Council of the European Union

Brussels, 10 December 2018
(OR. en)

15178/18

Interinstitutional File: 2018/0106(COD)

FREMP 218	ENFOCUSTOM 265
JAI 1245	AGRI 619
TELECOM 451	ETS 45
COMPET 848	SERVICES 73
RC 37	TRANS 617
CONSOM 350	FISC 523
DAPIX 370	SAN 450
DATAPROTECT 264	ENV 852
DROIPEN 196	GAF 61
FIN 967	ATO 92
EMPL 562	CYBER 306
MI 940	COPEN 432
PI 175	POLGEN 242
SOC 757	INF 241
CODEC 2221	ANIMAUX 28

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	14449/18
No. Cion doc.:	8713/18
Subject:	Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law - Presidency revised text

On the basis of the discussions at the meetings on 26 November and 3 December 2018, the Presidency drafted a third revision of the proposal which delegations will find in the Annex.

For ease of reference, changes in comparison to the second revised proposal (*14449/18*) have been made in the legal basis, recitals 1, 3, 7, new 10bis, 13, 17, 18, 21, 21bis, 21quater, 23bis, 23quinquies, 28, new 29bis, 30, 38, 43bis, 48ter, 49ter, 50ter, new 50quater, 64quater, 67, 73, 74, 74bis, new 75bis, 79bis, 79ter, 81 and 82, Articles 1bis(1),(2) and (3), 2(1)(c) and (2), 2bis(2) and (3), 2ter, 3(1), (4), (5), (8), (10), (12) and (13), 4(3), (3bis), (3ter), (4), (5) and (6), 5(1)(b), (1bis), 2(bis) and (3), 5bis (1), 6(1), (2), (3), (4), (5), (6) and (7), 9(1)(b) and (c), 10(g), 12, 12bis(1)(b), (2),

(3) and (4), 13bis(title) and (3), 13ter, 14(i), 15(2), (5) and (7), new 15bis, 20(1) and new (1bis) and 21(1) and (3).

With a view to advancing with the proposed directive, the Presidency invites delegations to share their positions and indicate whether they can agree on the compromise proposal or parts thereof.

2018/0106 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of persons reporting on breaches of Union law

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16, 33, 43, 50, 53(1), 62, 91, 100, 103, ~~109~~114, 168**(4)**, 169, 192**(1)** ~~207~~ and 325(4) thereof and to the Treaty establishing the European Atomic Energy Community, and in particular Article 31 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2]

Having regard to the opinion of the Court of Auditors[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Persons who work for an organisation or are in contact with it in the context of their work-related activities are often the first to know about threats or harm to the public interest which arise in this context. By 'blowing the whistle' they play a key role in exposing and preventing breaches of the law **harmful to the public interest** and in safeguarding the

1 OJ C […], […], p. […].
2 OJ C […], […], p. […].
3 OJ C […], […], p. […].

welfare of society. However, potential whistleblowers are often discouraged from reporting their concerns or suspicions for fear of retaliation.

(2) At Union level, reports by whistleblowers are one upstream component of enforcement of Union law: they feed national and Union enforcement systems with information leading to effective detection, investigation and prosecution of breaches of Union law.

(3) In certain policy areas, breaches of Union law **– notwithstanding their qualification under national law as administrative, criminal or other types of offences -** may cause serious harm to the public interest, in the sense of creating significant risks for the welfare of society. Where weaknesses of enforcement have been identified in those areas, and whistleblowers are in a privileged position to disclose breaches, it is necessary to enhance enforcement **by introducing effective reporting channels and** by ensuring effective protection of whistleblowers from retaliation ~~and introducing effective reporting channels~~.

(4) Whistleblower protection currently provided in the European Union is fragmented across Member States and uneven across policy areas. The consequences of breaches of Union law with cross-border dimension uncovered by whistleblowers illustrate how insufficient protection in one Member State not only negatively impacts ~~on~~ the functioning of EU policies in that Member State but can also spill over into other Member States and **into** the Union as a whole.

(5) Accordingly, common minimum standards ensuring effective whistleblower protection should apply in those acts and policy areas where i) there is a need to strengthen enforcement~~;~~**,** ii) under-reporting by whistleblowers is a key factor affecting enforcement, and iii) breaches of Union law cause serious harm to the public interest. **When transposing this Directive, Member States may extend the application of the national provisions to other areas with a view to ensuring a comprehensive and coherent framework at national level.**

(6) Whistleblower protection is necessary to enhance the enforcement of Union law on public procurement. In addition to the need of preventing and detecting fraud and corruption in the context of the implementation of the EU budget, including procurement, it is necessary to tackle insufficient enforcement of rules on public procurement by national public authorities and certain public utility operators when purchasing goods, works and services. Breaches of such rules create distortions of competition, increase costs for doing business, violate the interests of investors and shareholders and, overall, lower attractiveness for investment and create an uneven level playing field for all businesses across Europe, thus affecting the proper functioning of the internal market.

(7) In the area of financial services, the added value of whistleblower protection was already acknowledged by the Union legislator. In the aftermath of the financial crisis, which exposed serious shortcomings in the enforcement of the relevant rules, measures for the protection of whistleblowers**, including internal and external reporting channels as well as an explicit prohibition of retaliation,** were introduced in a significant number of legislative instruments in this area[4]. In particular, in the context of the prudential framework applicable to credit institutions and investment firms, Directive 2013/36/EU[5] provides for protection of whistleblowers, which extends also to Regulation (EU) No 575/2013 on prudential requirements for credit institutions and investment firms.

(8) As regards the safety of products placed into the internal market, the primary source of evidence-gathering are businesses involved in the manufacturing and distribution chain, so that reporting by whistleblowers has a high added value, since they are much closer to the source of possible unfair and illicit manufacturing, import or distribution practices of unsafe products. This warrants the introduction of whistleblower protection in relation to the safety requirements applicable both to 'harmonised products'[6] and to 'non-harmonised products'[7].

---

4 Communication of 8.12.2010 "Reinforcing sanctioning regimes in the financial services sector".

5 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

6 The body of relevant 'Union harmonisation legislation' is circumscribed and listed in Regulation [XXX] laying down rules and procedures for compliance with and enforcement of Union harmonisation legislation, 2017/0353 (COD).

Whistleblower protection is also instrumental in avoiding diversion of firearms, their parts and components and ammunition, as well as defence-related products, by encouraging the reporting of breaches, such as document fraud, altered marking or false declarations of import or export and fraudulent intra-communitarian acquisition of firearms where violations often imply a diversion from the legal to the illegal market. Whistleblower protection will also help prevent the illicit manufacture of homemade explosives by contributing to the correct application of restrictions and controls regarding explosives precursors.

(9) The importance of whistleblower protection in terms of preventing and deterring breaches of Union rules on transport safety which can endanger human lives has been already acknowledged in sectorial Union instruments on aviation safety[8] and maritime transport safety[9], which provide for tailored measures of protection to whistleblowers as well as specific reporting channels. These instruments also include the protection from retaliation of the workers reporting on their own honest mistakes (so called 'just culture'). It is necessary to complement the existing elements of whistleblower protection in these two sectors as well as to provide such protection to enhance the enforcement of safety standards for other transport modes, namely road and railway transport.

---

7 Regulated by Directive (EC) 2001/95 of the European Parliament and of the Council, of 3 December 2001, on general product safety (OJ L 11, p. 4).

8 Regulation (EU) No 376/2014 of the European Parliament and of the Council, of 3 April 2014, on the reporting, analysis and follow-up of occurrences in civil aviation (OJ L 122, p. 18).

9 Directive 2013/54/EU, of the European Parliament and of the Council, of 20 November 2013, concerning certain flag State responsibilities for compliance with and enforcement of the Maritime Labour Convention (OJ L 329, p. 1), Directive 2009/16/EC of the European Parliament and of the Council, of 23 April 2009, on port State control (OJ L 131, p. 57).

