNAL REPORTING AND FOLLOW-UP

Article 7
Reporting through internal reporting channels

1. As a general principle and without prejudice to Articles 10 and 15, information on breaches may be reported through the internal reporting channels and procedures provided for in this Chapter.

2. 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.

3. Appropriate information relating to the use of internal reporting channels referred to in paragraph 2 shall be provided in the context of the information given by legal entities in the private and public sector pursuant to point (g) of Article 9(1), and by competent authorities pursuant to point (a) of Article 12(4) and Article 13.

Article 8
Obligation to establish internal reporting channels

1. Member States shall ensure that legal entities in the private and public sector establish channels and procedures for internal reporting and for follow-up, following consultation and in agreement with the social partners where provided for by national law.

2. The channels and procedures referred to in paragraph 1 of this Article shall enable the entity‘s workers to report information on breaches. They may enable other persons, referred to in points (b), (c) and (d) of Article 4(1) and Article 4(2), who are in contact with the entity in the context of their work-related activities to also report information on breaches.

3. Paragraph 1 shall apply to legal entities in the private sector with 50 or more workers.

4. The threshold laid down in paragraph 3 shall not apply to the entities falling within the scope of Union acts referred to in Parts I.B and II of the Annex.

5. Reporting channels may be operated internally by a person or department designated for that purpose or provided externally by a third party. The safeguards and requirements referred to in Article 9(1) shall also apply to entrusted third parties operating the reporting channel for a legal entity in the private sector.

6. Legal entities in the private sector with 50 to 249 workers may share resources as regards the receipt of reports and any investigation to be carried out. This shall be without prejudice to the obligations imposed upon such entities by this Directive to maintain confidentiality, to give feedback, and to address the reported breach.

7. Following an appropriate risk assessment taking into account the nature of the activities of the entities and the ensuing level of risk for, in particular, the environment and public health, Member States may require legal entities in the private sector with fewer than 50 workers to establish internal reporting channels and procedures in accordance with Chapter II.

8. Member States shall notify the Commission of any decision they take to require legal entities in the private sector to establish internal reporting channels pursuant to paragraph 7. That notification shall include the reasons for the decision and the criteria used in the risk assessment referred to in paragraph 7. The Commission shall communicate that decision to the other Member States.

9. Paragraph 1 shall apply to all legal entities in the public sector, including any entity owned or controlled by such entities.

Member States may exempt from the obligation referred to in paragraph 1 municipalities with fewer than 10 000 inhabitants or fewer than 50 workers, or other entities referred to in the first subparagraph of this paragraph with fewer than 50 workers.

Member States may provide that internal reporting channels can be shared between municipalities or operated by joint municipal authorities in accordance with national law, provided that the shared internal reporting channels are distinct from and autonomous in relation to the relevant external reporting channels.

Article 9
Procedures for internal reporting and follow-up

1. The procedures for internal reporting and for follow-up as referred to in Article 8 shall include the following:

    (a) channels for receiving the reports which are designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the reporting person and any third party mentioned in the

report is protected, and prevents access thereto by non-authorised staff members;

(b) acknowledgment of receipt of the report to the reporting person within seven days of that receipt;

(c) the designation of an impartial person or department competent for following-up on the reports which may be the same person or department as the one that receives the reports and which will maintain communication with the reporting person and, where necessary, ask for further information from and provide feedback to that reporting person;

(d) diligent follow-up by the designated person or department referred to in point (c);

(e) diligent follow-up, where provided for in national law, as regards anonymous reporting;

(f) a reasonable timeframe to provide feedback, not exceeding three months from the acknowledgment of receipt or, if no acknowledgement was sent to the reporting person, three months from the expiry of the seven-day period after the report was made;

(g) provision of clear and easily accessible information regarding the procedures for reporting externally to competent authorities pursuant to Article 10 and, where relevant, to institutions, bodies, offices or agencies of the Union.

2. The channels provided for in point (a) of paragraph 1 shall enable reporting in writing or orally, or both. Oral reporting shall be possible by telephone or through other voice messaging systems, and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe.

CHAPTER III
EXTERNAL REPORTING AND FOLLOW-UP

Article 10
Reporting through external reporting channels

Without prejudice to point (b) of Article 15(1), reporting persons shall report information on breaches using the channels and procedures referred to in Articles 11 and 12, after having first reported through internal reporting channels, or by directly reporting through external reporting channels.

