Article 87

Reporting of infringements and protection of reporting persons

Commentary by Simon Gerdemann | Submitted: March 2026

AI Act provision

Article 87

Directive (EU) 2019/1937 shall apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

Recitals

Recital 172

Persons acting as whistleblowers on the infringements of this Regulation should be protected under the Union law. Directive (EU) 2019/1937 of the European Parliament and of the Council (54) should therefore apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

Related laws

Directive (EU) 2019/1938 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law

Select bibliography

- Abazi V, 'Whistleblowing in the European Union' (2021) 58 Common Market Law Review 813.
- Brown A, Lewis D, Moberly R and Vandekerckhove W (eds), *International Handbook of Whistleblower Research* (Edward Elgar Publishing 2014).
- Colneric N and Gerdemann S (eds), *Beck'scher Online-Kommentar Hinweisgeberschutzgesetz* (9th edn, C H Beck 2026).
- Gerdemann S, 'The European Court of Human Rights' Effects on the Transposition of the Whistleblowing Directive' in S Gerdemann (ed), *Europe's New Whistleblowing Laws* (Göttingen University Press 2023).
- Gerdemann S, 'Whistling in the void: The Whistleblowing Directive as a case study on why the direct effects doctrine and infringement proceedings fail to enforce Union law and how to fix it'

(2025) 31 European Law Journal 134.

- Gerdemann S and Colneric N, 'The EU Whistleblowing Directive and its Transposition: Part 1' (2021) 12 European Labour Law Journal 193.
- Gerdemann S and Colneric N, 'The EU Whistleblowing Directive and its Transposition: Part 2' (2021) 12 European Labour Law Journal 253.

Commentary

1. General remarks

1.1. Introduction

1. Article 87 declares Directive (EU) 2019/1937 applicable to the reporting of infringements of the AI Act's provisions in order to provide protection for AI whistleblowers, as Recital 172 AI Act explains.[1] The article, which was proposed by the European Parliament during the trilogue proceedings,[2] achieves a comprehensive integration of the AI Act with the so-called Whistleblowing Directive ("WBD").[3] It corresponds with functionally similar provisions in earlier legislative acts[4] and reflects the

[1] 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) [2024] OJ L 1689/1 ("AI Act").

[2] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM (2021) 0206 COD (2021) 0106, Document P9 [2023] 0236, amendment 135.

[3] 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 [2019] OJ L 305/17 ("WBD").

[4] See Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 [2020] OJ L 347, art 47; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2002] OJ L 265/1 ("DMA"), art 43; Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L 150/40, art 116; Regulation (EU) 2024/573 of the European Parliament and of the Council of 7 February 2024 on fluorinated greenhouse gases, amending Directive (EU) 2019/1937 and repealing Regulation (EU) No 517/2014 [2024] OJ L

gradual expansion of the scope of whistleblowing legislation as a typical feature of whistleblowing law. The main reason behind this development is the empirical finding that specific whistleblower protection provisions and reporting procedures have been shown to effectively reduce existing information asymmetries in law enforcement while creating few legislative and administrative costs.[5] This makes it attractive for legislators to ensure that the enforcement of new legislation, such as the AI Act, benefits from existing whistleblowing laws and structures by simply adding provisions such as Article 87. This is especially the case if it is expected that the enforcement of that new legislation will be substantially enhanced by insider knowledge, which is particularly the case in the field of regulating AI models and systems.[6]

1.2. Structure and overview

2. Compared to most other provisions of the AI Act, which are often significantly longer and systematically interlinked, the regulatory structure of Article 87 – consisting of only a single sentence – may appear relatively simple. On analysis, however, Article 87 is one of the most complex provisions of the AI Act, as it imports virtually all provisions of the WBD and all corresponding national laws enacted to implement the directive into the field of AI regulation.[7] Whilst the specific legal consequences of this approach will be explained later,[8] the following section aims to provide a general overview of the fundamental structure of the WBD and its core provisions.

3. To protect whistleblowers and make effective use of their insider knowledge and other whistleblowing-related information, the WBD primarily employs three regulatory instruments which are typical in international whistleblowing law:[9] (i) individual legal protection against retaliation, (ii) requirements for internal whistleblowing channels and procedures, and (iii) the establishment of specialised whistleblowing authorities. The fourth instrument, though less relevant in practice, is whistleblowing-specific sanctions and penalties. All four features are also found in the national implementing acts, which have now been adopted by all Member States. That said, the legislative structure and quality of national laws and practices may differ considerably in some respects, a matter which requires particular attention especially in international whistleblowing cases.[10]

4. The individual protection of whistleblowers or 'reporting persons' is primarily governed by Articles 6, 15, 19 and 21 WBD. At the heart of the protection framework lies a whistleblowing-specific 'anti-retaliation law', which functions similarly to the anti-discrimination law familiar from other directives.[11]

573/1, art 30; Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 [2024] OJ L 1760/1, arts 30 and 60.

[5] See Simon Gerdemann, *Transatlantic Whistleblowing: The Legal Development, Functioning and Status Quo of Whistleblowing in the USA and Its Significance for Germany* (Mohr Siebeck 2018) paras 15 et seqq. with further references.

[6] See paras 6–7.

[7] Certain other provisions of the AI Act, like article 75(1) and article 94, also contain underspecified references to the application of other EU instruments, particularly the Market Surveillance Regulation, whose effective operationalisation carries high levels of legal uncertainty and ambiguity. For more details, refer to the forthcoming commentaries on Article 75(1) and Article 94 in this work.

[8] See Section 2, paras 10 et seqq.

[9] See e.g. Gerdemann, 'Die internationale Entwicklung des Whistleblowing-Rechts', in Ralf Kölbel (ed), *Whistleblowing* (Volume 2: Normative Perspektiven, C. F. Müller 2024) 56 et seqq. with further references.

[10] See Ninon Colneric and Simon Gerdemann (eds), *Beck'scher Online-Kommentar Hinweisgeberschutzgesetz* (9th edn, C.H. Beck 2026) § 1 paras 171–181.

[11] See e.g. Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L 180/22, arts 7 et seqq.; Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation [2000] OJ L 303/16, arts 7 et seqq.; Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal

Unlike the latter, however, it is based not on personal characteristics but on the conduct of the protected person. The conditions for protection set out in Articles 6 and 15 WBD essentially require that a person has reasonable grounds to believe that breaches falling within the scope of the WBD have occurred and that they report information about these breaches to an internal or external reporting channel or disclose it publicly.[12] If a whistleblower meets the conditions for protection, retaliation – that is, detriments caused to them because of a protected activity[13] – is prohibited and may trigger further civil claims (Articles 19 and 21 WBD).

5. The establishment of internal reporting channels is primarily governed by Articles 7 to 9 WBD. The goal is to provide whistleblowers – who, in practice, overwhelmingly report their concerns internally[14] – with a suitable internal point of contact who can take appropriate follow-up measures based on the information provided. Apart from some special sector-specific requirements, all entities in the private and public sector are obliged to establish and operate an internal reporting channel if they have 50 or more workers.[15] When processing a report, the responsible persons are, in particular, obliged to maintain the confidentiality of the whistleblower's identity in accordance with Article 16 WBD in order to pre-emptively protect the individual from retaliation and to increase an overall willingness to report. The third regulatory instrument – the establishment of specialised whistleblowing authorities – is primarily governed by Articles 11 to 14 WBD. The specific authorities responsible at a national level for receiving and handling reports, as well as for implementing follow-up measures, are set up and regulated differently depending on the Member State. At the EU level, the external reporting channel of the AI Office is of particular importance with regard to the reporting of breaches of the AI Act; its responsibilities and procedures are discussed in more detail below.[16] In addition to the three key regulatory instruments, Article 23 WBD also requires Member States to introduce whistleblowing-specific sanctions, for example for engaging in retaliation against whistleblowers and for breaching the duty of confidentiality. In practice, however, such sanctions are of limited significance, particularly as experience shows that proving retaliation in whistleblowing cases is often particularly difficult without specific rules on which party bears the burden of proof.[17]

1.3. Opportunities and problems of (GP)AI whistleblowing

6. Experience shows that whistleblowing is particularly important as a means of overcoming information asymmetries in areas where breaches and serious malpractices occur within complex organisational structures, subject matters that are difficult for outsiders to understand, and/or where there is a lack of effective regulatory oversight. This has been observed in the past both in high-profile public disclosures, such as the case of the intelligence officer Edward Snowden,[18] and in many other sectors where whistleblowing legislation is of particular practical importance.[19] Where such information

---

treatment between men and women in the access to and supply of goods and services [2004] OJ L 373/37, arts 8 et seqq.