(10) Evidence-gathering, detecting and addressing environmental crimes and unlawful conduct against the protection of the environment remain a challenge and need to be reinforced as acknowledged in the Commission Communication "EU actions to improve environmental compliance and governance" of 18 January 2018[10]. Whilst whistleblower protection rules exist at present only in one sectorial instrument on environmental protection[11], the introduction of such protection appears necessary to ensure effective enforcement of the Union environmental *acquis*, whose breaches can cause serious harm to the public interest with possible spill-over impacts across national borders. This is also relevant in cases where unsafe products can cause environmental harm.

(10bis) Enhancing the protection of whistleblowers would also contribute to preventing and deterring breaches of Euratom rules on nuclear safety, radiation protection and responsible and safe management of spent fuel and radioactive waste. It would also strengthen the enforcement of existing provisions of the revised Nuclear Safety Directive [12] on the effective nuclear safety culture and, in particular, Article 8 b (2) (a), which requires, inter alia, that the competent regulatory authority establishes management systems which give due priority to nuclear safety and promote, at all levels of staff and management, the ability to question the effective delivery of relevant safety principles and practices and to report in a timely manner on safety issues.

(11) Similar considerations warrant the introduction of whistleblower protection to build upon existing provisions and prevent breaches of EU rules in the area of food chain and in particular on food and feed safety as well as on animal health and welfare. The different Union rules developed in these areas are closely interlinked. Regulation (EC) No 178/2002[13] sets out the general principles and requirements which underpin all Union and national measures relating to food and feed, with a particular focus on food safety, in order to ensure

---

10 COM(2018) 10 final.

11 Directive 2013/30/EU of the European Parliament and of the Council, of 12 June 2013, on safety of offshore oil and gas operations (OJ L 178, p. 66).

12 **Council Directive 2014/87/Euratom of 8 July 2014 amending Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations (OJ L 219, 25.7.2014, p. 42).**

13 Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, p. 1).

a high level of protection of human health and consumers' interests in relation to food as well as the effective functioning of the internal market. This Regulation provides, amongst others, that food and feed business operators are prevented from discouraging their employees and others from cooperating with competent authorities where this may prevent, reduce or eliminate a risk arising from food. The Union legislator has taken a similar approach in the area of 'Animal Health Law' through Regulation (EU) 2016/429 establishing the rules for the prevention and control of animal diseases which are transmissible to animals or to humans[14].

(12) ~~Enhancing the protection of whistleblowers would also favour preventing and deterring breaches of Euratom rules on nuclear safety, radiation protection and responsible and safe management of spent fuel and radioactive and would also reinforce the enforcement of existing provisions of the revised Nuclear Safety Directive[15] on the effective nuclear safety culture and, in particular, Article 8 b (2) (a), which requires, *inter alia*, that the competent regulatory authority establishes management systems which give due priority to nuclear safety and promote, at all levels of staff and management, the ability to question the effective delivery of relevant safety principles and practices and to report in a timely manner on safety issues.~~

(13) In the same vein, whistleblowers' reports can be key to detecting and preventing, reducing or eliminating risks to public health and to consumer protection resulting from breaches of Union rules which might otherwise remain hidden. In particular, consumer protection is also strongly linked to cases where unsafe products can cause considerable harm to consumers. Whistleblower protection should therefore be introduced in relation to relevant Union rules adopted pursuant to Articles 114, 168 and 169 ~~TFEU.~~ **of the Treaty on the Functioning of the European Union (hereinafter "TFEU").**

---

14 OJ L 84, p. 1.

15 ~~Council Directive 2014/87/Euratom of 8 July 2014 amending Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations (OJ L 219, 25.7.2014, p. 42).~~

(14) The protection of privacy and personal data is another area where whistleblowers are in a privileged position to disclose breaches of Union law which can seriously harm the public interest. Similar considerations apply for breaches of the Directive on the security of network and information systems[16], which introduces notification of incidents (including those that do not compromise personal data) and security requirements for entities providing essential services across many sectors (e.g. energy, health, transport, banking, etc.) and providers of key digital services (e.g. cloud computing services). Whistleblowers' reporting in this area is particularly valuable to prevent security incidents that would affect key economic and social activities and widely used digital services. It helps ensuring the continuity of services which are essential for the functioning of the internal market and the wellbeing of society.

(15) Reporting by whistleblowers is necessary to enhance the detection and prevention of infringements of Union competition law. This would serve to protect the efficient functioning of markets in the Union, allow a level playing field for business and deliver benefits to consumers. The protection of whistleblowers would enhance Union competition law enforcement, including State aid. As regards competition rules applying to undertakings, the importance of insider reporting in detecting competition law infringements has already been recognised in the EU leniency policy as well as with the recent introduction of an anonymous whistleblower tool by the European Commission[17]. The introduction of whistleblower protection at Member State level would increase the ability of the European Commission as well as the competent authorities in the Member States to detect and bring to an end infringements of Union competition law. With respect to State aid, whistleblowers can play a significant role in reporting unlawfully granted aid and informing when aid is misused, both at national, regional and local levels.

---

16 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

17 Commission Notice on Immunity from fines and reduction of fines in cartel cases (OJ C 298/~~17~~, 8.12.2006**, p. 17**); http://europa.eu/rapid/press-release IP-17-591 en.htm

(16) The protection of the financial interests of the Union, which relates to the fight against fraud, corruption and any other illegal activity affecting the use of Union expenditures, the collection of Union revenues and funds or Union assets, is a core area in which enforcement of Union law needs to be strengthened. The strengthening of the protection of the financial interests of the Union also encompasses implementation of the Union budget related to expenditures made on the basis of the Treaty establishing the European Atomic Energy Community. Lack of effective enforcement in the area of the financial interests of the Union, including fraud and corruption at national level, causes a decrease of the Union revenues and a misuse of EU funds, which can distort public investments and growth and undermine citizens' trust in EU action. Whistleblower protection is necessary to facilitate the detection, prevention and deterrence of relevant fraud and illegal activities.

(17) Acts which breach the rules of corporate tax and arrangements whose purpose is to obtain a tax advantage and to evade legal obligations, defeating the object or purpose of the applicable corporate tax law, negatively affect the proper functioning of the internal market. They can give rise to unfair tax competition and extensive tax evasion, distorting the level-playing field for companies and resulting in loss of tax revenues for Member States and for the Union budget as a whole. **This Directive provides for protection against retaliation for those who report on evasive and/or abusive arrangements that could otherwise go undetected, with a view to strengthening the ability of competent authorities to safeguard the proper functioning of the internal market and remove distortions and barriers to trade that affect the competitiveness of the companies in the internal market, directly linked to the free movement rules and also relevant for the application of the State aid rules. At the same time, it** ~~Whistleblower protection~~ **should be seen in the framework of** ~~adds to~~ recent Commission initiatives aimed at improving transparency and the exchange of information in the field of taxation[18] and creating a fairer corporate tax environment within the Union[19]~~.with a view to increasing Member States' effectiveness in~~

[18] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (as amended) **(OJ L 64, 11.3.2011, p. 1).**

[19] Council Directive (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market (as amended); Proposal for a Council Directive on a Common Consolidated Corporate Tax Base, COM/2016/0683

~~identifying evasive and/or abusive arrangements that could otherwise go undetected, and will help deter such arrangements.~~ **This Directive does not harmonise provisions relating to taxes, whether substantive or procedural, and it does not seek to strengthen the enforcement of national corporate tax rules, without prejudice to the possibility of Member States to use reported information for that purpose.**

(18) Certain Union acts, in particular in the area of financial services, such as Regulation (EU) No 596/2014 on market abuse[20], and Commission Implementing Directive 2015/2392, adopted on the basis of that Regulation[21], already contain detailed rules on whistleblower protection. Such existing Union legislation, including the list of Part II of the Annex, should ~~be complemented by the present Directive, so that these instruments are fully aligned with its minimum standards whilst maintaining~~ **maintain** any specificities they provide for, tailored to the relevant sectors. This is of particular importance to ascertain which legal entities in the area of financial services, the prevention of money laundering and terrorist financing are currently obliged to establish internal reporting channels. **At the same time, in order to ensure consistency and legal certainty across Member States, the sector-specific instruments should be complemented by the present Directive insofar as matters are not regulated in them, so that they are fully aligned with its minimum standards. In particular, this Directive should further specify the design of the internal and external channels, the obligations of competent authorities, as well as the specific forms of protection to be provided at national level against retaliation**.

