

EU Whistleblowing Monitor

TEMPLATE FOR SUMMARY GUIDE ON TRANSPOSITION LEGISLATION FOR EU WHISTLEBLOWING MONITOR (DIRECTIVE 2019/1937)

Understanding Hungary's Whistleblower Protection Law: A Simplified Guide

The template below has been developed by the Transparency International Chapter beneficiaries of the Safe4WBs and country editors of the [EU Whistleblowing Monitor](#) to produce a concise summary guide on their respective national whistleblowing laws adopted to transpose the EU Directive on Whistleblowing into their national legal systems. This is meant to capture basic information to assist the general public with understanding the law and basic information on reporting. Once finalised with each Chapter, these briefings will be published on the enhanced national country pages being piloted on the Monitor, funded by [the SAFE for Whistleblowers](#) project.

What is whistleblowing?

Whistleblowing draws attention to circumstances whose remedy or elimination serves the interests of the community or society as a whole. A whistleblowing report may also contain a proposal according to the Act XXV of 2023 on Complaints, Disclosures in the Public Interest, and Related Rules on Reporting Abuses (hereinafter: the Act).

Hungary's pre-existing law on public-interest disclosures was introduced by Act CLXIII of 2013, while the act to transpose the EU Whistleblowing Directive (2019/1937) was adopted in Hungary after significant delay. The Act creates two parallel systems by preserving the national regime, which serves to cover whistleblowers who report on breaches of Hungarian law, and introducing a simultaneous EU-regime that implements the Directive and only covers whistleblowers who report breaches of EU law. This confusing solution has a dissuasive effect, and it deters Hungarians from reporting on wrongdoing.

Key features of the whistleblower protection law

Who Can Report Wrongdoing (and Benefit from Protection)? The Act covers a wide range of persons who can make reports through internal whistleblowing systems. This includes: current employees (under any type of employment relationship); former employees whose employment has ended; candidates for employment whose application process has begun; self-employed individuals and sole traders in a contractual relationship with the employer; shareholders and members of governing, management, or supervisory bodies (including non-executive members); persons working under the direction of contractors, subcontractors, or suppliers; interns and volunteers; and persons whose employment or contractual relationship has already ended. Protection applies provided that the whistleblower had reasonable grounds to believe the information reported was true at the time of reporting.

What Types of Wrongdoing That Can Be Reported? Any information concerning unlawful or suspected unlawful acts or omissions, or other abuses, can be reported through internal systems. For the purposes of the whistleblower protection provisions of the Act, the reported conduct must relate to EU legal acts listed in Appendix 1 of the Act (or national rules



Co-funded by
the European Union



implementing those acts). These areas include: public procurement; financial services and markets; anti-money laundering and terrorist financing; product safety; transport safety; environmental protection; nuclear safety; food chain safety; data protection and cybersecurity; and public health. Employers may additionally designate further internal conduct rules whose breach can also be reported (e.g. expense policy violations, conflicts of interest). The Act chose to create a parallel regime for reports of breaches of EU law in the areas of the Directive, while other reports outside the Directive's scope are still governed by provisions originating from the pre-existing 2013 law, which proved insufficient both in terms of protection of reporting persons and investigation of reports. As mentioned above, this results in the fragmentation of the protection regime and leaves many potential whistleblowers with no or just very feeble protection.

What are the Conditions to Benefit from Protection? To benefit from protection under the Act, the following conditions must be met: (1) the report must be made through one of the prescribed reporting channels (internal or external); (2) the information must have been obtained in the course of the reporting person's work-related activities; and (3) the reporting person must have had reasonable grounds to believe the information was accurate at the time of reporting. As one of the requirements of lawfulness is good faith ('bona fide'), even though this term is not specifically used in the Act, reporting persons without a grounded reason to believe that the information they reported was true at the moment of the report are deprived of protection. A serious shortcoming of the Act relates to public disclosures: contrary to the Directive, disclosures published through the media are not protected. Intentionally false reports are not protected either, and the Act explicitly allows employers to establish proportionate and dissuasive sanctions for deliberate false reporting.

Who Else is Protected? The Act extends protection to persons beyond the primary reporter. A whistleblower who is considered "at risk"— meaning it is likely that the retaliation they face could seriously jeopardise their living conditions — is entitled to enhanced state legal aid. The Act does not explicitly enumerate protection for facilitators, family members, or civil society organisations in the same manner as some other Member States' implementations; civil society groups have flagged this as a limitation of the Hungarian transposition.