[12] See Section 2.2., paras 17 et seqq.

[13] Apart from reporting or disclosing information as a whistleblower, it should be noted that other activities, e.g. facilitating a report by another person, may also qualify as a protected activity (see Section 2.2., paras 17 et seqq.).

[14] See WBD, recital 35; among several similar studies, e.g. Ethics Resource Center (ERC), National Business Ethics Surveys of the US Workforce 2013 (2014) 29. The fact that well over 90% of people chose to report inside their organisation holds true across all regulatory areas and remains stable even when authorities introduce financial reports for external reporting (see e.g. National Whistleblower Centre, *Impact of Qui Tam Laws on Internal Compliance* (2010) 4; Gerdemann, *Transatlantic Whistleblowing* (n 5) paras 7, 81, 218; for a qualitative evaluation of several whistleblower cases and people's motivations for reporting internally, see e.g. Nico Herold, *Whistleblower* (Nomos 2016).

[15] See WBD, art 8; Section 2.2., para 19.

[16] See Section 2.3., paras 25 et seqq.

[17] See Section 2.2., para 24.

[18] See e.g. Edward Snowden, *Permanent Record* (Metropolitan Books 2019).

[19] See Gerdemann, *Transatlantic Whistleblowing* (n 5) paras 12 et seqq. and 27 et seqq. with further references.

asymmetries coincide with violations whose prevention and punishment are of particular public interest, both the necessity and the likelihood of whistleblowing increase.[20]

7. All these considerations generally apply to the field of AI and its regulation, and even more so specifically to general-purpose AI (GPAI) models and systems.[21] This is because identifying potentially harmful developments and their causes in the field of AI regularly requires specialist insider knowledge of the development and training processes of relevant models, which may, in many cases, prove difficult to obtain by external individuals and institutions without the initiative of people within the respective organisation. At the same time, the negative consequences – particularly, though not exclusively, in the case of exponentially hazardous developments in GPAI models – carry systemic risks of potentially grave magnitude and are thus a matter of considerable public interest.[22] This situation, however, is met by a regulatory oversight structure that, once established, is mostly dependent on assessments of information provided by providers themselves.[23] This reliance will likely give rise to practical supervisory difficulties in light of the specific administrative constraint involved in regulating a rapidly developing technology like GPAI models, given that the complexities of their design, training and testing are hard to ascertain for people not directly involved in the development process and application of such models.[24] Within the normative framework of the AI Act, these inherent shortcomings are already evident in, amongst other things, the regulatory strategies chosen to regulate GPAI model providers. Such strategies rely predominantly on an outside assessment of open-ended risk mitigation requirements, transparency obligations and methods of self-regulation.[25] Given this situation, it is unsurprising that both the European legislature as well as various other organisations and initiatives have recognised the necessity and potential significance of whistleblowing, which is why AI development and application are widely regarded as one of the most important future areas of whistleblowing law.[26]

8. However well-suited the asymmetries apparent in the field of AI may be to whistleblowing, the challenges facing effective AI-related whistleblowing legislation are equally significant. This is especially true when it comes to providing effective protection for whistleblowing concerning the development and use of GPAI models, where the framework of the WBD reaches its limits. A key reason for this

---

[20] This corresponds with empirical data and professional experience showing that most whistleblowers are primarily driven by altruistic motivations. See e.g. David Lewis, A.J. Brown, and Richard Moberly, ´Whistleblowing, its Importance and the State of Research´, in A.J. Brown, David Lewis, Richard Moberly, and Wim Vandekerckhove (eds) *International Handbook of Whistleblower Research* (Edward Elgar Publishing 2014) ch 1.

[21] See also Apoory Agarwal, Dimitrios Kafteranis and Adam Fenton, 'AI Whistleblowers - Regulators of Last Resort?' (*Coventry University Research and Enterprise Blog*, 10 February 2026) <https://www.coventry.ac.uk/research/research-blog/ai-whistleblowers/> accessed 5 May 2026 with similar assessments and conclusions; See (more broadly) Hannah Bloch-Wehba, 'The Promise and Perils of Tech Whistleblowing' (2024), 118 Northwestern University Law Review 1503.

[22] This is irrespective of the fact that these risks, specifically those of 'systemic' nature, are not well understood and regulated by the AI Act (See Philipp Hacker, Atoosa Kasirzadeh, and Lilian Edwards, 'AI, Digital Platforms, and the New Systemic Risk' (2025) <https://dx.doi.org/10.2139/ssrn.5475049> accessed 5 May 2026; Samuel Carey, 'Regulating Uncertainty: Governing General-Purpose AI Models and Systemic Risk' (2025) 17 European Journal of Risk Regulation 123).

[23] See AI Act, arts 91 et seq.

[24] Similar limitations in assessing algorithmic risks via external oversight have, for example, been observed with respect to the enforcement of the DSA (see Simon Gerdemann, 'Artificial Intelligence and Social Media – How AI Shapes Online Discourse and Why the European Commission Seeks to Centralize Control over AI Online Democracy' [2026] Künstliche Intelligenz und Recht 30). The fact that complex and often secretive industry sectors require insider knowledge to be regulated effectively has been the reason for many previous whistleblowing laws, e.g. in the area of US and EU financial regulation after the financial crisis of 2007–2009 (See Simon Gerdemann, Whistleblower als Agenten des Europarechts – Die Whistleblowing-Rechtsakte der EU von ihren Anfängen bis zur aktuellenWhistleblowing- Richtlinie (2020) 37 NZA-Beilage 43).

[25] See AI Act, arts 53–56.

[26] As an example of several NGO projects in this field, see 'The AI Whistleblower Initiative' <https://aiwi.org/> accessed 5 May 2026.

is that the providers of the most influential AI models are currently based outside the European Union, in countries such as the US and China, and are likely to remain in those jurisdictions in the foreseeable future.[27] Consequently, the individuals possessing insider knowledge for the purposes of reporting relevant breaches will generally not fall within the jurisdiction of any European Member State. This means in particular that the anti-retaliation provisions of the WBD and the respective national whistleblowing laws are unlikely to be able to provide comprehensive and effective protection for whistleblowers in many cases of GPAI whistleblowing. Whether and how the European Union will amend existing whistleblowing law to address the specific opportunities and risks of (GP)AI whistleblowing in a tailored manner remains to be seen. As a result of the current legal situation, the practical debate has now shifted to other means to incentivise whistleblowing. For example, when setting up its reporting channel, the AI Office became the first EU institution to voluntarily adopt an independent confidentiality policy in order to encourage potential GPAI whistleblowers to come forward.[28]

9. Even though the legal and practical circumstances regarding these and many other aspects of AI development and regulation are still evolving, it is already foreseeable that whistleblowing cases – and with them, whistleblowing law – are likely to be of significant importance for the future development of GPAI models, the systems that are built upon such models, and their societal impact. The practical consequences that may arise from the interplay between the AI Act and the WBD may be illustrated by the case of the Facebook whistleblower, Frances Haugen, whose disclosures concerned various risks to rights and interests also mentioned by Article 1 WBD, which the platform provider knew about based on internal studies on the consequences of their recommender algorithms but chose to ignore anyway.[29] As the development, marketing and take-up of AI continues to burgeon, it is reasonable to suggest that AI-related whistleblowing cases,[30] particularly concerning the most capable GPAI models, will also increase. If so, the inclusion of the AI Act into the scope of the WBD could prove to be a key pillar of the AI Act's regulatory framework despite the latter's several shortcomings.[31]

2. Substance

2.1. Purpose, mode and date of application

10. The primary regulatory purpose of Article 87 is to protect persons who report breaches of the provisions of the AI Act.[32] By incorporating breaches of the AI Act into the material scope of the WBD, the other regulatory objectives pursued by the WBD are also indirectly incorporated into the regulatory framework of the AI Act, foremost amongst them the objective of a more effective

[27] See e.g. Jamie Seville and Edu Roldán, 'Training Compute of Frontier AI Models Grows by 4-5x Per Year' (*Epoch AI*, 28 May 2024) <https://epoch.ai/blog/training-compute-of-frontier-ai-models-grows-by-4-5x-per-year> accessed 5 May 2026; Simon Gerdemann, 'Hidden Economic Potentials of the AI Act: How to Improve Europe's Position within the AI Value Chain [2025] Künstliche Intelligenz und Recht 413.