(19) ~~Each time a new Union act for which whistleblower protection is relevant and can contribute to more effective enforcement is adopted, consideration should be given to whether to amend the Annex to the present Directive in order to place it under its scope.~~

(20) This Directive should be without prejudice to the protection afforded to employees when reporting on breaches of Union employment law. In particular, in the area of occupational safety and health, Article 11 of Framework Directive 89/391/EEC already requires Member States to ensure that workers or workers' representatives shall not be placed at a

---

final — 2016/0336; Proposal for a Council Directive on a Common Corporate Tax Base, COM/2016/0685 final — 2016/0337.

20 OJ L 173, p. 1.

21 Commission Implementing Directive (EU) 2015/2392 of 17 December 2015 on Regulation (EU) No 596/2014 of the European Parliament and of the Council as regards reporting to competent authorities of actual or potential infringements of that Regulation (OJ L 332, p. 126).

disadvantage because of their requests or proposals to employers to take appropriate measures to mitigate hazards for workers and/or to remove sources of danger. Workers and their representatives are entitled to raise issues with the competent national authorities if they consider that the measures taken and the means employed by the employer are inadequate for the purposes of ensuring safety and health.

(20bis) This Directive is without prejudice to the protection afforded by the procedures for reporting possible illegal activities, including fraud or corruption, detrimental to the interests of the Union, or of conduct relating to the discharge of professional duties which may constitute a serious failure to comply with the obligations of officials of the established under Articles 22a, 22b and 22c of the Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community. The Directive applies where EU officials reporting in a work-related context outside their employment relationship with the EU institutions.

(21) **National security remains the sole responsibility of each Member State, in the fields of both defence and security. This Directive should apply to reports on breaches related to procurement involving defence or security aspects only to the extent that Directive 2014/24/EU is applicable to such procurement.**This Directive should **also** be without prejudice to the protection of classified information which Union law or the laws, regulations or administrative provisions in force in the Member State concerned require, for security reasons, to be protected from unauthorised access. In particular, Moreover, the provisions of this Directive should not affect the obligations arising from Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, or Council Decision of 23 September 2013 on the security rules for protecting EU classified information.

(21bis) This Directive should not affect the protection of confidentiality of communications between lawyers and their clients ('legal professional privilege') as provided for under national and, where applicable, Union law, in accordance with the case law of the Court of Justice of the European Union.[22] Moreover, the Directive should not affect the obligation of maintaining confidentiality of communications of health care providers,

[22] Cases C‑550/07 P, Akzo Nobel Chemicals and Akcros Chemicals v Commission, C-305/05 - Ordre des barreaux francophones en germanophone e.a.

including therapists, with their patients and of patient records ('medical privacy') as provided for under national and Union law. (21ter) Members of other professions may qualify for protection under this Directive when they report information protected by the applicable professional rules, provided that reporting that information is necessary for revealing a breach within the scope of this Directive.

(21quater) While this Directive provides under certain conditions for a limited exemption from liability, including criminal liability, in case of breach of confidentiality, it does not affect national rules on criminal procedure, particularly those aiming at safeguarding the integrity of the investigations and proceedings or the rights of defence of concerned persons. This is without prejudice to the introduction of measures of protection into other types of national procedural law, in particular, the reversal of the burden of proof in national administrative, civil or labour proceedings.

(22) Persons who report information about threats or harm to the public interest obtained in the context of their work-related activities make use of their right to freedom of expression. The right to freedom of expression, enshrined in Article 11 of the Charter of Fundamental Rights of the European Union ('the Charter') and in Article 10 of the European Convention on Human Rights (ECHR), encompasses media freedom and pluralism.

(23) Accordingly, this Directive draws upon the case law of the European Court of Human Rights on the right to freedom of expression, and the principles developed on this basis by the Council of Europe in its 2014 Recommendation on Protection of Whistleblowers[23].

(23bis) To enjoy protection, the reporting persons should reasonably believe, in light of the circumstances and the information available to them at the time of the reporting, that the matters reported by them are true. This is an essential safeguard against malicious and frivolous or abusive reports, ensuring that those who, at the time of the reporting, deliberately and knowingly reported wrong or misleading information, as well as those who, after the reporting, became aware that the information reported was false but did not seek to withdraw or update the report, do not enjoy protection. At the same time, it ensures that protection is not lost where the reporting person made an inaccurate report in honest error. In a similar vein, reporting persons should be entitled to protection under this Directive if they have reasonable grounds to believe that the information reported falls within its scope. The motives of the reporting person in

[23] CM/Rec(2014)7.

making the report should be irrelevant as to whether or not they should receive protection.

(23ter) The requirement of a tiered use of reporting channels, as a general rule, is necessary to ensure that the information gets to the persons who can contribute to the early and effective resolution of risks to the public interest as well as to prevent unjustified reputational damage from public disclosure. At the same time, some exceptions to its application are necessary, allowing the reporting person to choose the most appropriate channel depending on the individual circumstances of the case. Moreover, it is necessary to protect public disclosures taking into account democratic principles such as transparency and accountability, and fundamental rights such as freedom of expression and media freedom, whilst balancing the interest of employers to manage their organisations and to protect their interests with the interest of the public to be protected from harm, in line with the criteria developed in the case-law of the European Court of Human Rights[24].

(23quater) Without prejudice to existing obligations to provide for anonymous reporting by virtue of Union law, Member States may decide whether public entities and competent authorities accept and follow-up on anonymous reports of breaches falling within the scope of this Directive. However, persons who reported or made public disclosures falling within the scope of this Directive and meet its conditions should enjoy protection under this Directive if they suffer retaliation.

(23quinquies) In order to limit the burden on internal and external channels, and to allow them to concentrate on important breaches, information on breaches exclusively affecting the individual rights of the reporting person should, as a rule, not be reported under the procedures of this Directive, but under other available procedures, unless that information reveals a wider pattern of breaches.

(24) Persons need specific legal protection where they acquire the information they report through their work-related activities and therefore run the risk of work-related retaliation (for instance, for breaching the duty of confidentiality or loyalty). The underlying reason for

---

24 **One of the criteria for determining whether retaliation against whistleblowers making public disclosures interferes with freedom of expression in a way which is not necessary in a democratic society, is whether the persons who made the disclosure had at their disposal alternative channels for making the disclosure; see, for instance, Guja v. Moldova [GC], no 14277/04, ECHR 2008.**

providing them with protection is their position of economic vulnerability vis-à-vis the person on whom they *de facto* depend for work. When there is no such work-related power imbalance (for instance in the case of ordinary complainants or citizen bystanders) there is no need for protection against retaliation.

(25) Effective enforcement of Union law requires that protection is granted to the broadest possible range of categories of persons, who, irrespective of whether they are EU citizens or third-country nationals, by virtue of **their** work-related activities (irrespective of the nature of these activities, whether they are paid or not), have privileged access to information about breaches that would be in the public's interest to report and who may suffer retaliation if they report them. Member States should ensure that the need for protection is determined by reference to all the relevant circumstances and not merely by reference to the nature of the relationship, so as to cover the whole range of persons connected in a broad sense to the organisation where the breach has occurred.

(26) Protection should, firstly, apply to persons having the status of 'workers', within the meaning of Article 45**(1)** TFEU, as interpreted by the Court of Justice of the European Union[25], *i.e.* persons who, for a certain period of time, perform services for and under the direction of another person, in return of which they receive remuneration. **This notion also includes civil servants.** Protection should thus also be granted to workers in non-standard employment relationships, including part-time workers and fixed-term contract workers, as well as persons with a contract of employment or employment relationship with a temporary agency, which are types of relationships where standard protections against unfair treatment are often difficult to apply.

[25] Judgments of 3 July 1986, Lawrie-Blum, Case 66/85; 14 October 2010, Union Syndicale Solidaires Isère, Case C-428/09; 9 July 2015, Balkaya, Case C-229/14; 4 December 2014, FNV Kunsten, Case C-413/13; and 17 November 2016, Ruhrlandklinik, Case C-216/15.