Article 11
Obligation to establish external reporting channels and to follow up on reports

1. Member States shall designate the authorities competent to receive, give feedback and follow up on reports, and shall provide them with adequate resources.

2. Member States shall ensure that the competent authorities:

   (a) establish independent and autonomous external reporting channels, for receiving and handling information on breaches;

   (b) promptly, and in any event within seven days of receipt of the report, acknowledge that receipt unless the reporting person explicitly requested otherwise or the competent authority reasonably believes that acknowledging receipt of the report would jeopardise the protection of the reporting person‘s identity;

   (c) diligently follow up on the reports;

   (d) provide feedback to the reporting person within a reasonable timeframe not exceeding three months, or six months in duly justified cases;

   (e) communicate to the reporting person the final outcome of investigations triggered by the report, in accordance with procedures provided for under national law;

   (f) transmit in due time the information contained in the report to competent institutions, bodies, offices or agencies of the Union, as appropriate, for further investigation, where provided for under Union or national law.

3. Member States may provide that competent authorities, after having duly assessed the matter, can decide that a reported breach is clearly minor and does not require further follow-up pursuant to this Directive, other than closure of the procedure. This shall not affect other obligations or other applicable procedures to address the reported breach, or the protection granted by this Directive in relation to internal or external reporting. In such a case, the competent authorities shall notify the reporting person of their decision and the reasons therefor.

4. Member States may provide that competent authorities can decide to close procedures regarding repetitive reports which do not contain any meaningful new information on breaches compared to a past report in respect of which the relevant procedures were concluded, unless new legal or factual circumstances justify a different follow-up. In such a case, the competent authorities shall notify the reporting person of their decision and the reasons therefor.

5. Member States may provide that, in the event of high inflows of reports, competent authorities may deal with reports of serious breaches or breaches of essential provisions falling within the scope of this Directive as a matter of priority, without prejudice to the timeframe as set out in point (d) of paragraph 2.

6. Member States shall ensure that any authority which has received a report but does not have the competence to address the breach reported transmits it to the competent authority, within a reasonable time, in a secure manner, and that the reporting person is informed, without delay, of such a transmission.

Article 12
Design of external reporting channels

1. External reporting channels shall be considered independent and autonomous, if they meet all of the following criteria:

   (a) they are designed, established and operated in a manner that ensures the completeness, integrity and confidentiality of the information and prevents access thereto by non-authorised staff members of the competent authority;

   (b) they enable the durable storage of information in accordance with Article 18 to allow further investigations to be carried out.

2. The external reporting channels shall enable reporting in writing and orally. Oral reporting shall be possible by telephone or through other voice messaging systems and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe.

3. Competent authorities shall ensure that, where a report is received through channels other than the reporting channels referred to in paragraphs 1 and 2 or by staff members other than those responsible for handling reports, the staff members who receive it are prohibited from disclosing any information that might identify the reporting person or the person concerned, and that they promptly forward the report without modification to the staff members responsible for handling reports.

4. Member States shall ensure that competent authorities designate staff members responsible for handling reports, and in particular for:

    (a) providing any interested person with information on the procedures for reporting;

    (b) receiving and following up on reports;

    (c) maintaining contact with the reporting person for the purpose of providing feedback and requesting further information where necessary.

5. The staff members referred to in paragraph 4 shall receive specific training for the purposes of handling reports.

Article 13
Information regarding the receipt of reports and their follow-up

Member States shall ensure that competent authorities publish on their websites in a separate, easily identifiable and accessible section at least the following information:

(a) the conditions for qualifying for protection under this Directive;

(b) the contact details for the external reporting channels as provided for under Article 12, in particular the electronic and postal addresses, and the phone numbers for such channels, indicating whether the phone conversations are recorded;

(c) the procedures applicable to the reporting of breaches, including the manner in which the competent authority may request the reporting person to clarify the information reported or to provide additional information, the timeframe for providing feedback and the type and content of such feedback;

(d) the confidentiality regime applicable to reports, and in particular the information in relation to the processing of personal data in accordance with Article 17 of this Directive, Articles 5 and 13 of Regulation (EU) 2016/679, Article 13 of Directive (EU) 2016/680 and Article 15 of Regulation (EU) 2018/1725, as applicable;

(e) the nature of the follow-up to be given to reports;

(f) the remedies and procedures for protection against retaliation and the availability of confidential advice for persons contemplating reporting;

(g) a statement clearly explaining the conditions under which persons reporting to the competent authority are protected from incurring liability for a breach of confidentiality pursuant to Article 21(2); and

(h) contact details of the information centre or of the single independent administrative authority as provided for in Article 20(3) where applicable.