[28] See Section 2.3., para 28.

[29] See e.g. Nik Popli, "The 5 Most Important Revelations From the "Facebook Papers"' (*Time*, 11 December 2023) <https://time.com/6110234/facebook-papers-testimony-explained> accessed 5 May 2026; regarding recommender algorithms under the AI Act, see Simon Gerdemann, 'Systemische KI-Risken der Empfehlungssysteme von Social-Media-Plattformen' in Walter Bayer and others (eds) *In Publica Commoda: Gedächtnisschrift Gerald Spindler* (C. H. Beck 2025) 251.

[30] See e.g. Christian Djeffal, 'Article 87: Meldung von Verstößen und Schutz von Hinweisgebern' in Jens Schefzig and Robert Killan (eds), *Beck'scher Onlinekommentar KI-Recht* (C.H. Beck, 5th edn., 2025) para 2.1 with further examples.

[31] For a brief overview of potential future improvements, see Section 3, paras 30 et seqq.

[32] AI Act, recital 172.

enforcement of EU AI law.[33] To this end, the referential provision of Article 87 is intended to extend the WBD's existing material scope[34] to include breaches of all provisions of the AI Act, including the GPAI model provisions in Articles 53 to 55. The fact that Article 87 refers to 'infringements' rather than 'breaches', which is the language of the WBD, is a minor terminological mix-up without legal consequence.

11. Much more legally significant, however, is the fact that the legislature uses the AI Act as a regulation to amend the WBD as a directive. This is not unusual in EU whistleblowing law, given that the legislature has used similar provisions in both directives and regulations in order to amend the WBD's material scope of application.[35] It does, however, lead to the somewhat unusual situation that even though Article 87 forms part of a (directly applicable) regulation, its legal effects do – at least in principle – still require an act of transposition by each Member State. This causes several complications.[36] Based on the wording of Article 87 alone,[37] one might argue that rather than simply amending the WBD, Article 87's true purpose is to incorporate all of the WBD's provisions into the AI Act itself. If correct, the effect of this would be to transform the WBD's provisions into directly applicable provisions of the AI Act.[38] Such an effect appears, however, not intended by the EU legislature, who has generally understood provisions equivalent to Article 87 in other EU regulations to be amendments of the WBD.[39] Further, the 'incorporation reading' would not be able to achieve Article 87's legislative purpose,[40] since most of the WBD's provisions are not designed to be directly applicable[41] and require integration into the Member States' various national legal systems to operate properly.[42] While Article 87 is therefore to be read as an amendment to the WBD's material scope of application, this interpretation presents its own set of problems and legal uncertainties, to which the discussion now turns.

12. When reporting breaches of the AI Act, the provisions of the WBD take precedence over those of the AI Act in accordance with the *lex specialis* principle. The fact that the AI Act is a regulation and the WBD is a directive is of no consequence in this respect since there is no hierarchy between these two forms of EU legislation.[43] The fact that the WBD takes precedence over the AI Act insofar as whistleblowing is concerned is particularly relevant in view of the confidentiality provisions of Article 78 AI Act, which take a back seat whenever the WBD's conditions for whistleblower protection are met. In particular, employees of GPAI model providers (as well as employees of downstream AI

[33] See WBD, art 1 and recitals 1 et seqq.

[34] See WBD, art 2 and annex pts I and II.

[35] See Regulation (EU) 2020/1503 (n 4) art 47; DMA, art 43; Regulation (EU) 2023/1114 (n 4) art 116; Regulation (EU) 2024/573 (n 4) art 30; Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 [2024] OJ L 1640/1, art 60; Directive (EU) 2024/1760 (n 4) art 30.

[36] See para 12 et seqq.

[37] Saying that WBD 'shall apply' to the reporting of infringements of the AI Act.

[38] See, in particular, Joined cases C-37/06 and C-58/06 *Viamex Agrar Handels GmbH and Zuchtvieh-Kontor GmbH (ZVK) v Hauptzollamt Hamburg-Jonas* [2008] ECLI:EU:C:2008:18, paras 27 et seq., where the court ruled in favour of such an incorporating effect.

[39] See the WBD's consolidated version (n 3) which lists all prior provisions, including the ones found in regulations, under the 'Amended by' section of the WBD.

[40] See AI Act, recital 172.

[41] See Simon Gerdemann, 'Whistling in the Void: the Whistleblowing Directive as a Case Study on Why the Direct Effects Doctrine and Infringement Proceedings Fail to Enforce Union Law and How to Fix It' (2025) 31 European Law Journal 134.

[42] See e.g. WBD, arts 21 and 22, which require Member States to take 'the necessary measures' to protect whistleblowers and persons concerned. Depending on the area of law in question, this may, for example, include varying measures of national civil and labour law to ensure compensation in full and interim relief (see WBD, recitals 94 and 96) and/or changes to national criminal law (see WBD, art 23). none of which are self-executing.

[43] See e.g. Koen Lenaerts and Piet Van Nuffel, *EU Constitutional Law* (Oxford University Press 2021) para 23.005.

systems providers), business partners of such providers, and employees of notified bodies[44] may be allowed to report and disclose information, including trade secrets.[45] In this context, reporting breaches of the GPAI model providers' obligations in Articles 53 and 55 by employees and business partners may turn out to be of particular practical relevance given the fact that the technical complexity of many AI models and systems, as well as their compliance with the AI Act, may often prove practically difficult for outsiders to accurately assess.[46]

13. Under the second sentence of Article 288(2) TFEU,[47] regulations are generally binding in their entirety and directly applicable in every Member State. However, Article 87 constitutes a special case in that its intended legal effect is to amend a directive.[48] According to Article 288(3) TFEU, a directive is binding on each Member State to which it is addressed as regards the result to be achieved but leaves national legislators and authorities the choice of form and methods. Each Member State must therefore first transpose Article 87 by including breaches of the AI Act as potential whistleblowing information covered by their respective national whistleblowing laws by 2 August 2026.[49] Only once the material scope of national laws implementing the WBD has been extended to include the AI Act will these laws apply in full to the reporting and disclosure of breaches of the AI Act. The AI Office's FAQs about its external whistleblowing channel imply that persons who report or disclose breaches of the AI Act will be comprehensively protected under the WBD from 2 August 2026.[50] However, such a direct effect of a directive's (amended) provisions is possible only under narrow circumstances according to the Court of Justice of the European Union's (CJEU) long-standing case law.[51] Whilst it is conceivable that the CJEU might recognise such direct effect in favour of AI whistleblowers once the issue is to be determined by the court, this outcome is by no means certain.[52]

14. Nevertheless, there are good reasons to believe that reporting and disclosing breaches of the AI Act are already protected in most Member States, even before 2 August 2026. This is because, pursuant to Article 2(1)(a)(iii) WBD, breaches of product safety and compliance rules have fallen within its scope ever since the WBD's original adoption. If a Member State has transposed the WBD in such a way that its national whistleblowing laws cover all EU law or all breaches of EU product safety rules (as is often the case),[53] the national law may already provide protections for the reporting of breaches of the AI Act. This is because the AI Act is, in essential respects, a continuation of EU product safety law and draws upon well-established regulatory features of product safety law in many of its core provisions.[54] In particular, this applies to the rules on product conformity for high-risk AI systems in

[44] See AI Act, arts 28 et seqq.