Where and How to Report

Reporting Internally:

- All private sector employers with at least 50 employees are required to establish an internal whistleblowing system. Additionally, regardless of employee count, certain employers must always establish a system, including: those subject to anti-money laundering rules (e.g. credit institutions, law firms, auditors, real estate agents); employers registered in Hungary operating offshore oil and gas activities outside the EU; those covered by the EU Civil Aviation Safety Reporting Regulation; and operators of vessels in Hungarian territory. Employers with 50–249 employees may combine resources to set up a joint reporting channel. State bodies and municipalities with more than 10 thousand inhabitants are also required to establish reporting channels (the



Co-funded by
the European Union



NGOs FOR WHISTLEBLOWING



deadline in their case elapsed in 2025). Employers with fewer than 50 employees and municipalities with fewer than 10 thousand inhabitants may voluntarily establish a system.

- Internal systems must be operated by an impartial designated person or department or can be outsourced to a whistleblower protection attorney or to any other external organisation. Reports may be made in writing or orally (by phone, recorded voice system, or in person). For written reports, the operator must send an acknowledgement within 7 days of receipt, including general information on procedural and data protection rules. Investigations must be completed within 30 days (extendable in justified cases to a maximum of 3 months, with the whistleblower informed of the reasons). The reporter must be informed in writing of the investigation outcome, measures taken, or reasons for non-investigation. The operator must also provide clear, accessible information about how the system works.

Reporting Externally:

- External reports can be made to the designated competent authorities. Unlike the internal whistleblowing system, which is designed to receive reports relating to conduct or events falling in the scope of the operator's interest and made by persons who work for the operator, e.g., employees, suppliers, etc., the external reporting system is available to everyone.
- The following 21 state authorities, defined in Section 32 of the Act and in Government Decree 225/2023, must establish and operate an external reporting channel:
 1. Directorate-General for Auditing European Funds,
 2. Competition Authority,
 3. Integrity Authority,
 4. Public Procurement Authority,
 5. Hungarian Energy and Public Utility Regulatory Authority,
 6. Hungarian National Bank,
 7. National Data Protection and Freedom of Information Authority,
 8. National Media and Communications Authority,
 9. National Atomic Energy Authority,
 10. Regulated Activities Supervisory Authority,
 11. Budapest Capital Government Office,
 12. Central body of the state administration for health,
 13. National Food Chain Safety Authority,
 14. central body of the state administration for pharmaceuticals,
 15. National Waste Management Authority,
 16. Hungarian State Treasury,
 17. The National Environmental Protection Authority,
 18. The minister responsible for transport,
 19. National Tax and Customs Administration,
 20. National Police Headquarters,
 21. The national nature conservation authority.



Co-funded by
the European Union



- The Act establishes a protected electronic system operated by the Commissioner for Fundamental Rights (Ombuds), through which reports to public authorities can be made securely. Reports received through this system are forwarded to the competent authority, and a summary (without personal data) is published online so the public can track progress.
- Whistleblowers may go directly to external authorities without first using internal channels. When using the Ombuds' electronic system, the reporting persons may request that their personal data remain accessible only to the office of the Ombuds; in that case, the Ombuds will anonymise the report before forwarding it to the competent authority. Reports that cannot be attributed to an identifiable person may be disregarded, except where the underlying issue is a serious violation of rights.

What Will Happen with the Report?

- After a report is received, the operator must acknowledge receipt within 7 days (for written reports) and investigate within 30 days (up to 3 months maximum). During the investigation, the operator may request clarifications or additional information from the reporter. The person implicated by the report must be informed of the report at the start of the investigation, informed of their data rights, and given the opportunity to state their position (including through legal representation). If the investigation reveals grounds for criminal proceedings, the operator must file a complaint with the authorities. After the investigation, the whistleblower must be informed in writing of the findings and measures taken or planned. Records related to the report must be retained for 5 years after the last investigative action.