Article 14
Review of the procedures by competent authorities

Member States shall ensure that competent authorities review their procedures for receiving reports, and their follow-up, regularly, and at least once every three years. In reviewing such procedures, competent authorities shall take account of their experience as well as that of other competent authorities and adapt their procedures accordingly.

CHAPTER IV
PUBLIC DISCLOSURES

Article 15
Public disclosures

1. A person who makes a public disclosure shall qualify for protection under this Directive if any of the following conditions is fulfilled:

   (a) the person first reported internally and externally, or directly externally in accordance with Chapters II and III, but no appropriate action was taken in response to the report within the timeframe referred to in point (f) of Article 9(1) or point (d) of Article 11(2); or

   (b) the person has 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.

2. This Article shall not apply to cases where a person directly discloses information to the press pursuant to specific national provisions establishing a system of protection relating to freedom of expression and information.

CHAPTER V
PROVISIONS APPLICABLE TO INTERNAL AND EXTERNAL REPORTING

Article 16
Duty of confidentiality

1. Member States shall ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of that person. This shall also apply to any other information from which the identity of the reporting person may be directly or indirectly deduced.

2. By way of derogation from paragraph 1, the identity of the reporting person and any other information referred to in paragraph 1 may be disclosed only where 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 with a view to safeguarding the rights of defence of the person concerned.

3. Disclosures made pursuant to the derogation provided for in paragraph 2 shall be subject to appropriate safeguards under the applicable Union and national rules. In particular, reporting persons shall be informed before their identity is disclosed, unless such information would jeopardise the related investigations or judicial proceedings. When informing the reporting persons, the competent authority shall send them an explanation in writing of the reasons for the disclosure of the confidential data concerned.

4. Member States shall ensure that competent authorities that receive information on breaches that includes trade secrets do not use or disclose those trade secrets for purposes going beyond what is necessary for proper follow-up.

Article 17
Processing of personal data

Any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Any exchange or transmission of information by Union institutions, bodies, offices or agencies shall be undertaken in accordance with Regulation (EU) 2018/1725.

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.

Article 18
Record keeping of the reports

1. Member States shall ensure that legal entities in the private and public sector and competent authorities keep records of every report received, in compliance with the confidentiality requirements provided for in Article 16. Reports shall be stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by this Directive, or other requirements imposed by Union or national law.

2. Where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the reporting person, legal entities in the private and public sector and competent authorities shall have the right to document the oral reporting in one of the following ways:

    (a) by making a recording of the conversation in a durable and retrievable form; or

    (b) through a complete and accurate transcript of the conversation prepared by the staff members responsible for handling the report.

Legal entities in the private and public sector and competent authorities shall offer the reporting person the opportunity to check, rectify and agree the transcript of the call by signing it.

3. Where an unrecorded telephone line or another unrecorded voice messaging system is used for reporting, legal entities in the private and public sector and competent authorities shall have the right to document the oral reporting in the form of accurate minutes of the conversation written by the staff member responsible for handling the report. Legal entities in the private and public sector and competent authorities shall offer the reporting person the opportunity to check, rectify and agree the minutes of the conversation by signing them.

4. Where a person requests a meeting with the staff members of legal entities in the private and public sector or of competent authorities for reporting purposes pursuant to Articles 9(2) and 12(2), legal entities in the private and public sector and competent authorities shall ensure, subject to the consent of the reporting person, that complete and accurate records of the meeting are kept in a durable and retrievable form.

Legal entities in the private and public sector and competent authorities shall have the right to document the meeting in one of the following ways:

    (a) by making a recording of the conversation in a durable and retrievable form; or

(b) through accurate minutes of the meeting prepared by the staff members responsible for handling the report.

Legal entities in the private and public sector and competent authorities shall offer the reporting person the opportunity to check, rectify and agree the minutes of the meeting by signing them.