[45] For an overview of the conditions for protections, see Section 2.2., paras 17 et seqq.

[46] See Section 1.3, para 7.

[47] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47 ("TFEU").

[48] See Section 2.2, paras 17 et seqq.

[49] See AI Act, art 113(2).

[50] See European Artificial Intelligence Office, 'AI Act Whistleblower Tool: FAQs' <https://ai-act-whistleblower.integrityline.app/app-page;appPageName=What%20can%20be%20reported> accessed 5 May 2026.

[51] See Case 148/78 *Criminal proceedings against Tullio Ratti* [1979] ECR 01629; Case 8/81 *Ursula Becker v Finanzamt Münster-Innenstadt* [1982] ECR 00053; Case 271/82 *Vincent Rodolphe Auer v Ministère public* [1983] ECLI:EU:C:1983:243; Joint Cases C-6/90 to C-9/90 *Andrea Francovich and Danila Bonifaci and others v Italian Republic* [1991] ECLI:EU:C:1991:428; Case C-131/97 *Annalisa Carbonari and Others v Università degli studi di Bologna, Ministero della Sanità, Ministero dell'Università e della Ricerca Scientifica and Ministero del Tesoro* [1999] ECLI:EU:C:1999:98.

[52] For an in-depth analysis of the WBD's direct effects, see Gerdemann, 'Whistling in the Void' (n 41).

[53] See European Commission, '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' COM (2024) 269 final ("Report from the Commission"), s 3.1.1.

[54] In particular, the AI Act draws from product safety blueprint legislation such as Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market

Articles 8 to 50 AI Act, which are inspired by earlier acts such as the Medical Device Regulation.[55] Whether the same is true for the comparatively novel GPAI model rules in Articles 51 to 56 AI Act, particularly the risk mitigation obligations of Articles 53 and 55 AI Act, is less clear.[56] One argument against characterising these provisions as product safety law is that there are no directly comparable provisions in prior product safety regulation that match the approach taken to regulate GPAI model providers. It is particularly noteworthy that the reference to 'systemic risks' in Article 55 AI Act derives not from product safety law but from financial market regulation.[57]

15. Nevertheless, there are some compelling arguments in favour of treating the AI Act's rules on GPAI models as substantively being product safety law in nature,[58] and thus for regarding the reporting and disclosure of breaches even prior to 2 August 2026 as protected, provided that national whistleblowing laws transposing the WBD do contain a dynamic reference to EU (product safety) law. For one, the main blueprint for the AI Act was prior product safety legislation and the act's core elements are derived from similar product safety rules.[59] While those rules have been adapted to fit the needs of AI regulation and not all of the new rules have direct counterparts in prior legislation, the AI Act's provisions are often inseparably intertwined, making any attempt to neatly distinguish between product safety and non-product safety provisions or even paragraphs within provisions almost impossible and ultimately rather meaningless. Secondly, the mere use of some new rules and mechanisms to regulate the novel challenges posed by GPAI models does not mean that the new rules enshrined by the AI Act are not product safety law by nature. In particular, the GPAI model provider obligations under Articles 53 and 55 AI Act can be understood as a logical evolution of traditional product safety law, in part even clearly drawing from traditional product safety terminology and concepts.[60] Consequently, AI whistleblowers can be assumed to already fall under the umbrella of national whistleblowing laws to

---

surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 [2008] OJ L 218/30, Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] OJ L 169/1, and Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council [2012] OJ L 316/12. See European Commission, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD (2021) 84 final; Michael Veale and Frederik Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act: Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97; Hans-W. Micklitz, ' AI Standards, EU Digital Policy Legislation and Stakeholder Participation' (2023) 12 Journal of European Consumer and Market Law 212; Simon Gerdemann and Maren K. Wöbbeking, 'Art. 40 Harmonisierte Normen und Normungsdokumente' in Mario Martini and Christiane Wendehorst (eds), *KI-VO: Verordnung über künstliche Intelligenz* (C.H. Beck, 2nd edn., 2026) paras 10 et seqq.

[55] See Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1, arts 5 et seqq.

[56] See also the forthcoming chapter on Product, Model and Entity Regulation in this work.

[57] See e.g. Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board [2010] OJ L 331/1, art 2(c).

[58] For alternative considerations that the rules on GPAI models differ from product safety legislation as traditionally understood under the New Legislative Framework, see forthcoming chapters on Product, Model and Entity Regulation and on Interpreting the AI Act through Systematic Analogies in this work.

[59] See Lenaerts and Van Nuffel (n 43) para 23.005.

[60] See, *inter alia*, AI Act, arts 3(9) and (10) on placing and making available of GPAI models on the market, as well as arts 53(4) and 55(2) read together with art 40 on the reliance of harmonised AI standards, as a traditional concept in EU product safety regulation. For a more detailed discussion on the relationship of the AI Act's rules on GPAI models with product safety legislation, see the forthcoming chapters on Product, Model and Entity Regulation and on Interpreting the AI Act through Systematic Analogies in this work.

the extent that those laws contain a reference to product safety law even before Member States explicitly expand the material scope of their respective laws.[61] While this result could certainly improve AI whistleblowers' legal protection if they are covered by such a law, the overall situation remains one of legal uncertainty at this point. This is unfortunate given that the practical effectiveness of whistleblowing laws is predicated on a high level of legal certainty: the decision whether or not to become a whistleblower is typically made in a state of high personal uncertainty and risk.[62]

2.2. Overview of the WBD's structure and substance

16. The WBD is the first legal framework in Union law that comprehensively deals with the issue of whistleblowing across various legal areas, thereby being the foundational document of what is, arguably, an independent area of Union law.[63] The main objective of the WBD is to enhance the enforcement of Union law, provide for a high level of whistleblower protection and unify the previous patchwork of different national laws.[64] While the transposition process was precarious and led to infringement proceedings against all but three Member States with no less than six sanctions issued by the CJEU,[65] the WBD led to the creation and/or modification of self-standing whistleblowing laws in all Member States, most of which did not have distinct whistleblowing laws before.[66] When drafting the WBD, the legislature drew on the experiences of whistleblowing legislation from various jurisdictions, in particular from US whistleblowing law and previous whistleblowing laws of individual Member States.[67]

17. The personal scope of the WBD is – deliberately – very broad.[68] First and foremost, the WBD refers to workers within the meaning of Article 45(1) TFEU, including civil servants.[69] However, it also covers, for example, shareholders, board members,[70] and self-employed persons.[71] The only limiting factor is that potential whistleblowers must have obtained their information in a 'work-related context', that is, during any current or past work activity in the private or public sector,[72] excluding whistleblowing in a

[61] Irrespective of whether the AI Act is thus already covered by national whistleblowing laws, the Member States are, however, still required to amend their laws by explicitly including breaches of the AI Act in order to achieve the level specificity, precision and clarity necessary to satisfy the requirements of legal certainty (see Case C-648/13 *European Commission v Republic of Poland* [2016] ECLI:EU:C:2016:490, paras 78 et seq. with further references).

[62] See e.g. Richard Moberly, 'Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley Whistleblowers Rarely Win' (2007) 49 William & Mary Law Review 65, 120 et seq.; Gerdemann, *Transatlantic Whistleblowing* (n 5) paras 62, 132, 168–69, 210, 220, 226, 243, 254, 287 with further references.

[63] See Vigjilenca Abazi, 'Whistleblowing in the European Union' (2021) 58 Common Market Law Review 813, 847–849.

[64] WBD, art 1, recitals 1 et seqq.

[65] See Report from the Commission (n 53) s 2. The six Member States sanctioned were Czechia, Germany, Estonia, Luxembourg, Hungary and Poland, with the CJEU underlining the special importance of the WBD for the effective enforcement of Union law as a reason for the amount of sanctions of up to 34 million EUR (see e.g. Case C-149/23 *European Commission v Federal Republic of Germany* [2024] ECLI:EU:C:2025:145).

[66] European Commission, 'Impact Assessment for the Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law' SWD (2018) 116 final, s B.

[67] Gerdemann, 'Die internationale Entwicklung des Whistleblowing-Rechts' (n 9) 56 et seqq. with further references.

