CONSULTATION RESPONSE

Evaluation of Directive (EU) 2019/1937

on the Protection of Persons who Report Breaches of Union Law

Document Reference: Ares 2025/6765097

The European Pirate Party is a pan European political party representing Pirate Parties across EU Member States. Our movement is rooted in the defence of digital rights, civil liberties, and democratic participation. We advocate for civil rights, transparency, and the protection of fundamental freedoms in the digital age, and we view the internet and digital infrastructure as common goods and public utilities that must serve all citizens. We welcome the review of Directive (EU) 2019/1937 and recognise its importance in protecting individuals who report wrongdoing in the public interest.

Our position on the evaluation of the Whistle blower Protection Directive follows directly from the core principles shared by the Pirate movement across Europe. Our manifesto commits us to the highest standards of civil rights, individual privacy, and transparency of public institutions.

We believe that:

- Whistle-blowers should be protected by law and not subject to legal action.
- The privacy of the individual should be valued at all times and protected from exploitation by public and economic actors.
- Power resides with the people. Their rights and their dignity stand above all else.
- Transparency and accountability for public institutions are essential to good data protection regulation to the protection of privacy.

Why We Are Responding

The Whistleblower Protection Directive (Directive (EU) 2019/1937) was adopted in October 2019 in the wake of major scandals including Lux Leaks, Cambridge Analytica, the Panama and Paradise Papers, that demonstrated how systemic abuse remains hidden unless individuals inside organisations are willing to report it[1]. The Directive set minimum standards to protect those who do however, the Commission's July 2024 transposition report confirmed that while all Member States have now transposed the Directive, shortcomings have been identified in several areas relevant to its effectiveness, including material scope, conditions for protection, and measures against retaliation.[2]

We are responding because the shortcomings in the current framework matter most in the areas where our manifesto commitments are most at stake. Whistle blowers who expose surveillance infrastructure, AI system harms, platform manipulation, or data protection violations face the most complex and cross border retaliation risks, yet the current framework is least equipped to protect them. Effective protection is essential not only for individual reporters but also for democratic accountability in the digital age.

We are also responding because the Article 27(3) evaluation is an opportunity the Commission has explicitly identified as the vehicle for assessing whether the Directive's scope should be extended to further areas[3]. We intend to use this opportunity to argue for the extensions that our manifesto values require.

Opportunities and Risks

The Directive represents genuine and important progress. A common minimum standard of whistle-blower protection across all EU Member States, covering areas from public procurement to data protection, is a foundation worth building on. The evaluation process now underway is an opportunity to strengthen that foundation before its gaps become entrenched.

[1] European Commission, 2019
[2] (COM (2024) 269)
[3] (COM (2024) 269)

The European Commission's report[4], which assesses the transposition and application of the Directive across Member States, identifies several challenges in the current framework. These include inconsistencies in national implementation, uncertainty regarding the material scope, and differences in the level of protection available.

In particular, the report suggests that the current scope may not fully reflect certain developments in the digital economy, which can create uncertainty for individuals considering whether to report wrongdoing. This may discourage reporting in some cases, while available evidence suggests that awareness of the Directive's protections remains limited, particularly among informal and platform workers who are most vulnerable to retaliation.

Under Article 11 of the Charter of Fundamental Rights of the European Union, freedom of expression, which whistle-blowing directly enables, must be actively protected, not merely nominally guaranteed. The evaluation is an opportunity to close the gap between what the Directive promises and what it delivers. The sections below set out where revision is needed and what we are asking for.

1. Retaliation Protection and Fundamental Rights

The Directive has established the legal architecture for whistle-blower protection. Articles 19 and 21 prohibit retaliation and require measures of protection including a reversal of the burden of proof, whereby it falls to the employer to demonstrate that any adverse measure taken against a reporting person was not triggered by their report[5].

Also, Article 23 requires Member States to establish effective, proportionate, and dissuasive penalties for those who retaliate. However, in practice, these penalties may not always be sufficiently dissuasive or consistently applied, which can reduce their effectiveness. The Commission's 2024 transposition report indicates that this architecture has not been fully realised in practice[6]. The gaps between what the Directive requires and what Member States have implemented are precisely where the people it is meant to protect, are most vulnerable.