(27) Protection should also extend to further categories of natural ~~or legal~~ persons, who, whilst not being 'workers' within the meaning of Article 45**(1)** TFEU, can play a key role in exposing breaches of the law and may find themselves in a position of economic vulnerability in the context of their work-related activities. For instance, in areas such as product safety, suppliers are much closer to the source of possible unfair and illicit manufacturing, import or distribution practices of unsafe products; in the implementation of Union funds, consultants providing their services are in a privileged position to draw attention to breaches they witness. Such categories of persons, including self-employed persons providing services, freelance, contractors, sub-contractors and suppliers, are typically subject to retaliation in the form of early termination or cancellation of contract of services, licence or permit, loss of business, loss of income, coercion, intimidation or harassment, blacklisting/business boycotting or damage to their reputation. Shareholders and persons in managerial bodies, may also suffer retaliation, for instance in financial terms or in the form of intimidation or harassment, blacklisting or damage to their reputation. Protection should also be granted **to persons whose work-based relationship ended and** to candidates for employment or for providing services to an organisation who acquired the information on breaches of law during the recruitment process or other pre-contractual negotiation stage, and may suffer retaliation for instance in the form of negative employment references or blacklisting/business boycotting.

(28) Effective whistleblower protection implies protecting also further categories of persons who, whilst not relying on their work-related activities economically, may nevertheless suffer retaliation for exposing breaches. Retaliation against volunteers and **paid or** unpaid trainees may take the form of no longer making use of their services, or of giving a negative reference for future employment or otherwise damaging their reputation.

(29) ~~Effective detection and prevention of serious harm to the public interest requires that the information reported which qualifies for protection covers not only unlawful activities but also abuse of law, namely acts or omissions which do not appear to be unlawful in formal terms but defeat the object or the purpose of the law.~~

(29bis) Effective detection and prevention of serious harm to the public interest requires that the notion of breach also includes abusive practices, as determined by the case law of

the European Court of Justice[26], namely acts or omissions which do not appear to be unlawful in formal terms but defeat the object or the purpose of the law.

(30) Effective prevention of breaches of Union law requires that protection is ~~also~~ granted to persons who provide information **necessary to reveal** ~~about~~ ~~potential~~ breaches **which have already taken place, breaches** which have not yet materialised, but are **very** likely to be committed**, acts or omissions which the reporting person has reasonable grounds to consider as breaches of Union law as well as attempts to conceal breaches.** ~~.~~ For the same reasons, protection is warranted also for persons who do not provide positive evidence but raise reasonable concerns or suspicions. At the same time, protection should not apply to the reporting of information which is already **fully available** in the public domain or of unsubstantiated rumours and hearsay.

(31) Retaliation expresses the close (cause and effect) relationship that must exist between the report and the adverse treatment suffered, directly or indirectly, by the reporting person, so that this person can enjoy legal protection. Effective protection of reporting persons as a means of enhancing the enforcement of Union law requires a broad definition of retaliation, encompassing any act or omission occurring in the work-related context which causes them detriment.

(32) Protection from retaliation as a means of safeguarding freedom of expression and media freedom should be provided both to persons who report information about acts or omissions within an organisation (internal reporting) or to an outside authority (external reporting) and to persons who disclose such information to the public domain (for instance, directly to the public via web platforms or social media, or to the media, elected officials, civil society organisations, trade unions or professional/business organisations).

(33) Whistleblowers are, in particular, important sources for investigative journalists. Providing effective protection to whistleblowers from retaliation increases the legal certainty of (potential) whistleblowers and thereby encourages and facilitates whistleblowing also to the media. In this respect, protection of whistleblowers as journalistic sources is crucial for safeguarding the 'watchdog' role of investigative journalism in democratic societies.

---

[26] Case C-110/99 Emsland-Stärke, Case C-255/02 Halifax and Others , Case C-524/04 Test Claimants in the Th in Cap Group Litigation and Case C-182/08 Glaxo Wellcome.

(34) ~~It is for the Member States to identify the authorities competent to receive and give appropriate follow up to the reports on breaches falling within the scope of this Directive. These may be regulatory or supervisory bodies in the areas concerned, law enforcement agencies, anti-corruption bodies and ombudsmen. The authorities designated as competent shall have the necessary capacities and powers to assess the accuracy of the allegations made in the report and to address the breaches reported, including by launching an investigation, prosecution or action for recovery of funds, or other appropriate remedial action, in accordance with their mandate.~~

(35) ~~Union law in specific areas, such as market abuse[27], civil aviation[28] or safety of offshore oil and gas operations[29] already provides for the establishment of internal and external reporting channels. The obligations to establish such channels laid down in this Directive should build as far as possible on the existing channels provided by specific Union acts.~~

(36) ~~Some bodies, offices and agencies of the Union, such as the European Anti-Fraud Office (OLAF), the European Maritime Safety Agency (EMSA), the European Aviation Safety Agency (EASA) and the European Medicines Agency (EMA), have in place external channels and procedures for receiving reports on breaches falling within the scope of this Directive, which mainly provide for confidentiality of the identity of the reporting persons. This Directive does not affect such external reporting channels and procedures, where they exist, but will ensure that persons reporting to those bodies, offices or agencies of the Union benefit from common minimum standards of protection throughout the Union.~~

---

27 Cited above.

28 Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, **(**OJ L 122, p. 18**)**.

29 Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC **(OJ L 178, 28.6.2013, p. 66).**

(37) For the effective detection and prevention of breaches of Union law it is vital that the relevant information reaches swiftly those closest to the source of the problem, most able to investigate and with powers to remedy it, where possible. **This requires that reporting persons should first use the internal channels where such channels are available to them and report to their employer. It also** ~~This~~ requires that legal entities in the private and the public sector establish appropriate internal procedures for receiving and following-up on reports. **The obligation to first use the existing internal channels applies also where the legal entity has established them without being required to do so by law.**

(38) For legal entities in the private sector, the obligation to establish internal channels is commensurate with their size and the level of risk their activities pose to the public interest. It should apply to all **companies with more than 50 employees** ~~medium-sized and large entities~~irrespective of the nature of their activities, based on their obligation to collect VAT. As a general rule small and micro undertakings, as defined in Article 2 of the Annex of the Commission Recommendation of 6 May 2003[30] as amended[31], should be exempted from the obligation to establish internal channels. However, following an appropriate risk assessment, Member States may require **also other**~~small~~ undertakings to establish internal reporting channels in specific cases (e.g. due to the significant risks that may result from their activities).

(39) The exemption of small and micro undertakings from the obligation to establish internal reporting channels should not apply to private undertakings **which are currently obliged to establish internal reporting channels by virtue of Union acts referred to in Part II of the Annex** ~~active in the area of financial services Such undertakings should remain obliged to establish internal reporting channels, in line with the current obligations set forth in the Union acquis on financial services~~.

~~[30] **Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).**~~

~~[31] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).~~

(40) It should be clear that, in the case of private legal entities which do not provide for internal reporting channels, reporting persons should be able to report directly externally to the competent authorities and such persons should enjoy the protection against retaliation provided by this Directive.

(41) To ensure in particular, the respect of the public procurement rules in the public sector, the obligation to put in place internal reporting channels should apply to all public legal entities, at local, regional and national level, whilst being commensurate with their size. ~~In cases where internal channels are not provided in small public entities, Member States may provide for internal reporting within a higher level in the administration (that is to say at regional or central level).~~

(42) Provided the confidentiality of the identity of the reporting person is ensured, it is up to each individual private and public legal entity to define the kind of reporting channels to set up~~,~~ ~~such as in person,~~. **More specifically, they should allow for written reports that may be submitted** by post, by physical complaint box(es), ~~by telephone hotline~~ or through an online platform (intranet or internet**) and/or for oral reports that may be submitted by telephone hotline. Upon request by the reporting person, such channels should also allow for physical meetings, within a reasonable time frame.** ~~However, reporting channels should not be limited to those amongst the tools, such as in-person reporting and complaint box(es), which do not guarantee confidentiality of the identity of the reporting person.~~

(43) Third parties may also be authorised to receive reports on behalf of private and public entities, provided they offer appropriate guarantees of respect for independence, confidentiality, data protection and secrecy. These can be external reporting platform providers, external counsel or auditors or trade union representatives.