[68] See Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 1 paras 206 et seqq.

[69] WBD, art 4(1)(a).

[70] WBD, art 4(1)(c). The equal protection of board members as whistleblowers has sometimes been questioned primarily due to their specific duty of loyalty towards the company, which is supposed to limit their right to externally report or disclose information on internal breaches of law (see Klaus Ulrich Schmolke, 'Clash of Cultures: The EU Whistleblowing Directive and National Company Law' (2025) 41 International Journal of Comparative Labour Law and Industrial Relations 57). However, neither does the WBD offer any basis for a reduced standard of protection for board members, nor are considerations based in national corporate law able to affect the specific rules of the directive or the general principle of the primacy of Union law (see Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 1 paras 218.1 et seqq.).

[71] WBD, art 4(1)(b).

[72] WBD, art 4(1) in connection with art 5(9).

private context. Apart from the whistleblowers themselves, other persons such as facilitators (e.g. colleagues who support the whistleblower) or persons connected to the whistleblower (e.g. relatives working in the same company) may also invoke the protection of the WBD if they suffer retaliation.[73] The material scope of the WBD is determined by the kind of information whistleblowers report or disclose, covering breaches against a wide range of key regulatory areas of EU law.[74] When transposing the WBD, most Member States have opted to voluntarily extend the material scope of their national laws to also cover various kinds of breaches of national law to avoid unequal treatment and legal uncertainty.[75] However, the WBD – and with it most Member States laws – does not affect certain sensitive areas such as national security and legal as well as medical professional privilege.[76] That said, it should be noted that these exceptions do not exclude certain professionals, such as attorneys, from the WBD's protections entirely; it only excludes them insofar as the applicable national or Union rules on professional confidentiality prohibit them from forwarding certain types of information to anyone. Hence, legal professionals working for GPAI model providers could, for example, report acts of their provider manipulating model algorithms or training data insofar as the information obtained does not fall under the attorney-client privilege according to relevant national law.

18. The WBD sets up several material conditions for protection, which, if met, grant whistleblowers and other protected persons the rights and privileges required by the WBD.[77] Among these, the two core conditions are a report or disclosure in accordance with the WBD and the whistleblower's belief in a breach having occurred or being very likely to occur. The first condition requires the whistleblower to report information about (potential) breaches either through an internal or external reporting channel required by the WBD ('internal/external reporting') or to disclose such information to the public either directly or via proxy, for example by passing on information to journalists ('public disclosure').[78] The second core condition requires the whistleblower to have reasonable grounds to believe that the information was true at the time of the report or disclosure and that it fell within the material scope of the WBD.[79] Importantly, this means that the whistleblower does not bear the risk of proving that a breach has in fact occurred, and it protects whistleblowers even if they make mistakes in law or in fact, as long as they reasonably believe in the existence of a breach. Following other whistleblowing laws, this 'reasonable belief standard' is intentionally lenient in order to encourage people to come forward with reports or disclosures and avoid legal uncertainties.[80] Consequently, this condition is mainly meant as a safeguard against malicious and frivolous or abusive reports. However, it is worth noting that the standard exclusively focuses on the whistleblower's belief in the information being true, without requiring any kind of specific altruistic motivation.[81]

19. With respect to the appropriate recipients of a report, the WBD follows a strict approach by granting protection only to reports made via the specific channels set out in the WBD. This condition for

[73] WBD, art 4(4).

[74] WBD, art 2, annex pts I and II.

[75] See Report from the Commission (n 53) s 3.1.1.

[76] WBD, art 3. Regarding the term 'national security' and its limits, see Joined Cases C-511/18, C-512/18, C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* [2020] ECLI:EU:C:2020:791.

[77] See in particular articles 6, 15, 21 WBD. For a detailed discussion of the WBD's conditions of protection, see Simon Gerdemann and Ninon Colneric 'The EU Whistleblowing Directive and its Transposition: Part 1' (2021) 12 European Labour Law Journal 193; Simon Gerdemann and Ninon Colneric 'The EU Whistleblowing Directive and its Transposition: Part 2' (2021) 12 European Labour Law Journal 253.

[78] See WBD, art 6(1)(b) in connection with WBD, art 5(3–6).

[79] WBD, art 6(1)(a).

[80] See Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 33 paras 22 et seqq. with further references.

[81] See WBD, recital 32. The decision to protect whistleblowers irrespective of their personal motivation stems from the experience that questioning a whistleblower's motives and/or character has been a frequent strategy in court to deprive them of protection and from the WBD's main goal to uncover breaches of Union law, for which a whistleblower's personal reasons to report or disclose a breach are irrelevant.

protection is directly linked to the structural regulatory instrument of requiring all legal entities in the private and public sector with 50 or more workers to establish internal channels and procedures to receive and follow up on internal reports[82] to ensure that potential whistleblowers have a suitable point of contact within their respective organisation. In addition to internal reporting channels, the WBD requires Member States to establish external whistleblowing channels, that is, designate competent institutions or administrative units that serve as professional whistleblowing authorities.[83] With respect to external reports on breaches of the GPAI model rules in Articles 53 to 56 AI Act, the competent authority to receive such reports sits at Union level in the form of the AI Office and its dedicated whistleblowing channel, discussed in more detail below.[84] Importantly, whistleblowers are free to choose between internal and external reporting channels, without being required to report a breach internally first before contacting the competent authorities.[85]

20. The WBD contains certain rules in common for both internal and external reporting channels and their responsible personnel, including, *inter alia*, provisions on the required follow-up and timely feedback to the whistleblower,[86] record-keeping[87] and a comparatively strict duty of confidentiality subject to penalties in case of violations.[88] The latter is a particularly important aspect in whistleblowing practice, since protecting the confidentiality of the whistleblower's identity as well as information from which their identity may be inferred is the first and sometimes only line of defence to effectively shield whistleblowers from subsequent acts of retaliation.[89] This is particularly true for potential whistleblowers who report infringements concerning GPAI model provider obligations; they often will not benefit from the WBD's other protective features if they fall outside the territorial scope of such protections.[90]

21. Unlike internal and external reporting, disclosing information publicly requires additional justification falling into one of two categories: (i) either the whistleblower has already reported the breach externally, but no appropriate action has been taken by the competent authority within three to six months (report-dependent disclosure)[91] or (ii) the whistleblower has reasonable grounds to believe that the breach constitutes an imminent or manifest danger to the public interest or to believe that the breach would not be addressed effectively or cause retaliation when reported externally (report-independent disclosure).[92] Report-dependent disclosures will, as a rule, not be available to GPAI model whistleblowers, since the AI Office is not bound by the WBD's follow-up and feedback rules.[93] The requirements for report-independent disclosures on the other hand are, in effect, strict and will rarely

[82] See WBD, art 8, with exceptions to the minimum workers requirement for certain entities, especially in the financial sector.
[83] WBD, art 11.
[84] See Section 2.3., paras 25 et seqq.
[85] WBD, art 10. As a reaction to some Member States' scepticism towards direct external reporting, article 7(2) WBD states that Member States shall encourage internal before external reporting in cases where a breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation. This legislative compromise does, however, not affect the whistleblower's individual right to choose direct external reporting (see Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 7 paras 1 et seqq. with further references).
[86] WBD, arts 9 and 11 respectively.
[87] WBD, art 18.
[88] WBD, art 16, 23(1)(d).
[89] See WBD, recital 82.
[90] See Section 1.3., para 8 and Section 2.3., paras 26 et seq.
[91] WBD, art 15(1)(a). While the regular deadline for follow-up measures and feedback is three months, the whistleblowing authority may extend it to up to six months in duly justified cases, in particular if the nature and complexity of the subject of the report require a lengthy investigation (WBD, art 11(2)(d), recital 67). Since this extension does not have to communicated to the whistleblower, it is advisable for whistleblowers to generally wait for six months before going public.
[92] WBD, art 15(1)(b).
[93] See Section 2.3., paras 26 et seq.