[4] COM (2024) 269
[5] (Directive (EU) 2019/1937, Articles 19–21
[6] (COM (2024) 269).

1.1 Anti-Retaliation Measures in Practice

COM (2024) 269 found deficiencies across Member States in the transposition of retaliation protection measures, specifically identifying that penalties under Article 23 are in some cases, too low to act as a genuine deterrent, and that unclear conditions for receiving protection under Article 21 create legal uncertainty that discourages reporting. The practical consequence is that the system deters the people it is meant to protect.

Legal procedures are slow and costly and where employers know that penalties for retaliation are low and that proceedings will take years, the rational calculation for a potential whistle-blower is silence. Mandatory minimum standards for penalties, and procedural mechanisms such as interim reinstatement pending the outcome of legal proceedings, are necessary to change this calculation.

1.2 The Fundamental Rights Dimension

National courts often treat whistle blower cases as ordinary employment disputes rather than as matters involving fundamental rights. This distinction is important because it changes the legal standard that applies. A fundamental rights approach requires a more rigorous proportionality analysis and a stronger justification for any harmful measures taken against the reporting person.

Retaliation against whistle blowers constitutes a direct restriction of freedom of expression protected under Article 11 of the Charter of Fundamental Rights of the European Union. When courts fail to apply this framing, they also fail to give effect to Article 47 of the Charter, which guarantees the right to an effective remedy. The Directive's own preamble links whistleblowing to freedom of expression and the public interest, yet the 2024 report indicates that this fundamental rights perspective has not been applied consistently. As a result, it remains more aspirational than enforceable and should be strengthened in practice.

1.3 Whistle-Blowers Reporting GDPR Breaches

Data protection violations fall within the material scope of the Directive. However, when a whistle blower reports a GDPR breach, the link between the Directive's protection framework and the data protection authority's investigation process is not clearly defined. Article 10 of the Directive requires competent authorities to give information and support to reporting persons, yet this duty is not applied consistently in data protection cases. In practice, authorities often

focus on investigating the breach and do not give equal attention to protecting the person who reported it[7]. This creates a structural imbalance between enforcement obligations under Regulation (EU) 2016/679 (GDPR) and the protective framework established by Directive (EU) 2019/1937, which should be addressed through clearer procedural coordination. The coordination between data protection authorities and whistle blower protection authorities needs to be clarified so that people who report GDPR violations are not left without protection

1.4 Cross-Border Retaliation

Many digital whistle blowers report wrongdoing by multinational platforms or state actors. The Directive requires cooperation between Member States, but the 2024 report found that this cooperation is still limited and not always effective[8]. A whistle blower in one Member State who faces retaliation from an organisation based in another may lack a clear or effective remedy in practice. This gap is especially serious in the digital sector, where platforms operate across borders by design and retaliation can occur in several jurisdictions at the same time.

In light of these concerns, we call on the Commission to:

- Introduce mandatory minimum standards for penalties under Article 23 that are clearly dissuasive, with the Commission empowered to assess their adequacy as part of future monitoring.
- Require Member States to ensure that interim protection measures, including provisional reinstatement pending the outcome of legal proceedings, are available to reporting persons who demonstrate a prima facie link between their report and the adverse measure taken.
- Issue binding guidance requiring national courts to apply a fundamental rights framework under Articles 11 and 47 of the Charter when adjudicating whistle-blower retaliation cases, rather than treating them as ordinary employment disputes.

[7] (Directive (EU) 2019/1937, Article 10 ; COM(2024) 269)
[8] (COM (2024) 269)

- Clarify the coordination obligations between data protection authorities and whistle-blower competent authorities in cases involving GDPR breach reports, including explicit obligations under Article 10 to support reporters throughout the investigative process.
- Strengthen the cross-border cooperation mechanisms under Article 24 to include enforceable timelines, designated contact points, and clear jurisdiction rules where retaliation originates in a different Member State from the report.