CHAPTER VI
PROTECTION MEASURES

Article 19
Prohibition of retaliation

Member States shall take the necessary measures to prohibit any form of retaliation against persons referred to in Article 4, including threats of retaliation and attempts of retaliation including in particular in the form of:

(a) suspension, lay-off, dismissal or equivalent measures;

(b) demotion or withholding of promotion;

(c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;

(d) withholding of training;

(e) a negative performance assessment or employment reference;

(f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;

(g) coercion, intimidation, harassment or ostracism;

(h) discrimination, disadvantageous or unfair treatment;

(i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;

(j) failure to renew, or early termination of, a temporary employment contract;

(k) harm, including to the person‘s reputation, particularly in social media, or financial loss, including loss of business and loss of income;

(l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;

(m) early termination or cancellation of a contract for goods or services;

(n) cancellation of a licence or permit;

(o) psychiatric or medical referrals.

Article 20
Measures of support

1. Member States shall ensure that persons referred to in Article 4 have access, as appropriate, to support measures, in particular the following:

    (a) comprehensive and independent information and advice, which is easily accessible to the public and free of charge, on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned;

    (b) effective assistance from competent authorities before any relevant authority involved in their protection against retaliation, including, where provided for under national law, certification of the fact that they qualify for protection under this Directive; and

    (c) legal aid in criminal and in cross-border civil proceedings in accordance with Directive (EU) 2016/1919 and Directive 2008/52/EC of the European Parliament and of the Council,[6] and, in accordance with national law, legal aid in further proceedings and legal counselling or other legal assistance.

2. Member States may provide for financial assistance and support measures, including psychological support, for reporting persons in the framework of legal proceedings.

3. The support measures referred to in this Article may be provided, as appropriate, by an information centre or a single and clearly identified independent administrative authority.

[6] Expert Forum Romania, 'Draft Law on the Protection of Whistleblowers – EFOR's Comments and Position (Policy Brief No 113, April 2021) 2.

Article 21
Measures for protection against retaliation

1. Member States shall take the necessary measures to ensure that persons referred to in Article 4 are protected against retaliation. Such measures shall include, in particular, those set out in paragraphs 2 to 8 of this Article.

2. Without prejudice to Article 3(2) and (3), where persons report information on breaches or make a public disclosure in accordance with this Directive they 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 for revealing a breach pursuant to this Directive.

3. Reporting persons shall not incur liability in respect of the acquisition of or access to the information which is reported or publicly disclosed, provided that such acquisition or access did not constitute a self-standing criminal offence. In the event of the acquisition or access constituting a self-standing criminal offence, criminal liability shall continue to be governed by applicable national law.

4. Any other possible liability of reporting persons arising from acts or omissions which are unrelated to the reporting or public disclosure or which are not necessary for revealing a breach pursuant to this Directive shall continue to be governed by applicable Union or national law.

5. In proceedings before a court or other authority relating to a detriment suffered by the reporting person, and subject to that person establishing that he or she reported or made a public disclosure and suffered a detriment, it shall be presumed that the detriment was made in retaliation for the report or the public disclosure. In such cases, it shall be for the person who has taken the detrimental measure to prove that that measure was based on duly justified grounds.

6. Persons referred to in Article 4 shall have access to remedial measures against retaliation as appropriate, including interim relief pending the resolution of legal proceedings, in accordance with national law.

7. In legal proceedings, including 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, persons referred to in Article 4 shall not incur liability of any kind as a result of reports or public disclosures under this Directive. Those persons shall have the right to rely on that reporting or public disclosure to seek dismissal of the case, provided that they had reasonable grounds to believe that the reporting or public disclosure was necessary for revealing a breach, pursuant to this Directive.

Where a person reports or publicly discloses information on breaches falling within the scope of this Directive, and that information includes trade secrets, and where that person meets the conditions of this Directive, such reporting or public disclosure shall be considered lawful under the conditions of Article 3(2) of the Directive (EU) 2016/943.

8. Member States shall take the necessary measures to ensure that remedies and full compensation are provided for damage suffered by persons referred to in Article 4 in accordance with national law.

Article 22
Measures for the protection of persons concerned

1. Member States shall ensure, in accordance with the Charter, that persons concerned fully enjoy the right to an effective remedy and to a fair trial, as well as the presumption of innocence and the rights of defence, including the right to be heard and the right to access their file.

2. Competent authorities shall ensure, in accordance with national law, that the identity of persons concerned is protected for as long as investigations triggered by the report or the public disclosure are ongoing.