(43bis) Private and public legal entities which have in place internal reporting channels may designate 'trusted persons' such as trade union representatives who will provide advice to reporting persons and those considering reporting, and who should be under an obligation to maintain the confidentiality of their communications with the aforementioned persons. Without prejudice to the protection trade union representatives enjoy in their capacity as such under other Union and national rules, they should enjoy the protection provided for under this Directive both where they report in their capacity as workers and where they have provided advice and support to the reporting person.

(44) Internal reporting procedures should enable private legal entities to receive and investigate in full confidentiality reports by the employees of the entity and of its subsidiaries or affiliates (the group), but also, to any extent possible, by any of the group's agents and suppliers and by any person who acquires information through his/her work-related activities with the entity and the group.

(45) The most appropriate persons or departments within a private legal entity to be designated as competent to receive and follow-up on reports depend on the structure of the entity, but, in any case, their function should ensure absence of conflict of interest and independence. In smaller entities, this function could be a dual function held by a company officer well placed to report directly to the organisational head, such as a chief compliance or human resources officer, **an integrity officer**, a legal or privacy officer, a chief financial officer, a chief audit executive or a member of the board.

(46) In the context of internal reporting, **informing, as far as legally possible,** the ~~quality and transparency of information provided on~~ **reporting person about** the follow-up ~~procedure~~ to the report is crucial to build trust in the effectiveness of the overall system of whistleblower protection and reduces the likelihood of further unnecessary reports or public disclosures. The reporting person should be informed within a reasonable timeframe about the action envisaged or taken as follow-up to the report **and the grounds for this follow-up** (for instance, **referral to other channels or procedures in cases of reports exclusively affecting individual rights of the reporting person,** closure based on lack of sufficient evidence or other grounds, launch of an internal enquiry**,** and possibly its findings and/or measures taken to address the issue raised, referral to a competent authority for further

investigation) **in** as far as such information would not prejudice the enquiry or investigation or affect the rights of the concerned person. ~~Such reasonable timeframe should not exceed in total three months. Where the appropriate follow-up is still being determined, the reporting person should be informed about this and about any further feedback he or she should expect.~~

(46bis) Such reasonable timeframe should not exceed in total three months. Where the appropriate follow-up is still being determined, the reporting person should be informed about this and about any further feedback he or she should expect.

(47) Persons who are considering reporting breaches of Union law should be able to make an informed decision on whether, how and when to report. Private and public entities having in place internal reporting procedures shall provide information on these procedures as well as on procedures to report externally to relevant competent authorities. Such information must be easily understandable and easily accessible, including, to any extent possible, also to other persons, beyond employees, who come in contact with the entity through their work-related activities, such as service-providers, distributors, suppliers and business partners. For instance, such information may be posted at a visible location accessible to all these persons and ~~to~~ **on** the web of the entity and may also be included in courses and trainings on ethics and integrity.

(48) Effective detection and prevention of breaches of Union law requires ensuring that, where internal reporting channels do not exist, do not function properly or cannot be reasonably expected to function properly, potential whistleblowers can easily and in full confidentiality bring the information they possess to the attention of the relevant competent authorities which are able to investigate and to remedy the problem, where possible.

(48bis) It may be the case that internal channels do not exist or that their use is not mandatory (which may be the case for persons who are not in an employment relationship), or that they were used but did not function properly (for instance the report was not dealt with diligently or within a reasonable timeframe, or no appropriate action was taken to address the breach of law despite the positive results of the enquiry).

(48ter) In other cases, internal channels could not reasonably be expected to function. Examples include cases where the reporting persons have valid reasons to believe i) that they would suffer retaliation in connection with the reporting, including as a result of a breach of their confidentiality; ii) that the ultimate responsibility holder within the work-related context is involved in the breach, that the breach or related evidence may be concealed or destroyed; or that the effectiveness of investigative actions by competent authorities might be jeopardised (examples may be reports on cartel arrangements and other breaches of competition rules) and iii) that urgent action is required for instance because of an imminent risk of a substantial and specific danger to the life, health and safety of persons, or to the environment. In all such cases, persons reporting externally to the competent authorities and, where relevant, to institutions, bodies, offices or agencies of the Union shall be protected. Moreover, protection is also to be granted in cases where Union legislation allows for the reporting person to report directly to the competent national authorities or institutions, bodies, offices or agencies of the Union, for example in the context of fraud against the Union budget, prevention and detection of money laundering and terrorist financing or in the area of financial services. This Directive does not create additional reporting obligations. Rather, it grants protection where Union or national law requires the reporting person to report directly to the competent national authorities for instance as part of their job duties and responsibilities or because the breach is a criminal offence.

(49) Lack of confidence in the usefulness of reporting is one of the main factors discouraging potential whistleblowers. This warrants imposing a clear obligation on competent authorities to **set up appropriate external reporting channels,** to diligently follow-up on the reports received and, within a reasonable timeframe, give feedback to the reporting persons**.** ~~about the action envisaged or taken as follow-up (for instance, closure based on lack of sufficient evidence or other grounds, launch of an investigation and possibly its findings and/or measures taken to address the issue raised; referral to another authority competent to give follow-up) to the extent that such information would not prejudice the investigation or the rights of the concerned persons.~~

(49bis) It is for the Member States to designate the authorities competent to receive and give appropriate follow-up to the reports falling within the scope of this Directive. Such competent authorities may be regulatory or supervisory bodies competent in specific areas concerned or authorities of a more general competence such as law enforcement agencies, anti-corruption bodies or ombudsmen.

(49ter) As recipients of reports, the authorities designated as competent should have the necessary capacities and powers to ensure appropriate follow-up - including assessing the accuracy of the allegations made in the report and addressing the breaches reported by launching an internal enquiry, investigation, prosecution or action for recovery of funds or other appropriate remedial action, in accordance with their mandate, or should have the necessary powers to refer the report to another authority that should investigate the breach reported, ensuring an appropriate follow-up by such authority. With regard to breaches of State aid rules, this is without prejudice to the exclusive power of the Commission as regards the declaration of compatibility of State aid measures in particular pursuant to Article 107(3) TFEU. With regard to breaches of Articles 101 and 102 of the TFEU, Member States should designate as competent authorities those referred to in Article 35 of Regulation (EC) 1/2003 without prejudice to the powers of the Commission in this area.

(49quater) Competent authorities should also give feedback to the reporting persons about the action envisaged or taken as follow-up (for instance, referral to another authority, closure based on lack of sufficient evidence or other grounds or launch of an investigation and possibly its findings and/or measures taken to address the issue raised), as well as about the grounds justifying the follow-up. In criminal proceedings, the obligation to give feedback should not prejudice the investigation or the rights of the concerned persons.

(50) Follow- up and feedback should take place within a reasonable timeframe; this is warranted by the need to promptly address the problem that may be the subject of the report, as well as to avoid unnecessary public disclosures. Such timeframe should not exceed three months, but could be extended to six months, where necessary due to the specific circumstances of the case, in particular the nature and complexity of the subject of the report, which may require a lengthy investigation.

(50bis) Union law in specific areas, such as market abuse[32]**, civil aviation**[33] **or safety of offshore oil and gas operations**[34] **already provides for the establishment of internal and external reporting channels. The obligations to establish such channels laid down in this Directive should build as far as possible on the existing channels provided by specific Union acts.**

(50ter) The European Commission, as well as some bodies, offices and agencies of the Union, such as the European Anti-Fraud Office (OLAF), the European Maritime Safety Agency (EMSA), the European Aviation Safety Agency (EASA) and the European Medicines Agency (EMA), have in place external channels and procedures for receiving reports on breaches falling within the scope of this Directive, which mainly provide for confidentiality of the identity of the reporting persons. This Directive does not affect such external reporting channels and procedures, where they exist, but will ensure that persons reporting to those institutions, bodies, offices or agencies of the Union benefit from common minimum standards of protection throughout the Union.