2. Scope Extension to Digital and Tech Sectors

The Directive's material scope, defined by Article 2 and the Annex, covers specific areas of EU law. The Commission's own 2024 report confirmed that several Member States have "*restrictively transposed the definition of breaches*" under Article 5(1), in particular by omitting breaches that defeat the object or purpose of the rules in covered areas[9]. If the scope is already problematic for areas the Directive nominally covers, the gap is potentially wider for digital harms it does not explicitly address.

2.1 AI Systems, Surveillance, and Algorithmic Harm

The Directive does not cover harms that arise from AI systems, algorithmic decision making, biometric surveillance, or mass scanning proposals. An insider who knows that an AI system is producing discriminatory outcomes, a government agency deploying surveillance tools that undermine data protection principles, or a platform using content moderation algorithms to suppress lawful speech has no clear path to protected reporting under the current framework.

From the main application date of the AI Act in August 2026, violations of that Regulation will fall within the Directive's scope through Article 87 of Regulation (EU) 2024/1689. This is a meaningful step, but it does not close the gap. The AI Act has a limited scope that applies only to systems and operators covered by its definitions. Broader AI harms, including harms from systems that fall below the Act's risk thresholds or from data practices that are technically compliant with the Act but undermine fundamental rights, will remain outside the Directive

[9] (COM (2024) 269).

unless its scope is extended. The evaluation must look beyond the AI Act to ensure that the Directive covers the full range of digital harms that whistle blowers are uniquely placed to report.

2.2 The Public Interest Threshold

The Directive protects reports on breaches that are unlawful or that "*defeat the object or the purpose*" of the rules in covered areas[10]. This threshold ties protection to legality rather than to public interest harm. An insider who reports that a government agency is deploying mass data collection infrastructure that complies with its legal basis but defeats the purpose of data protection principles faces an uncertain path. National implementations have applied this threshold in inconsistent ways, as confirmed in COM (2024) 269. For digital infrastructure harms, where the line between lawful and harmful is often disputed, a wider reading is needed that clearly covers conduct that is technically lawful but contrary to fundamental rights.

2.3 Platforms, the DSA, and Copyright Enforcement

The Digital Markets Act (Regulation (EU) 2022/1925) has been added to the Directive's Annex since its adoption, meaning insiders reporting certain platform abuses under the DMA are now protected. The Digital Services Act (Regulation (EU) 2022/2065), however, has not yet been added to the Annex. As a result, the Directive does not explicitly guarantee protection for disclosures relating to obligations arising under that Regulation. Workers and insiders at major platforms who report on content moderation abuses, illegal content handling failures, or advertising targeting harms under the DSA have no explicit protection. Thus, the DSA should be added to the Annex without delay.

Copyright and intellectual property law remain outside the Directive's material scope entirely. Insiders who report on abusive copyright enforcement, anti-competitive licensing practices, or automated takedown systems that suppress lawful expression have no path to protected reporting. Our manifesto commits us to a fair and balanced copyright system that serves society as a whole. The Directive should be extended to cover reporting on abusive copyright enforcement practices.

2.4 Interaction with NIS2 Maximum Harmonisation

The Commission's January 2026 proposal to amend NIS2 (COM (2026) 13) introduces maximum harmonisation for cybersecurity implementing acts under Article 21(5). This creates a tension

[10] (Directive (EU) 2019/1937, Article 5(1))

with whistle-blower protection because, if the Commission adopts implementing acts defining reporting formats and significance thresholds for cybersecurity incidents, Member States could face constraints in maintaining additional whistle-blower-specific digital reporting protections, depending on the interpretation of those implementing acts. The Directive's material scope should explicitly cover NIS2 obligations, including deliberate concealment of cybersecurity incidents, and the interaction between NIS2's maximum harmonisation provisions and the Directive's protections should be clarified.

In light of these concerns, we call on the Commission to:

- Amend Article 2 to explicitly cover AI system harms, algorithmic decision-making, and large-scale biometric surveillance, beyond what is covered by the AI Act's own scope from August 2026.
- Add Regulation (EU) 2022/2065 (the Digital Services Act) to the Directive's Annex to ensure insiders reporting platform manipulation, content moderation abuses, and advertising targeting harms receive explicit protection.
- Extend the Directive's material scope to cover abusive copyright enforcement and anti-competitive intellectual property practices.
- Broaden the public interest threshold under Article 5(1) to explicitly cover digital infrastructure harms, mass data collection, and surveillance, including where the reported conduct is technically lawful but defeats the purpose of fundamental rights protections.
- Clarify the interaction between NIS2's maximum harmonisation provisions and the Directive's protections, ensuring that implementing acts do not prevent Member States from maintaining whistle-blower-specific channels for cybersecurity disclosures.