3. The rules set out in Articles 12, 17 and 18 as regards the protection of the identity of reporting persons shall also apply to the protection of the identity of persons concerned.

Article 23
Penalties

1. Member States shall provide for effective, proportionate and dissuasive penalties applicable to natural or legal persons that:

   (a) hinder or attempt to hinder reporting;

   (b) retaliate against persons referred to in Article 4;

   (c) bring vexatious proceedings against persons referred to in Article 4;

   (d) breach the duty of maintaining the confidentiality of the identity of reporting persons, as referred to in Article 16.

2. Member States shall provide for effective, proportionate and dissuasive penalties applicable in respect of reporting persons where it is established that they knowingly reported or publicly disclosed false information. Member States shall also provide for measures for compensating damage resulting from such reporting or public disclosures in accordance with national law.

Article 24
No waiver of rights and remedies

Member States shall ensure that the rights and remedies provided for under this Directive cannot be waived or limited by any agreement, policy, form or condition of employment, including a pre-dispute arbitration agreement.

CHAPTER VII
FINAL PROVISIONS

Article 25
More favourable treatment and non-regression clause

1. Member States may introduce or retain provisions more favourable to the rights of reporting persons than those set out in this Directive, without prejudice to Article 22 and Article 23(2).

2. The implementation of this Directive shall under no circumstances constitute grounds for a reduction in the level of protection already afforded by Member States in the areas covered by this Directive.

Article 26
Transposition and transitional period

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

2. By way of derogation from paragraph 1, as regards legal entities in the private sector with 50 to 249 workers, Member States shall by 17 December 2023 bring into force the laws, regulations and administrative provisions necessary to comply with the obligation to establish internal reporting channels under Article 8(3).

3. When Member States adopt the provisions referred to in paragraphs 1 and 2, those provisions shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made. They shall forthwith communicate to the Commission the text of those provisions.

Article 27
Reporting, evaluation and review

1. Member States shall provide the Commission with all relevant information regarding the implementation and application of this Directive. On the basis of

the information provided, the. Commission shall, by 17 December 2023, submit a report to the European Parliament and the Council on the implementation and application of this Directive.

2. Without prejudice to reporting obligations laid down in other Union legal acts, Member States shall, on an annual basis, submit the following statistics on the reports referred to in Chapter III to the Commission, preferably in an aggregated form, if they are available at a central level in the Member State concerned:

   (a) the number of reports received by the competent authorities;

   (b) the number of investigations and proceedings initiated as a result of such reports and their outcome; and

   (c) if ascertained, the estimated financial damage, and the amounts recovered following investigations and proceedings, related to the breaches reported.

3. The Commission shall, by 17 December 2025, taking into account its report submitted pursuant to paragraph 1 and the Member States‘ statistics submitted pursuant to paragraph 2, submit a report to the European Parliament and to the Council assessing the impact of national law transposing this Directive. The report shall evaluate the way in which this Directive has functioned and consider the need for additional measures, including, where appropriate, amendments with a view to extending the scope of this Directive to further Union acts or areas, in particular the improvement of the working environment to protect workers‘ health and safety and working conditions.

In addition to the evaluation referred to in the first subparagraph, the report shall evaluate how Member States made use of existing cooperation mechanisms as part of their obligations to follow up on reports regarding breaches falling within the scope of this Directive and more generally how they cooperate in cases of breaches with a cross-border dimension.

4. The Commission shall make the reports referred to in paragraphs 1 and 3 public and easily accessible.

Article 28
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 29
Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 23 October 2019.

For the European Parliament
The President
D. M. Sassoli

For the Council
The President
T. Tuppurainen

APPENDIX II: INDEPENDENT EXPERT

Kieran Pender, Canberra, Australia

Kieran Pender is an honorary lecturer at The Australian National University College of Law, a senior lawyer at the Human Rights Law Centre and a consultant to Bradley Allen Love Lawyers. Kieran was previously a senior legal advisor with the International Bar Association (IBA) Legal Policy and Research Unit in London, where he led the IBA's work on whistleblowing – coordinating *Whistleblower Protections: A Guide* (IBA, 2018) and co-authoring *Are Whistleblowing Laws Working? A Global Study of Whistleblower Protection Litigation* (IBA and Government Accountability Project, 2021). Kieran has spoken about whistleblowing at the United Nations, World Bank, European Parliament, OECD and B20, and published numerous book chapters and peer-reviewed academic articles. He is also an award-winning freelance journalist for *The Guardian.* The views expressed in this Report are those of the author alone and do not represent the views of any affiliated organisation.