(50quater) To ensure the effectiveness of the procedures for following up on reports and addressing breaches of the Union rules concerned, Member States should have the possibility to take measures to alleviate burdens for competent authorities resulting from repetitive reports or reports on minor breaches of provisions falling within the scope of this Directive or reports on breaches of ancillary provisions (for instance provisions on documentation or notification obligations). Such measures may consist in allowing competent authorities to prioritise the treatment of reports on serious breaches or breaches of essential provisions falling within the scope of this Directive in cases of high inflows of reports. Member States may also allow competent authorities to close the procedure regarding repetitive reports whose substance does not include any new meaningful information to a past report that was already closed, unless new legal or factual circumstances justify a different follow-up. Furthermore, Member States may allow competent authorities, after a due review of the matter, to decide that

---

[32] **Cited above**.

[33] **Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, (OJ L 122, p. 18).**

[34] **Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC (OJ L 178, 28.6.2013, p. 66).**

a reported breach is clearly minor and does not require follow-up measures pursuant to this Directive. These decisions should be subject to judicial review.

(51) Where provided for under national or Union law, the competent authorities should refer cases or relevant information to relevant institutions, bodies, offices or agencies of the Union, including, for the purposes of this Directive, the European Anti-Fraud Office (OLAF) and the European Public Prosecutor Office (EPPO), without prejudice to the possibility for the reporting person to refer directly to such bodies, offices or agencies of the Union.

(52) In order to allow for effective communication with their ~~dedicated~~ staff **who are responsible for handling reports,** it is necessary that the competent authorities have in place and use ~~specific~~ **user-friendly** channels ~~,~~**which are secure, ensure confidentiality for receiving and handling information provided by the reporting person and enable the storage of durable information to allow for further investigations. This may require that they are separated from the general channels through which the competent authorities communicate with the public, such as normal public complaints systems or channels through which the competent authority communicates internally and with third parties in its ordinary course of business.** ~~separate from their normal public complaints systems, that should be user-friendly and allow for written and oral, as well as electronic and non-electronic reporting.~~

(53) ~~Dedicated s~~**S**taff members of the competent authorities **who are responsible for handling reports should be** ~~, who are~~ professionally trained, including on applicable data protection rules,~~would be necessary~~ in order to handle reports and to ensure communication with the reporting person, as well as **to** follow~~ing~~ up on the report in a suitable manner.

(54) Persons intending to report should be able to make an informed decision on whether, how and when to report. Competent authorities should therefore publicly disclose and make easily accessible information about the available reporting channels with competent authorities, about the applicable procedures and about the ~~dedicated~~**specialised** staff members **responsible for handling** reports within these authorities. All information regarding reports should be transparent, easily understandable and reliable in order to promote and not deter reporting.

(55) Member States should ensure that competent authorities have in place adequate protection procedures for the processing of reports of infringements and for the protection of the personal data of the persons referred to in the report. Such procedures should ensure that the identity of every reporting person, concerned person, and third persons referred to in the report (e.g. witnesses or colleagues) is protected at all stages of the procedure. ~~This obligation should be without prejudice to the necessity and proportionality of the obligation to disclose information when this is required by Union or national law and subject to appropriate safeguards under such laws, including in the context of investigations or judicial proceedings or to safeguard the freedoms of others, including the rights of defence of the concerned person.~~

(56) It is necessary that ~~dedicated~~ staff of the competent authority **who is responsible for handling reports** and staff members of the competent authority who ~~receive~~**have the right to** access to the information provided by a reporting person ~~to the competent authority~~ comply with the duty of professional secrecy and ~~the~~ confidentiality when transmitting the data both inside and outside of the competent authority, including where a competent authority opens an investigation or an inquiry or ~~subsequent~~ **engage in** enforcement activities in connection with the report of infringements.

(57) Member States should ensure the adequate record-keeping of all reports of infringement**s**, and that every report is retrievable within the competent authority and that information received through reports could be used as evidence in enforcement actions where appropriate.

(58) Protection of personal data of the reporting and concerned person is crucial in order to avoid unfair treatment or reputational damages due to disclosure of personal data, in particular data revealing the identity of a person concerned. Hence, in line with the requirements of Regulation (EU) 2016/679 ~~on the protection of~~ **-** ~~natural persons with regard to the processing of~~ personal data ~~and~~**on the free movement of such data** ~~on the free movement of such data~~ (General Data Protection Regulation, hereinafter also referred to as 'GDPR'**)**[35], competent authorities should establish adequate data protection procedures specifically geared to the protection of the reporting person, the concerned person and any third person referred to in the report~~that~~, **which** should include a secure system within the competent authority with restricted access rights for authorised staff only.

(59) The regular review of the procedures of competent authorities and the exchange of good practices between them should guarantee that those procedures are adequate and thus serving their purpose.

(60) ~~To enjoy protection, the reporting persons should reasonably believe, in light of the circumstances and the information available to them at the time of the reporting, that the matters reported by them are true. This reasonable belief should be presumed unless and until proven otherwise. This is an essential safeguard against malicious and frivolous or abusive reports, ensuring that those who deliberately and knowingly report wrong or misleading information do not enjoy protection. At the same time, it ensures that protection is not lost where the reporting person made an inaccurate report in honest error. In a similar vein, reporting persons should be entitled to protection under this Directive if they have reasonable grounds to believe that the information reported falls within its scope.~~

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016, p. 1).

(61) ~~The requirement of a tiered use of reporting channels, as a general rule, is necessary to ensure that the information gets to the persons who can contribute to the early and effective resolution of risks to the public interest as well as to prevent unjustified reputational damage from public disclosure. At the same time, some exceptions to its application are necessary, allowing the reporting person to choose the most appropriate channel depending on the individual circumstances of the case. Moreover, it is necessary to protect public disclosures taking into account democratic principles such as transparency and accountability, and fundamental rights such as freedom of expression and media freedom, whilst balancing the interest of employers to manage their organisations and to protect their interests with the interest of the public to be protected from harm, in line with the criteria developed in the case-law of the European Court of Human Rights[36].~~

(62) ~~As a rule, reporting persons should first use the internal channels at their disposal and report to their employer. However, it may be the case that internal channels do not exist (in case of entities which are not under an obligation to establish such channels by virtue of this Directive or applicable national law) or that their use is not mandatory (which may be the case for persons who are not in an employment relationship), or that they were used but did not function properly (,for instance the report was not dealt with diligently or within a reasonable timeframe, or no action was taken to address the breach of law despite the positive results of the enquiry).~~

36 One of the criteria for determining whether retaliation against whistleblowers making public disclosures interferes with freedom of expression in a way which is not necessary in a democratic society, is whether the persons who made the disclosure had at their disposal alternative channels for making the disclosure; see, for instance, Guja v. Moldova [GC], no 14277/04, ECHR 2008.

(63) ~~In other cases, internal channels could not reasonably be expected to function properly, for instance. where the reporting persons have valid reasons to believe that they would suffer retaliation in connection with the reporting; that their confidentiality would not be protected; that the ultimate responsibility holder within the work-related context is involved in the breach, that the breach might be concealed; that evidence may be concealed or destroyed; that the effectiveness of investigative actions by competent authorities might be jeopardised or that urgent action is required(, for instance because of an imminent risk of a substantial and specific danger to the life, health and safety of persons, or to the environment. In all such cases, persons reporting externally to the competent authorities and, where relevant, to bodies, offices or agencies of the Union shall be protected. Moreover, protection is also to be granted in cases where Union legislation allows for the reporting person to report directly to the competent national authorities or bodies, offices or agencies of the Union, for example in the context of fraud against the Union budget, prevention and detection of money laundering and terrorist financing or in the area of financial services.~~

(64) Persons making a public disclosure ~~directly~~should ~~also~~qualify for protection in cases where, **despite the internal and/or external report made, the** ~~a~~ breach remains unaddressed~~(for example, it was not properly assessed or investigated or no remedial action was taken)despite having been reported internally and/or externally following a tiered use of available channels; or in cases where reporting persons~~, **for instance in cases where such persons have valid reasons to believe that the breach was not (appropriately) assessed or investigated or no appropriate remedial action was taken. The appropriateness of the follow-up should be assessed according to objective criteria, linked to the obligation of the competent authorities to assess the accuracy of the allegations and put an end to any possible breach of Union law. It will thus depend on the circumstances of each case and of the nature of the rules that have been breached.**

(64bis) Persons making a public disclosure directly should also qualify for protection in cases where they have reasonable grounds to believe that there is an imminent or manifest danger for the public interest, or a risk of irreversible damage, including harm to physical integrity, which would not be addressed through internal and/or external reporting.