3. Transparency, Awareness, and Citizen Participation

Our manifesto commits us to transparency and accountability for public institutions as the counterpart of good data protection, and to democratic participation as a fundamental right. The Directive's effectiveness depends not only on the strength of its legal protections but on whether ordinary citizens and workers can access those protections in practice. The evidence from the 2024 transposition report and the evaluation consultation suggests a significant gap between legal provision and practical reality.

3.1 Internal Reporting Channels: Accessibility and Transparency

Article 8 of the Directive requires private sector organisations with 50 or more employees and all public sector entities to establish internal reporting channels[11]. The existence of a channel is not the same as its accessibility. COM (2024) 269 found deficiencies in follow-up procedures, unclear timelines for acknowledging reports, and gaps in procedural guidance in several Member States. Workers in junior positions, gig workers, and contractors, those most vulnerable to retaliation — are often the least aware that these channels exist and the least equipped to use them without fear.

There is also a transparency gap at the institutional level. Competent authorities that receive external reports are not required to publish information about the volume, nature, or outcome of the reports they receive. Without this transparency, it is impossible for civil society or citizens to assess whether the system is working, to identify systemic patterns in the types of wrongdoing being reported, or to hold authorities accountable for their follow-up obligations under Article 11 of the Directive.[12]

3.2 Awareness, Underreporting, and the Late Transposition Gap

The Directive's goal of encouraging reporting is weakened by low public awareness. The evaluation identifies socio-cultural factors and underreporting as major concerns. The transposition timeline has made this worse. Only a few Member States met the December 2021

[11] (Directive (EU) 2019/1937, Article 8)
[12] (Directive (EU) 2019/1937, Article 11)

deadline, and most completed transposition in 2023 and 2024. In many Member States, awareness campaigns have had very little time to operate. Citizens cannot benefit from protections they do not know exist.

Under Article 10, competent authorities must provide information and support to potential whistle-blowers, including making them aware of the protections available.[13] The evidence shows that this obligation has not been applied consistently. The link between late transposition, which is itself a breach of EU law, and the awareness gap is direct. The Commission should require Member States to demonstrate concrete awareness programmes as part of their ongoing compliance obligations, as well as provide concrete guidelines for how member states can conduct such awareness programmes.

3.3 Protection for Informal and Platform Workers

The Directive's personal scope covers employees, self-employed persons, volunteers, and contractors[14]. However, COM (2024) 269 found that some Member States have applied this scope in a restrictive way and have excluded groups such as volunteers, contractors, and suppliers. This problem is especially serious for platform economy workers who work through digital platforms on gig or zero hours arrangements. Their position in a legal grey zone makes it difficult for them to rely on the Directive's protections in practice.

Platform workers who witness wrongdoing by the platforms they work through, such as data collection abuses, algorithmic manipulation, or discriminatory content moderation, are among the people who most need protection. Yet they may be less likely to receive it under current national implementations. The evaluation should address this gap directly, and any revision of the Directive should make clear that platform workers are fully within its personal scope regardless of the form of their contract.

3.4 Accountability of Competent Authorities

The Directive requires competent authorities to receive reports, follow them up, and protect reporting persons. However, it does not require them to publish information about how they are meeting these obligations. As a result, citizens and civil society have no way to see whether

[13] (Directive (EU) 2019/1937, Article 10).
[14] (Directive (EU) 2019/1937, Article 4)

reports are being acted on, whether certain sectors or types of wrongdoing are being overlooked, or whether the protection system is working as the Directive intends.

This lack of transparency is at odds with the Directive's own aim of strengthening accountability in the enforcement of EU law. Annual transparency reports from all competent authorities, covering the volume, categories, and outcomes of the reports they receive, would improve public oversight without revealing the identity of reporting persons. Confidentiality would remain fully protected under Article 16 of the Directive[15].