be fulfilled in practice.[94] The main reason behind this comparatively restrictive approach is that the WBD views whistleblowing primarily as a tool for effective law enforcement rather than a human rights issue and enabler of democratic transparency and debate.[95] As a consequence, GPAI model whistleblowers who consider making public disclosures might prefer to rely on the second pillar of European whistleblower protection: the European Court of Human Right's (ECtHR) whistleblowing case law. Unlike the WBD, the ECtHR determines whether a whistleblower is protected based on a flexible six-factor balancing test which places particular importance on the public interest in the information being disclosed and may lend itself to GPAI whistleblowing cases of general importance that may give rise to public debate as to whether certain developments cause harm to the public interest.[96] However, the clear drawbacks of this second pillar of European whistleblowing law as a source of protection for potential whistleblowers are that the result of a given case is far less predictable than under the WBD's bright-line rules and that the overall level of protection is lower than that under WBD's specific anti-retaliation framework.[97]

22. Focusing again on the WBD and its conditions for protection, it should be noted that the WBD contains a hidden, additional requirement known as the 'necessity criterion'.[98] Apart from having reasonable grounds to believe in the existence of a breach, whistleblowers must also have reasonable grounds to believe that the reported or publicly disclosed information was necessary for revealing that breach, thereby limiting the scope of information that may be forwarded. This does not, however, mean that whistleblowers may only forward specific pieces of information strictly relating to vital details of the breach; rather, it is intended to avoid the disclosure of superfluous (and potentially harmful) information without any justification.[99] Consequently, under this interpretation, GPAI whistleblowers would, for example, also be allowed to send complete sets of training data as potential pieces of evidence for alleged breaches as well as further information about internal practices and procedures to contextualise the environment in which breaches have occurred and help authorities understand and investigate the matter.[100]

23. If the abovementioned conditions are met, reporting and/or disclosing information as well as further acts of communication relating to a report or disclosure are protected.[101] Furthermore, the WBD also protects the prior acquisition of, or access to, the information that is being reported or disclosed, as

[94] See Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 32 paras 9 et seqq., 59 et seqq.

[95] See WBD, art 1, recitals 1 et seqq. and 79.

[96] See *Halet v. Luxembourg* (Judgement) [GC] ECtHR App No 21884/18 (14 February 2023), paras 108 et seqq. and para 140 specifically.

[97] This is due to the nature of the ECtHR's whistleblowing case law as a judicial balancing test which may eventually result in a national sanction or verdict against a whistleblower being overturned but cannot offer preventative or active methods of whistleblower protection. See Simon Gerdemann, 'The European Court of Human Rights' Effects on the Transposition of the Whistleblowing Directive' in Simon Gerdemann (ed), *Europe's New Whistleblowing Laws: Research Papers from the 2nd European Conference on Whistleblowing Legislation* (Göttingen University Press 2023).

[98] See WBD, art 21(2). Despite materially being a condition for protection, this requirement is mentioned in neither article 6 nor 15 WBD, but within the measures of protection of article 21 WBD, displaying an action-based systematic understanding usually found in common law jurisdictions (see Ninon Colneric and Simon Gerdemann, *Die Umsetzung der Whistleblower-Richtlinie in deutsches Recht: Rechtsfragen und rechtspolitische Überlegungen* (Bund Verlag 2020) 56 et seq. and 173).

[99] See WBD, recital 91 sentence 4.

[100] See Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 33 paras 44 et seqq.; Jan Lieder and Raphael Wagner in Jan Lieder and Philipp Ceesay, *Hinweisgeberschutzgesetz* (1st edn, C H Beck 2025), s 35 paras 45 et seqq.

[101] The later includes subsequent communication with the internal or external recipients of a report as well providing further information during a following investigation. See Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 35 paras 72 et seqq.; LAG Hessen, 10 GLa 337/25 (30 May 2025), ECLI:DE:LAGHE:2025:0530.10GLA337.25.00, paras 59 et seqq.

long as these acts do not constitute a 'self-standing criminal offence'.[102] Most scholars agree that this means whistleblowers may breach certain legal obligations in certain cases to access relevant information and evidence, for example by copying documents or accessing and forwarding files in violation of contractual duties owed to their employer, but does not allow them to commit crimes in order to gain access to such information.[103] It should be noted that, arguably, the Commission extends this by indicating that the WBD allows whistleblowers to commit (any) kind of criminal offence as long as it is necessary to obtain information relevant to a later report or disclosure, deeming only criminal offences that are not necessary for, or have nothing to do with, the later report or disclosure to be 'self-standing' and therefore not justified.[104] Committing a criminal offence to access information, such as hacking into a computer system or trespassing on restricted physical property, may of course be justified in certain cases in accordance with relevant national criminal law. There is, however, no indication that the WBD's legislature intended to provide whistleblowers with carte blanche to commit any kind of crime they deem necessary to access information, thereby effectively granting them private investigative powers which would far surpass those of any public investigative authority.[105] Accordingly, it should be noted that an authoritative reading of the term 'self-standing criminal offence' under EU law may be given only by the CJEU. As a consequence, whistleblowers will generally be best advised not to obtain potential whistleblowing information in a way that might bring them in conflict with national criminal law but instead point the competent authorities towards where such information and evidence can be found and seized using authorised or formal powers, if necessary.

24. To the extent a person has the status of a protected whistleblower under the WBD, there are three main layers of protection that apply. First, as a pre-emptive measure against retaliation, the whistleblower's identity, and information from which their identity could be inferred, may not be disclosed by the authorised staff members competent to receive or investigate internal or external reports.[106] Second, any protected activity[107] is justified in the sense that it is considered not to be a breach of any kind of confidentiality restriction or similar statutory or contractual obligation, meaning that it may not serve as legal grounds for any kind of liability.[108] In effect, this protective measure is designed to shield whistleblowers across all areas of law and can, for example, be invoked in civil proceedings to avoid liability in (i) defamation lawsuits, (ii) claims for damages based on a violation of trade-secret laws, (iii) criminal proceedings as justification for alleged criminal offenses, and/or (iv) labour law proceedings to counter dismissals and other employment-related consequences.[109] Finally, the WBD prohibits any kind of retaliation against the whistleblower and requires Member States to ensure that remedies and full compensation are provided for all damages suffered,[110] including interim relief against

[102] WBD, art 21(3).

[103] See WBD, recital 92 sentence 1–4; Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 35 paras 3 et seqq.; Andrea Schmitt in Claudia Schubert, Jörn Axel Kämmerer, and Rüdiger Veil (eds), *Beck'scher Online-Großkommentar Hinweisgeberschutzgesetz* (C H Beck 2026) § 35 paras 18 et seqq.; Lieder and Wagner (n 100) § 35 paras 12 et seqq.; Sebastian Rombey, 'Ausschluss der Verantwortlichkeit' in Gregor Thüsing (ed), *Hinweisgeberschutzgesetz* (1st edn. C H Beck 2024) § 35 paras 8 et seqq.; Torsten Groß, 'Ausschluss der Verantwortlichkeit' in Martin Reufels (ed), *Hinweisgeberschutzgesetz* (1st edn. Nomos 2026), § 35 para 3.

[104] See Report from the Commission (n 53) 8.

[105] To the contrary, WBD, recital 92 sentence 5 explicitly states that criminal offenses like trespassing and hacking ought to be governed by national criminal law and does not mention any criminal offenses that might be justified solely by fulfilling the WBD's conditions for protection.

[106] WBD, art 16; see para 20. If a whistleblower does not report the information but discloses it to a journalist, their identity is usually protected by national laws and standards based on the confidentiality of journalistic sources.

[107] I.e. reports, disclosures, access to information, facilitating reports, etc.

[108] WBD, art. 21(2) and (7).

[109] For an extensive, yet far from comprehensive, overview of the potential effects on different areas of law, see Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 35 paras 32 et seqq.