(64ter) Similarly, such persons should qualify for protection where they have reasonable grounds to believe that there is collusion between the perpetrator of the breach and the competent authority or that the competent authority has been directly or indirectly involved in the breach disclosed, as, in such cases, there is a high risk of retaliation or that evidence may be concealed or destroyed by the competent authority.

(64quater) Safeguarding the confidentiality of the identity of the reporting person during the reporting process and follow-up investigations is an essential ex-ante measure to prevent retaliation. The identity of the reporting person may be disclosed only where this is a necessary and proportionate obligation required by Union or national law with a view to addressing an imminent or irreversible danger for the public interest, or in the context of investigations by authorities or judicial proceedings, in particular to safeguard the rights of defence of the concerned persons. Such an obligation may derive, in particular, from Directive 2012/13 of the European Parliament and of the Council of 22 May 2012, on the right to information in criminal proceedings. The protection of confidentiality should not apply where the reporting person has intentionally revealed his or her identity in the context of a public disclosure.

(65) Reporting persons should be protected against any form of retaliation, whether direct or indirect, taken, **recommended or tolerated** by their employer or customer/recipient of services and by persons working for or acting on behalf of the latter, including co-workers and managers in the same organisation or in other organisations with which the reporting person is in contact in the context of his/her work-related activities~~where retaliation is recommended or tolerated by the concerned person.~~. Protection should be provided against retaliatory measures taken vis-à-vis the reporting person him/herself but also those that may be taken vis-à-vis the legal entity he **or** she ~~represents~~ **is connected to**, such as denial of provision of services, blacklisting or business boycotting. Indirect retaliation also includes actions taken against relatives of the reporting person who are also in a work-related

connection with the latter's employer or customer/recipient of services and workers' representatives who have provided support to the reporting person.

(66) Where retaliation occurs undeterred and unpunished, it has a chilling effect on potential whistleblowers. A clear prohibition of retaliation in law has an important dissuasive effect, further strengthened by provisions for personal liability and penalties for the perpetrators of retaliation.

(67) Potential whistleblowers who are not sure about how to report or whether they will be protected in the end may be discouraged from reporting. Member States should ensure that relevant information is provided in a user-friendly way and is easily accessible to the general public. Individual, impartial and confidential advice, free of charge, should be available on, for example, whether the information in question is covered by the applicable rules on whistleblower protection, which reporting channel may best be used and which alternative procedures are available in case the information is not covered by the applicable rules ('signposting'). Access to such advice can help ensure that reports are made through the appropriate channels, in a responsible manner and that breaches and wrongdoings are detected in a timely manner or even prevented. **Member States may choose to extend such advice to legal counselling.**

(68) **Competent authorities should provide reporting persons with the support necessary for them to effectively access protection. In particular, they should provide proof or other documentation required to confirm before other authorities or courts that external reporting had taken place.** Under certain national frameworks and in certain cases, reporting persons ~~suffering retaliation~~ may benefit from forms of certification of the fact that they meet the conditions of the applicable rules. Notwithstanding such possibilities, they should have effective access to judicial review, whereby it falls upon the courts to decide, based on all the individual circumstances of the case, whether they meet the conditions of the applicable rules.

(69) ~~It should not be possible to waive the rights and obligations established by this Directive by contractual means.~~ Individuals' legal or contractual obligations, such as loyalty clauses in contracts or confidentiality/non-disclosure agreements, cannot be relied on to preclude ~~workers from~~ reporting, to deny protection or to penalise ~~them~~ **reporting persons** for having done so, **where providing the information falling within the scope of such clauses and agreements is necessary for revealing the breach**. **Where these conditions are met, reporting persons should not incur any kind of liability, be it civil, criminal, administrative or employment-related.** ~~At the same time, this Directive should not affect the protection of legal and other professional privilege as provided for under national law.~~

(70) Retaliatory measures are likely to be presented as being justified on grounds other than the reporting and it can be very difficult for reporting persons to prove the link between the two, whilst the perpetrators of retaliation may have greater power and resources to document the action taken and the reasoning. Therefore, once the reporting person demonstrates *prima facie* that he **or** ~~/~~she made a report or **public** disclosure in line with this Directive and suffered a detriment, the burden of proof should shift to the person who took the detrimental action, who should then demonstrate that ~~their~~the action taken was not linked in any way to the reporting or the **public** disclosure.

(71) Beyond an explicit prohibition of retaliation provided in law, it is crucial that reporting persons who do suffer retaliation have access to legal remedies. The appropriate remedy in each case will be determined by the kind of retaliation suffered. It may take the form of actions for reinstatement (for instance, in case of dismissal, transfer or demotion, or of withholding of training or promotion) or for restauration of a cancelled permit, licence or contract; compensation for actual and future financial losses (for lost past wages, but also for future loss of income, costs linked to a change of occupation); compensation for other economic damage**s** such as legal expenses and costs of medical treatment, and for intangible damage (pain and suffering).

(72) The types of legal action may vary between legal systems but they should ensure a **real and effective compensation or reparation, in a way which is dissuasive and proportionate to the detriment suffered. Of relevance in this context are the Principles of the European Pillar of Social Rights, in particular Principle 7 according to which "(p)rior to any dismissal, workers have the right to be informed of the reasons and be granted a reasonable period of notice. They have the right to access to effective and impartial dispute resolution and, in case of unjustified dismissal, a right to redress, including adequate compensation."**~~as full and effective a remedy as possible~~. **The r**emedies **established at national level** should not discourage potential future whistleblowers. For instance, allowing for compensation as an alternative to reinstatement in case of dismissal might give rise to a systematic practice in particular by larger organisations, thus having a dissuasive effect on future whistleblowers.

(73) Of particular importance for reporting persons are interim remedies pending the resolution of legal proceedings that can be protracted. **Particularly, actions of i**~~I~~nterim relief, as **provided for under national law, should also be available to reporting persons** ~~can be in particular necessary~~ in order to stop threats, attempts or continuing acts of retaliation, such as harassment at the workplace, or to prevent **all** forms of retaliation such as dismissal, which might be difficult to reverse after the lapse of lengthy periods and which can ruin financially the individual a perspective which can seriously discourage potential whistleblowers.

(74) Action taken against reporting persons outside the work-related context, through proceedings, for instance, related to defamation, breach of copyright, trade secrets, confidentiality and personal data protection, can also pose a serious deterrent to whistleblowing. **Actions taken against reporting persons outside the work-related context, through proceedings, for instance, related to defamation or breach of copyright, can also pose a serious deterrent to whistleblowing. Also in such proceedings, reporting persons should be able to rely on having made a report or disclosure in accordance with this Directive as a defence, provided that the information reported or disclosed was necessary to reveal the breach. In such cases, the person initiating the proceedings should carry the burden to prove that the reporting person does not meet the conditions of the Directive**.

(74bis) Directive (EU) 2016/943 of the European Parliament and of the Council lays down rules to ensure a sufficient and consistent level of civil redress in the event of unlawful acquisition, use or disclosure of a trade secret. However, it also provides that the disclosure of a trade secret shall be considered lawful to the extent that it is allowed by Union law (Article 3(2)). Persons who disclose trade secrets acquired in a work-related context and whose disclosure is necessary to reveal a breach falling within the substantive scope of this Directive should benefit from the protection granted herein (including the exemption from civil liability), provided that they meet the conditions of this Directive. Before revealing a trade secret, reporting persons should carefully weigh the value of the trade secret or copyrighted work and consider whether there is a more appropriate and adequate alternative. Where these conditions are met, disclosures of trade secrets are to be considered as "allowed" by Union law within the meaning of Article 3(2) of Directive (EU) 2016/943. Directive (EU) 2016/943 should remain applicable for all disclosures of trade secrets falling outside the scope of this Directive. Competent authorities receiving reports including trade secrets should ensure that these are not used or disclosed for other purposes beyond what is necessary for the proper follow-up of the reports.