Making a Public Disclosure:

- The Act does not contain detailed stand-alone provisions for public disclosures equivalent to those in the EU Directive. Public disclosures may be protected if prior internal or external reporting was not acted upon, if there was no competent authority to report to, or if the whistleblower had reasonable grounds to believe the matter posed an imminent or manifest danger to the public interest.
- The Act's provision excludes protection of whistleblowers who disclose their reports to the media. Therefore, the only protection available to whistleblowers talking to the press is the protection of sources under the Press Act, which is only guaranteed if invoked by the journalist. We can thus conclude that the Act intentionally fails to properly transpose provisions relating to public disclosure of whistleblower reports to the press, which clearly infringes upon Article 15(2) of the Directive. Transparency International Hungary, in a complaint jointly submitted with anti-corruption watchdog K-Monitor to the European Commission, asked the EU's executive to initiate an infringement procedure against the Hungarian government.

Measures to Protect Whistleblowers

Protection of the Whistleblower's Identity



Co-funded by
the European Union



- The internal system must be designed so that the personal data of the reporter (and the person named in the report) is accessible only to authorised persons. Personal data may only be shared with the authority competent to handle the case or transferred if the whistleblower consents. Data may not be made public without the whistleblower's consent. When using the Ombuds' protected external electronic system, reporters can request that their identity be shared only with the Ombuds' office. If a whistleblower protection attorney handles the report, they must forward it to the employer in an anonymised form, unless the whistleblower explicitly waives confidentiality in writing.
- Anonymous reporting is permitted but not guaranteed full protection. An employer may choose not to investigate a report if the reporter cannot be identified. However, when a report is made via the Ombuds' protected electronic system with a confidentiality request, the competent authority cannot disregard the report solely on the grounds that the reporter is unidentifiable — the Ombuds' office handles communication to maintain the reporter's anonymity. Reporters who identify themselves benefit from stronger protection guarantees.

Prohibition of Retaliation

- Any adverse measure taken against a whistleblower as a direct result of their lawful report is unlawful, even if that measure would otherwise be legally permissible. Prohibited forms of retaliation include (but are not limited to): suspension or dismissal; demotion or denial of promotion; salary reduction; denial of training; negative performance evaluation; disciplinary action; blacklisting; early termination of contracts; and any other act or omission that causes detriment to the reporter. This protection applies equally to persons who assisted the reporter or are associated with them, to the extent covered by the Act.
- The Act does not explicitly provide for interim or injunctive relief. Whistleblowers who suffer retaliation may seek remedies through standard civil litigation or labour court proceedings. There is no dedicated interim protection mechanism (such as reinstatement pending proceedings) specified in the Act, which civil society groups consider a weakness compared to the full scope of the Directive.
- In practice, this means that the person who suffers unlawful retaliation because of a report must seek justice on his or her own, with no specific or specialised legal aid or assistance within reach. Even though the reverse burden of proof is helpful, reporting persons may still find themselves abandoned in cases of retaliation.

Protection Against Lawsuits

- A whistleblower who lawfully makes a report is not considered to have breached any obligation of confidentiality or secrecy (except in relation to classified information), and is not liable for obtaining or accessing the information reported, provided they had reasonable grounds to believe it was necessary for the purpose of the report. Whistleblowers are therefore shielded from civil and criminal liability for the act of reporting itself — but this protection does not extend to conduct that is independently criminal.

- The Act does not offer protection, for instance, to whistleblowers who breach the secrecy of classified information or infringe upon judicial secrecy or other professional secrecy or the confidentiality of criminal procedures, and to those whistleblowers who violate rules governing the work of law enforcement. Although this approach corresponds to Article 3(3) of the Directive, it entirely neglects areas of outstanding importance and discourages potential whistleblowers who work in justice or law-enforcement

If a Whistleblower Suffers Retaliation or Identity Disclosure

- Whistleblowers who suffer retaliation may seek redress through civil court or labour court proceedings. In theory, the state provides legal aid to whistleblowers in need under the Legal Aid Act (Act LXXX of 2003). However, persons are entitled to financial assistance only on condition that they meet the requirements outlined in Council Directive 2003/8/EC (access to justice in cross-border disputes by establishing minimum common rules relating to legal aid for such disputes) and Council Directive 2012/29/EU (minimum standards on the rights, support and protection of victims of crime). In practical terms, this means that whistleblowers with a monthly income exceeding approx EUR 100 are not eligible for any financial assistance or compensation.
- Taking adverse action against a whistleblower, or obstructing or attempting to obstruct a report, constitutes an administrative offence (misdemeanour) under Hungarian law (Act II of 2012 on Administrative Offences), punishable by a fine of maximum EUR 500.
- In Hungary, there is no single authority responsible for whistleblower protection or for managing and examining whistleblower reports, nor is any government agency entrusted with the necessary powers to oversee the Whistleblower Protection Act or the way it is put into practice. Although certain oversight duties are accorded to the Office of the Commissioner for Fundamental Rights ('Ombuds') and the Employment Inspection and Occupational Safety Departments of the county (metropolitan) government offices, in lack of the power to impose sanctions on those who fail to properly enforce the regulation, malpractice stays unassessed and often even unrecognised. The National Authority for Data Protection and Freedom of Information (NAIH) handles data protection breaches.