APPENDIX III: RESEARCH QUESTIONS

In late 2020, the CEELI Institute requested that the Partner Organisations each provide a research document that addresses the following queries and any other issues the Partner Organisations consider material to the transposition process.

Scope

A. What subject matters are covered by the Existing Domestic Law (material scope)?

   a. Does it cover all subject matters or is the material scope confined?

   b. In initial transposition discussions, has the state indicated a desire to transpose the Directive in a limited manner (i.e., limiting material scope to areas of EU legislative competency) or a comprehensive manner?

   c. Where there is no Existing Domestic Law, are there sector-specific laws that provide limited protections for whistleblowers?

B. What individuals are protected by the Existing Domestic Law (personal scope)?

   a. Does the Existing Domestic Law only apply to government employees, only to private sector employees or to both?

   b. Does the Existing Domestic Law protect former employees, contractors, volunteers, interns and related third parties, or is it limited to employees (strictly-defined)?

   c. Where there is no Existing Domestic Law, are there employment or labour laws that provide limited protections for whistleblowers?

Conditions for Reporting

C. Does the Existing Domestic Law provide protections to an individual within the personal scope (the whistleblower) who reports through a specified channel?

   a. Are these protections conditioned on the whistleblower having had reasonable grounds to believe that the information they reported was true at the time of reporting and fell within the material scope of the law?

   b. Are these protections conditioned on the whistleblower having reported in good faith or by reference to some other standard in relation to the whistleblower's motive?

D. Does the Existing Domestic Law permit anonymous whistleblowing?

    a. Does the Existing Domestic Law provide protection to whistleblowers who report anonymously but subsequently have their identity revealed and suffer retaliation?

Internal Reporting

E. Does the Existing Domestic Law prioritise or otherwise promote reporting through proper channels within the whistleblower's employer or organisation (internal reporting)?

F. Does the Existing Domestic Law require private and/or public sector entities to establish channels and procedures for receipt and follow-up of internal reporting?

    a. What is the minimum size (if any) of private entity that this requirement extends to?

    b. Does the Existing Domestic Law specify the nature of these required procedures, including:

        i. Secure channels for receiving reports (whether in writing, orally or both) that ensure confidentiality and prevents access by unauthorised employees;

        ii. Acknowledgement of receipt within a specified period;

        iii. The designation of an impartial individual or department as a contact point for the whistleblower;

        iv. A specified period for the designated individual or department to provide feedback on the report to the whistleblower; and

        v. Provision of information about procedures for reporting to external authorities?

    c. Where there is no Existing Domestic Law, do employment or labour laws require employers to establish complaint channels and procedures?

External Reporting

G. Does the Existing Domestic Law permit the whistleblower to report to relevant state authorities, either following internal reporting or directly?

a. Does the Existing Domestic Law require the government to designate relevant state authorities as competent to receive feedback, give feedback and follow up on reports?

b. Does the Existing Domestic Law require that the designated state authorities:

    i. Acknowledge receipt of reports from whistleblowers within a specified time period;

    ii. Investigate reports; and

    iii. Provide feedback to whistleblowers within a specified time period?

c. Does the Existing Domestic Law specify that external reporting channels must be independent and autonomous, including by ensuring confidential and secure reporting systems, durable storage of information and specific training for staff about handling reports?

d. Does the Existing Domestic Law require relevant state authorities to publish information on their websites to facilitate external reporting?

e. Does the Existing Domestic Law require competent authorities to review their procedures for receiving and following up reports at least every three years?

f. Where there is no Existing Domestic Law, do other laws provide protections for a whistleblower who reports to relevant state authorities?

Public Reporting

H. Does the Existing Domestic Law provide protection for a whistleblower who reports publicly, such as to the press or via social media **(public reporting)**?

    a. Is that protection limited to:

        i. Whistleblowers who reported internally and/or externally but no appropriate action was taken within any timeframes specified within the Existing Domestic Law; and/or

        ii. The whistleblower has reasonable grounds to believe that: (a) their report discloses an imminent or manifest danger to the public interest or (b) there is a risk of retaliation and a low prospect of the disclosure being effectively addressed due to the particular circumstances of the case, such as collusion or the potential for evidence to be destroyed?