In light of these concerns, we call on the Commission to:

- Require all competent authorities designated under the Directive to publish annual transparency reports covering the volume, categories, and outcomes of reports received, without disclosing information that would identify reporting persons.
- Mandate concrete, measurable awareness programmes for employers and the public as part of Member States' ongoing compliance obligations, with the Commission assessing their adequacy in future monitoring.
- Clarify, through a revision of the Directive or binding guidance, that platform workers, zero-hours contractors, and self-employed persons engaged through digital platforms are unambiguously within the Directive's personal scope under Article 4.
- Require Member States to ensure that internal reporting channels are actively communicated to all persons within their personal scope, including contractors and non-permanent staff, as a condition of compliance with Article 8.
- Introduce standardised, machine-readable formats for the transparency reports of competent authorities to enable civil society monitoring and cross-border comparison.

Conclusion

The European Pirate Party supports the Whistleblower Protection Directive as a vital instrument for transparency, accountability, and the effective enforcement of EU law. Whistle-blowers play

[15] (Directive (EU) 2019/1937, Article 16)

an irreplaceable role in exposing wrongdoing that would otherwise remain hidden, and the Directive's evaluation is an opportunity to ensure its protections match that role.

However, as currently implemented, the Directive risks falling short in several key areas of practical importance. Retaliation protection is too weak to change the rational calculation facing potential reporters. The scope does not cover the digital harms that are most pressing in 2026. And awareness of available protections remains inadequate among the workers who most need them.

We call on the Commission to revise the Directive to:

- Introduce mandatory minimum standards for penalties and interim protection measures that genuinely deter retaliation and protect reporting persons during proceedings;
- Require national courts to apply a fundamental rights framework under Articles 11 and 47 of the Charter in whistle-blower retaliation cases;
- Extend the material scope to cover AI system harms, algorithmic discrimination, and large-scale surveillance beyond the AI Act's own scope, and add the Digital Services Act to the Directive's Annex;
- Broaden the public interest threshold to cover digital infrastructure harms that are technically lawful but contrary to fundamental rights;
- Clarify the interaction with NIS2's maximum harmonisation provisions to prevent whistle-blower-specific protections from being displaced;
- Require mandatory annual transparency reports from all competent authorities and measurable awareness programmes from Member States;
- Ensure platform workers and informal workers are unambiguously protected within the Directive's personal scope.

A whistle-blower protection framework that works in practice not only on paper, is essential to the functioning of democratic accountability in the EU.

References

CFR. (2000). *Charter of Fundamental Rights of the European Union (2012/C 326/02).* Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf

COM(2024) 269 final. European Commission. (2024). *Report from the Commission to the European Parliament and the Council on the implementation and application of 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.* Retrieved from https://commission.europa.eu/document/download/7cc63350-88c9-4c0b-a46e-04fc11e673e7_en?filename=COM_2024_269_1_EN_ACT_part1_v6.pdf

COM(2026) 13. European Commission. (2026). *Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2].* Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:9b9c0d74-f6e3-11f0-b9bc-01aa75ed71a1.0001.02/DOC_1&format=PDF

Directive (EU) 2019/1937. European Parliament and Council. (2019). *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.* Retrieved from https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng

EU AI Act. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

European Commission. (2019). *Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1937

European Commission. (2026). *AI Act Whistleblower Tool.* Retrieved from https://digital-strategy.ec.europa.eu/en/policies/ai-act-whistleblower-tool

GDPR. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).* Retrieved from https://gdpr-info.eu/

Manifesto, E. P. (n.d.). *European Pirate Party Manifesto.* Retrieved from https://europeanpirates.eu/manifesto/

Regulation (EU) 2022/1925. European Parliament and Council. (2022). *Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925

Regulation (EU) 2022/2065. European Parliament and Council. (2022). *Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act).* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

Transparency International. (2025, January). *EU Whistleblower Protection: Falling Short When It Matters Most.* Retrieved from https://www.transparency.org/en/news/eu-whistleblower-protection-falling-short-when-it-matters-most

European Pirate Party (PPEU)

europeanpirates.eu