Key considerations: Key considerations for whistleblowers in Hungary include: (1) Keep contemporaneous records of all relevant events, communications, and your reporting actions — these may be essential if you face retaliation and need to seek redress. (2) Whistleblowers must take action themselves if, despite the legal prohibition, they suffer adverse treatment because they made a report. For example, they must go to court because they were dismissed from their job. (3) Litigation can be costly and lengthy; legal aid is available but subject to conditions. (4) Using identified (rather than anonymous) channels generally provides stronger protection.

Other key legislation: Other relevant legislation includes: Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (AML Act) — which imposes specific whistleblowing obligations on financial sector entities; Act LXXX of 2003 on Legal Aid — which

governs state support for whistleblowers; Act CXII of 2011 on Informational Self-Determination and Freedom of Information (the “Privacy Act”) — governing data protection; and the Hungarian Criminal Code (Act C of 2012) — which may apply in relation to AML reporting failures or other criminal conduct. Hungary does not yet have a general anti-SLAPP law, which means whistleblowers can face strategic lawsuits intended to intimidate them.

Cautions for whistleblowers Important cautions: Do not conduct your own investigation into suspected wrongdoing — gather and preserve evidence of what you have observed, but do not hack systems, access restricted information beyond what you have legitimately seen, or take physical documents unlawfully. Do not share sensitive or confidential information beyond what is necessary for your report. Keep detailed contemporaneous notes with dates and times. Be aware that deliberately false reports are not protected and may result in sanctions. Given the absence of anti-SLAPP measures in Hungary, whistleblowers facing harassment lawsuits should seek legal counsel promptly. The Act is considered a minimum transposition; not all protections provided by the EU Directive may be fully enforceable in practice.

Where to Seek Information, Support & Advice (to include:)

- Official Information on the Law: The full text of Act XXV of 2023 is available (in Hungarian) on the National Legal Database: <https://njt.hu/jogszabaly/2023-25-00-00>
- The Ombuds’ protected electronic reporting system is accessible via the Commissioner for Fundamental Rights’ official website: <https://www.ajbh.hu>
- National Authority for Data Protection and Freedom of Information (NAIH) — for data protection complaints (www.naih.hu).
- (Trusted) CSOs: Transparency International Hungary (TI Hungary) — works on anti-corruption and whistleblower protection advocacy (www.transparency.hu). K-Monitor — a public funds watchdog organisation that tracks corruption cases and supports reporters (www.k-monitor.hu). TASZ (Hungarian Civil Liberties Union) — provides legal support and advocacy on civil rights, including whistleblower cases (www.tasz.hu). Átlátszó — investigative journalism platform covering corruption and public interest matters (english.atlatszo.hu).
- The Hungarian Bar Association can assist in finding a whistleblower protection attorney www.magyarugyvedikamara.hu

Further Reading & Helpful Resources

Full text of Act XXV of 2023 (Hungarian): <https://njt.hu/jogszabaly/2023-25-00-00>

Ombudsman’s protected electronic system: <https://www.ajbh.hu>

TI Hungary — Guidelines on Whistleblowers’ Protection (Hungarian):

<https://transparency.hu/tegy-a-korrupcio-ellen/bejelentovedelmi-utmutato/>

TI Hungary and K-Monitor — Analysis on the transposition of the Whistleblowing directive (Hungarian): <https://transparency.hu/hirek/uj-bejelentovedelmi-torvenyjavaslat-a-kormany-alulrol-surolja-a-minimumot/>



TI Hungary and K-Monitor — Letter to the European Commission: https://transparency.hu/wp-content/uploads/2024/01/K-Monitor_Transparency-Int-HU_letter_to_COM_on_transposition_of_whistleblower_directive_21122023.pdf

European Commission Whistleblowing Directive overview: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/whistle-blowers-protection_en

SAFE for Whistleblowers project: <https://www.transparency.org/en/projects/enabling-environment-safe-for-whistleblowers-european-union>



Co-funded by
the European Union