[110] WBD, arts 19 and 21(8).

retaliatory actions and compensation for pain and suffering as well as (future) lost income.[111] To exemplify the kinds of retaliation typical in whistleblowing cases, the WBD contains a non-exhaustive list of detrimental actions that may not be taken, threatened or attempted against whistleblowers, including dismissals, demotions, transfers of duties, intimidation, coercion, ostracism, and blacklisting within the industry.[112] Crucially, the WBD provides for a reversal of the burden of proof with respect to the causal link between the protected activity and the detriments suffered, meaning that whoever takes detrimental action against a whistleblower has to prove that the action was not based on whistleblowing but instead on other unrelated grounds.[113]

2.3. The AI Office's external whistleblowing channel

25. In November 2025, the European Commission's AI Office established an external reporting channel for breaches of the AI Act, referred to as the 'AI Act Whistleblower Tool'.[114] The competences of the reporting channel and its authorised staff members follow the supervisory competences of the AI Office and thus cover receiving and following-up on reports on any breaches of the GPAI model provisions in Articles 51 to 56 AI Act, as well breaches of other provisions of the AI Act relating to AI systems, provided that the system in question is based on a GPAI model and was developed by the same provider.[115] The competence to enforce other kinds of breaches primarily lies with the Member States and their national market surveillance authorities,[116] although Member States are free to designate other national authorities as competent AI whistleblowing authorities to receive and investigate reports. The AI Office is not competent to independently follow up on and address breaches of AI Act provisions that fall under the authority of the Member States, for example to investigate providers of high-risk AI systems not built in-house on the basis of an own GPAI model, with respect to breaches of the high-risk AI rules in Articles 8 to 49. That said, the AI Office has expressed that where it receives such reports that fall outside its remit, it will still assess the report and, if possible, refer whistleblowers to the appropriate national whistleblowing authority.[117]

26. Compared to other external reporting channels, such as those established by the European Anti-Fraud Office ("OLAF")[118] or for reports on other breaches of EU digital laws such as the Digital Services Act ("DSA") and Digital Markets Act ("DMA"),[119] the AI Office's external reporting channel provides whistleblowers with more detailed information on the reporting procedure and mechanisms for

[111] See WBD, recital 94. The way in which these rights have been transposed by each Member State does, however, vary greatly, with many national laws falling short of the WBD's requirements in one way or another (see Report from the Commission (n 53) s 3.4.3.). In practice, this means that whistleblowers will have to rely on a interpretation in accordance with Union law or on the CJEU's direct effects doctrine (see Gerdemann, 'Whistling in the Void' (n 41); Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 37 paras 26 et seqq.).

[112] WBD, art 19.

[113] WBD, art 21(5), recital 93. As international experience and data show, this feature is of particular practical importance for the effectiveness of a whistleblower protection statute given that retaliatory acts are often disguised behind a pretext of other reasons and proving the retaliatory intent of another person is often near impossible for whistleblowers to do (See e.g. Moberly (n 62) 120 et seq.; Gerdemann, *Transatlantic Whistleblowing* (n 5) paras 62, 132, 168–169, 210, 220, 226, 243, 254, 287).

[114] See European Commission, 'AI Act Whistleblower Tool' <https://digital-strategy.ec.europa.eu/en/policies/ai-act-whistleblower-tool> accessed 6 May 2026.

[115] See AI Act, art 75(1) sentence 1; see also the forthcoming commentary on Article 75(1) in this work.

[116] See AI Act, art 74 et seqq.

[117] See European Artificial Intelligence Office, 'AI Act Whistleblower Tool: FAQs' (n 50); See WBD, art 11(6), 12(3).

[118] See European Anti-Fraud Office, 'How to Report to OLAF', <https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en#how-to-report-to-olaf> accessed 6 May 2026.

[119] See European Artificial Intelligence Office, 'AI Act Whistleblower Tool' <https://digital-services-act-whistleblower.integrityline.app/> accessed 6 May 2026; European Commission, 'Whistleblower Tool' <https://digital-markets-act.ec.europa.eu/citizens-and-whistleblower-portal/whistleblower-tool_en> accessed 6 May 2026.

protection.[120] However, no mention is made of one crucial weakness which the AI Office's reporting channel shares with all other EU reporting channels – namely, unlike national whistleblowing authorities and their reporting channels, the EU and its institutions are not bound by the provisions of the WBD. This is because directives only address and bind the Member States, not the EU institutions themselves. This means that (i) the AI Office is, *inter alia*, not obliged to provide feedback to whistleblowers within three to six months[121] (see Article 13 WBD); (ii) AI Office staff members are not subject to a strict duty of confidentiality nor are they vulnerable to penalties in case of its violation;[122] and (iii) whistleblowers do not have the right to disclose whistleblowing information publicly if the external channel does not act within given time limits.[123] In practice, the absence of such legal safeguards is likely to have contributed to the fact that potential whistleblowers tend to refrain from reporting to EU institutions and turn to other recipients instead.[124]

27. To resolve this issue, one might argue that by establishing an external reporting channel that is supposed to grant whistleblowers protection in accordance with the WBD and its national transposition laws,[125] the AI Office has also bound itself to the WBD's provisions on the external reporting channel, thereby requiring the AI Office (and all other EU reporting channels) to comply with the same rules and standards set out for national external reporting channels. A line of CJEU case law has already established that if the Commission employs phrases and standards in internal staff regulations which are already established by secondary Union law, these phrases and standards are to be interpreted in the same way.[126] However, the situation at hand is distinguishable from those cases in several ways. First, even though the AI Office has drafted a whistleblowing policy that is much closer to the WBD's provisions than is the EU's other external channel, it has refrained from simply copying the WBD's provisions; instead, it uses its own language and rules, for example by referring to the Commission's (internal) Security Notice C(2019)1903.[127] Second, several of the WBD's requirements on external reporting channels require an act of transposition which the Commission has not carried out.[128] Third and most importantly, overriding the Commission's internal whistleblowing policies by directly applying the WBD's provisions would go against the established legal nature of directives as legal acts that (only) address the Member States, according to Article 288(3) TFEU. Hence, even though it may be desirable from a policy perspective, forcing EU institutions to abide by the same rules they apply to Member States, requiring the Commission to fully comply with the WBD would depart from a core doctrine of EU law. The one instance where it could be argued that the WBD effectively applies is with respect to the right to go public in accordance with Article 15(1) WBD if the AI Office does not provide feedback within 3–6 months. Strictly speaking, this is not a question of forcing an EU institution to comply with a directive, but rather an extension of the whistleblower's individual rights. Furthermore, the AI Office has voluntarily adopted the same 3–6 month feedback period as the WBD

[120] See European Artificial Intelligence Office, 'AI Act Whistleblower Tool: FAQs' (n 50).
[121] WBD, art 13.
[122] WBD, arts 16, 23(1)(d).
[123] See WBD, art 15(1).
[124] Such recipients include, for example, the US SEC and its SEC whistleblower program, which offers strict confidentiality and anonymity protection as well as potential rewards (see U.S. Securities and Exchanges Commission, 'Whistleblower Program' <https://www.sec.gov/enforcement-litigation/whistleblower-program> accessed 6 May 2026; Gerdemann, *Transatlantic Whistleblowing* (n 5) paras 184 et seqq.). For example, one whistleblower who opted for the SEC whistleblower program by framing revelations about algorithmic risks as violations of financial regulation was Frances Haugen (para 9).
[125] See WBD, art. 6(4).
[126] See e.g. Case F-65/07 *Laleh Aayhan and Others v European Parliament* [2009] ECR-SC I-A-1-1054 and II-A-1-567, para 116; Case T-268/11 P *European Commission v Guido Strack* [2012] ECLI:EU:T:2012:588, para 43; Case T-713/14, *Organisation des salariés auprès des institutions européennes et internationales en République fédérale d'Allemagne (IPSO) v European Central Bank* [2016] ECLI:EU:T:2016:727, para 106.
[127] See European Commission, 'Security Notice: Information assessment and classification' C (2019) 1903 final.
[128] See e.g. WBD, art. 23(1)(d).

in its internal whistleblowing policy.[129] This would make it reasonable, from a whistleblower's perspective, to believe that publicly disclosing information in accordance with Article 15(1) WBD is permissible if the AI Office violates its own rules.