Confidentiality and Record-Keeping

I. Does the Existing Domestic Law provide confidentiality in relation to the identity of a whistleblower, with disclosure limited only to authorised staff members competent to receive or follow up reports and appropriate national and judicial authorities?

J. Does the Existing Domestic Law provide conditions and limitations in relation to the handling, retention and destruction of records and information in relation to a whistleblower's report?

K. Where there is no Existing Domestic Law, do employment or labour laws provide any obligations on employers in relation to confidentiality and record-keeping following employee complaints?

Retaliation

L. Does the Existing Domestic Law prohibit retaliation against a whistleblower? Where there is no Existing Domestic Law, do other domestic laws provide comparable protection against unfair workplace treatment?

M. If the Existing Domestic Law does prohibit retaliation, is the prohibition limited to certain extreme forms of retaliation (termination of employment, demotion, etc.) or is it wide-ranging (encompassing, for example, discrimination, reputational damage, industry-wide blacklisting, improper medical referrals, etc.)?

N. Does the Existing Domestic Law (or regulatory and administrative initiatives) provide support measures to a whistleblower? These might include:

   a. Comprehensive, independent, accessible and free information and advice about the rights of whistleblowers;

   b. Effective assistance from relevant national authorities in pursuing retaliation claims; and

   c. Legal aid.

O. Does the Existing Domestic Law (or distinct regulatory and administrative initiatives) provide financial or psychological support for a whistleblower?

P. Does the Existing Domestic Law confer on a whistleblower immunity from civil (including defamation, breach of copyright, breach of secrecy, breach of data protection, disclosure of trade secrets, etc.) and/or criminal liability in relation to their internal, external or public reporting?

a. Does the Existing Domestic Law retain liability where a whistleblower's access of the reported information was contrary to criminal law?

Burden and Remedies

Q. Does the Existing Domestic Law provide, in proceedings relating to retaliation against a whistleblower, for a reversed burden of proof (or similar), whereby it is presumed that the detrimental act was done in retaliation for the whistleblower's report and the retaliator is required to prove otherwise?

a. If not, or where there is no Existing Domestic Law, does any comparable area of law (such as employment law) provide a similar mechanism?

R. What remedies does the Existing Domestic Law provide for a whistleblower who succeeds in retaliation proceedings?

a. Can a relevant judicial authority, either pursuant to the Existing Domestic Law or its inherent power, order interim relief pending the resolution of retaliation proceedings?

Rights of Persons Concerned

S. Does the Existing Domestic Law (or other law) ensure that 'persons concerned' (such as those accused by a whistleblower of a breach of the law) retain the right to a fair trial, the presumption of innocence, procedural fairness and other such legal norms?

a. Does the Existing Domestic Law (or other law) provide for confidentiality in relation to the identity of persons concerned for the duration of any investigations?

Penalties

T. Does the Existing Domestic Law provide for penalties against individuals or organisations that: (i) obstruct whistleblowing, (ii) retaliate against a whistleblower, (iii) bring vexatious proceedings against a whistleblower, or (iv) breach confidentiality owed to a whistleblower? Does the Existing Domestic Law provide for penalties against whistleblowers who knowingly report false information?

a. In both circumstances, are the penalties proportionate and dissuasive?

Waiver

U. Does the Existing Domestic Law (or other law) permit whistleblowers to waive their rights as a condition of employment, such as pursuant to a pre-dispute arbitration agreement?

Non-Regression and More Favourable Treatment

V. Does the Existing Domestic Law provide any protections to whistleblowers not already outlined above?

W. Where there is no Existing Domestic Law, are there any protections available to whistleblowers under other laws that are more favourable than those outlined above?

Review

X. Does the Existing Domestic Law provide an evaluation or review process?

   a. Does the Existing Domestic Law require the collection and publication of data, including:

      i. The number of reports made to relevant authorities;

      ii. The number of investigations and proceedings initiated as a result; and

      iii. The estimated financial damage and amounts recovered as a result?

Funding provided
by the United States
Government

CEELI Institute
Villa Grébovka
Havlíčkovy Sady 58
120 00 Prague
Czech Republic

www.ceeliinstitute.org
office@ceeli.eu