28. It should be noted, however, that the AI Office's external reporting channel does offer a higher degree of protection than do other EU reporting mechanisms, due to the AI Office's adoption of a unique and comparatively strict confidentiality policy, the provisions of which have been largely modelled on the requirements of the WBD.[130] According to this policy, only three designated staff members have access to the external reporting channel, which itself is subject to various cybersecurity measures. As a general rule, the content of reports may be shared with third parties, including other members of the AI Office, only if, and to the extent that, the whistleblower has explicitly consented to the information being forwarded.[131] This policy significantly reduces the risk that the identity of a GPAI whistleblower will be disclosed by accident and makes the inherent risks associated with the decision to report breaches easier to assess and control. While this kind of self-imposed confidentiality regime still lags behind the obligations imposed on national whistleblowing authorities in terms of substance, legal certainty and enforceability, it does grant a noticeably higher level of protection than is common among other EU-level reporting mechanisms. The AI Office was willing to voluntarily bind itself to rules similar to those found in the WBD because its channel is primarily aimed at potential whistleblowers from outside the EU due to the EU's relative industrial insignificance to the GPAI model layer of the AI value chain.[132] Since employees of influential GPAI model providers and other people with relevant insider knowledge about breaches of GPAI model provider obligations are likely to work in countries such as the US and China, they will usually not benefit from protection such as the WBD's anti-retaliation law, which generally only apply within the European Union.[133] Hence, the AI Office's offer of a heightened level of preventative protection via a comparatively strict confidentiality policy is one of the few effective ways to mitigate the personal risks faced by potential whistleblowers, especially from outside the EU, and increase the likelihood of valuable reports being made.

29. A report made to the external reporting channel of the AI Office constitutes an external report within the meaning of the WBD.[134] Provided that the WBD's other conditions for protection are met, the legal protections and rights under the respective Member State's whistleblowing laws are in principle triggered by reports on breaches of GPAI model provider obligations to the AI Office. However, this requires both that the GPAI whistleblower falls within the international scope of application of the respective national whistleblowing law and that its material scope of application covers breaches of the AI Act.[135] From the perspective of potential GPAI whistleblowers, both aspects should be examined carefully when assessing the risk of falling into the existing gaps of protection under the current legal framework.

---

[129] See European Artificial Intelligence Office, 'AI Act Whistleblower Tool: FAQs' (n 50).

[130] See European Artificial Intelligence Office, 'Confidentiality Policy: AI Act Whistleblower Tool' <https://ai-act-whistleblower.integrityline.app/app-page;appPageName=Whistleblower%20policy> accessed 6 May 2026; see WBD, art 10 et seqq. and 16; see also Johannes Dilling, 'Die externe Meldestelle beim Europäischen KI-Büro' [2026] EuDIR 66, 68–70.

[131] The exception to this rule is cases where the AI Office is required to share relevant information with national authorities or in the course of judicial proceedings based on a specific obligation imposed by Union or national law.

[132] See Section 1.3. and AI Act, arts 53–56.

[133] See Colneric and Gerdemann, *BeckOK HinSchG* (n 10) § 1 paras 134 et seqq. with further details on territorial applicability and the WBD's other conflict of laws issues.

[134] See WBD, art 5(5).

[135] See Section 2.1., paras 14 et seqq.

3. Law and policy assessment

30. Assessing the deceptively simple provision of Article 87 and its likely consequences is anything but straightforward given the legal complexity of the AI Act's inclusion into the scope of the WBD and its various practical implications. On the one hand, the prospect of GPAI whistleblowing offers significant opportunities to uncover and mitigate the risks posed by GPAI models and their providers' significant influence over the digital economy and society as a whole.[136] Thus, leveraging the laws and principles of whistleblowing regulation offers regulators the possibility of gaining significantly deeper insights into the often arcane details of AI algorithms, training data, and the provider's internal decision-making than do most traditional methods of oversight and law enforcement. In this respect, it is to be welcomed that the EU legislature recognised the particular potential of AI whistleblowing at an early stage and sought to increase the likelihood of an effective enforcement of the AI Act by making use of the established regulatory framework and features of the WBD.

31. On the other hand, the protection of whistleblowers intended by Article 87 faces significant hurdles due to the specific circumstances of GPAI whistleblowing and the legal uncertainties surrounding the WBD and its national transposition laws.[137] Such uncertainties will make it difficult to persuade potential whistleblowers to report or disclose crucial information whilst they are exposed to significant personal risks. Most relevantly, the EU's limited developmental significance at the GPAI model level means that most individuals with insider knowledge will not fall within the territorial scope of the anti-retaliation protection afforded by national laws implementing the WDB. Even if they do, the specific level of protection will be anything but simple to ascertain in individual cases before the report is made, given the existing and well-known discrepancies and transposition failures in national whistleblowing laws.[138] Consequently, preventative protection through an effective and legally certain guarantee of confidentiality adhered to by the competent whistleblowing channels is of particular importance. This makes it all the more regrettable that the EU institutions have not yet bound themselves to the same rules for whistleblowing channels and procedures as required of Member States. Consequently, the level of protection afforded to potential GPAI whistleblowers is especially uncertain. This is all the more problematic given that enforcement of GPAI model regulation will be substantively enhanced by the availability of relevant insider knowledge more than in almost any other regulatory field.

32. It is doubtful whether the legislature was aware of these specific issues when it swiftly inserted the cross-reference provision of Article 87 into the AI Act during the trilogue proceedings. If the EU wishes to improve the legal and practical situation of future GPAI whistleblowers and thereby increase the EU's influence on GPAI models and their providers as the foundational cornerstones of the AI economy, a series of targeted adjustments would have to be made, which are outlined here in broad terms only. A first essential step would be for the EU to comply with the long-standing *petitum* that it should follow its own rules, meaning that it should legally bind itself to the same set of whistleblowing rules and procedures it requires its Member States to follow. The active interest of EU institutions to take this step has, however, been limited thus far. This may be linked to the fact that EU staff would expose themselves to the risk of personal sanctions if they violated the WBD's strict duty of confidentiality. Second, it will likely be necessary to closely monitor the explicit inclusion of breaches of the AI Act within the material scope of national whistleblowing laws from 2 August 2026 onwards, given that many Member States have proven to be more than hesitant to transpose the WBD in a timely and fully compliant manner. The same applies with respect to monitoring the establishment of effective internal whistleblowing channels and procedures within the organisational structures of GPAI model providers

[136] See Section 1.3.
[137] See Section 2.
[138] See Report from the Commission (n 53).

insofar as they are subject to the WBD.[139] Finally, the upcoming reform of the WBD, following the conclusion of the ongoing review process, could be used to expressly address the particular regulatory value, and the specific vulnerability, of AI whistleblowers, especially to cure the current uncertainty of the international applicability of the WBD and its national transposition laws, which is already causing problems in other international whistleblowing situations.[140]

33. If all this fails, there is a risk that the enforcement of obligations imposed on GPAI model providers and such providers that develop their own system will follow a similar path to other EU digital legislation, whereby obvious violations are identified and penalised, whilst the fundamental risks hidden deep within the code and/or in the back rooms of companies are rarely addressed.[141] Admittedly, the existing regulatory gaps and uncertainties may not deter whistleblowers from reporting or disclosing serious breaches and significant risks posed by GPAI models and systems, if most whistleblowers are motivated by altruistic motivations rather than personal cost-benefit analyses.[142] However, given the likely extent of the influence of GPAI models and their providers on our societies in the future, it would be more than negligent not to further improve the regulatory framework for whistleblowers and, in doing so, to make effective legislative use of the wealth of empirical findings and experience in the field of whistleblowing law.

[139] See WBD, art 8. This requires that the legal entity in question has more than 50 workers and falls under EU jurisdiction (see WBD, art 8; Section 2.2., para 19), including European subsidiaries of providers whose main place of operation is outside the EU.

[140] These include, for example, cases in which a whistleblower from one Member State reports breaches of law through reporting channels situated in another Member State and/or information on breaches which are covered by one national whistleblowing but not the other, creating conflict of laws problems yet to be clearly resolved by the WBD or other applicable laws.

[141] See e.g. on the enforcement of the DSA's rules for very large online platforms: Gerdemann, 'Artificial Intelligence and Social Media' (n 24).

[142] See e.g. Lewis, Brown, and Moberly (n 20).