(75) A significant cost for reporting persons contesting retaliation measures taken against them in legal proceedings can be the relevant legal fees. Although they could recover these fees at the end of the proceedings, they might not be able to cover them up front, especially if they are unemployed and blacklisted. Assistance for criminal legal proceedings, particularly ~~in accordance with~~**where** the ~~provisions~~**reporting persons meet the conditions** of Directive (EU) 2016/1919 of the European Parliament and of the Council[37] and more generally support to those who are in serious financial need might be key, in certain cases, for the effective enforcement of their rights to protection.

(75bis) In view of the key role that trade unions can play in terms of providing advice and support to those who report or consider reporting and of the need to prevent attempts to hinder reporting, it is essential to provide protection against retaliation prompted by the fact that the latter consulted their trade union in connection to reporting. As such consultations do not constitute internal or external reporting or public disclosures, protection against retaliation occurring because of such consultations should not be dependent on the conditions of Article 2bis.

(76) The rights of the concerned person should be protected in order to avoid reputational damages or other negative consequences. Furthermore, the rights of defence and access to remedies of the concerned person should be fully respected at every stage of the procedure following the report, in accordance with Articles 47 and 48 of the Charter of Fundamental Rights of the European Union. Member States should ensure the right of defence of the concerned person, including the right to access to the file, the right to be heard and the right to seek effective remedy against a decision concerning the concerned person under the applicable procedures set out in national law in the context of investigations or subsequent judicial proceedings.

(77) Any person who suffers prejudice, whether directly or indirectly, as a consequence of the reporting or **public** disclosure of inaccurate or misleading information should retain the protection and the remedies available to him or her under the rules of general law. Where such inaccurate or misleading report or **public** disclosure was made deliberately and

---

37 Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297 4.11.2016, p. 1).

knowingly, the concerned persons should be entitled to compensation in accordance with national law.

(78) **Criminal, civil or administrative p**~~P~~enalties are necessary to ensure the effectiveness of the rules on whistleblower protection. Penalties against those who take retaliatory or other adverse actions against reporting persons can discourage further such actions. Penalties against persons who make a report or **public** disclosure demonstrated to be knowingly false are necessary to deter further malicious reporting and preserve the credibility of the system. The proportionality of such penalties should ensure that they do not have a dissuasive effect on potential whistleblowers.

(79) Any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, should be undertaken in accordance with Regulation (EU) 2016/679, and with Directive (EU) 2016/680~~of the European Parliament and of the Council~~[38], and any exchange or transmission of information by Union level competent authorities should be undertaken in accordance with Regulation (EC) No 45/2001~~of the European Parliament and of the Council~~[39]. Particular regard should be had to the principles relating to processing of personal data set out in Article 5 of the GDPR, Article 4 of Directive (EU) 2016/680 and Article 4 of Regulation (EC) No 45/2001, and to the principle of data protection by design and by default laid down in Article 25 of the GDPR, Article 20 of Directive (EU) 2016/680 and Article XX of Regulation (EU) No 2018/XX repealing Regulation No 45/2001 and Decision No 1247/2002/EC.

---

[38] **Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).**

[39] **Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).**

79(bis) The effectiveness of the procedures set out in the present Directive related to following-up on reports on breaches of Union law in the areas falling within its scope serves an important objective of general public interest of the Union and of the Member States, within the meaning of Article 23(1)(e) GDPR, as it aims at enhancing the enforcement of Union law and policies in specific areas where breaches can cause serious harm to the public interest. The effective protection of the confidentiality of the identity of the reporting persons is necessary for the protection of the rights and freedoms of others, in particular those of the reporting persons, provided for under Article 23(1)(i) GDPR. Member States should ensure the effectiveness of this Directive, including, where necessary, by restricting, by legislative measures, the exercise of certain data protection rights of the concerned persons in line with Article 23(1)(e) and (i) and 23(2) GDPR to the extent and as long as necessary to prevent and address attempts to hinder reporting, to impede, frustrate or slow down follow-up to reports, in particular investigations, or attempts to find out the identity of the reporting persons.

79(ter) The effective protection of the confidentiality of the identity of the reporting persons is equally necessary for the protection of the rights and freedoms of others, in particular those of the reporting persons, where reports are handled by by authorities as defined in Article 3(7) of Directive (EU) 2016/680. Member States should ensure the effectiveness of this Directive, including, where necessary, by restricting, by legislative measures, the exercise of certain data protection rights of the concerned persons in line with Articles 13(3)(a) and (e), 15(1)(a) and (e), 16(4)(a) and (e) and Article 31(5) of Directive (EU) 2016/680 to the extent that, and for as long as necessary to prevent and address attempts to hinder reporting, to impede, frustrate or slow down follow-up to reports, in particular investigations, or attempts to find out the identity of the reporting persons.

(80) This Directive introduces minimum standards and Member States should have the power to introduce or maintain more favourable provisions to the reporting person, provided that such provisions do not interfere with the measures for the protection of concerned persons.

(81) In accordance with Article 26(2) TFEU, the internal market needs to comprise an area without internal frontiers in which the free and safe movement of goods and services is ensured. The internal market should provide Union citizens with added value in the form of better quality and safety of goods and services, ensuring high standards of public health and

environmental protection as well as free movement of personal data. Thus, Article 114 TFEU is the appropriate legal basis to adopt the measures necessary for the establishment and functioning of the internal market. In addition to Article 114 TFEU, this Directive should have additional specific legal bases in order to cover the fields that rely on Articles 16,33, 43, 50, 53(1), 62, 91, 100, 103, ~~109~~, 168, 169 **and 192(1)** ~~and 207~~ TFEU and Article 31 of the **Treaty establishing the** ~~Euratom Treaty~~ **European Atomic Energy Community** for the adoption of Union measures. Since this Directive also aims at better protecting the financial interests of the Union, Article 325(4) TFEU should be included as a legal basis.

(82) The ~~material~~**substantive** scope of this Directive is based on the identification of areas where the introduction of whistleblower protection appears justified and necessary on the basis of currently available evidence. Such material scope may be extended to further areas or Union acts, if this proves necessary as a means of strengthening their enforcement in the light of evidence that may come to the fore in the future**,** or on the basis of the evaluation of the way in which this Directive has operated.

(83) Whenever subsequent legislation relevant for this Directive is adopted, it should specify where appropriate that this Directive will apply. Where necessary, Article 1 and the Annex should be amended.

(84) The objective of this Directive, namely to strengthen enforcement in certain policy areas and acts where breaches of Union law can cause serious harm to the public interest through effective whistleblower protection, cannot be sufficiently achieved by the Member States acting alone or in an uncoordinated manner, but can rather be better achieved by Union action providing minimum standards of harmonisation on whistleblower protection. Moreover, only Union action can provide coherence and align the existing Union rules on whistleblower protection. Therefore, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve this objective.

(85) This Directive respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. Accordingly, this Directive must be implemented in accordance with those rights and principles. In particular, this Directive seeks to ensure full respect for freedom of expression and information, the

right to protection of personal data, the freedom to conduct a business, the right to a high level of consumer protection, the right to an effective remedy and the rights of defence.

(86) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001. ~~and delivered an opinion on […]~~[40]

~~40~~ ~~OJ C ….~~

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SCOPE, CONDITIONS FOR PROTECTION AND DEFINITIONS

Article 1

Material scope

1. With a view to enhancing the enforcement of Union law and policies in specific areas, this Directive lays down common minimum standards for the protection of persons reporting on the following **breaches** ~~unlawful activities or abuse of law~~:

   a) breaches falling within the scope of the Union acts set out in the Annex (Part I and Part II) as regards the following areas:

      (i) public procurement;

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

      (iii) product safety;

      (iv) transport safety;

      (v) protection of the environment;

      (vi) nuclear safety;

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

      (viii) public health;

      (ix) consumer protection;

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

b) breaches of Articles 101, 102, 106, 107 and 108 TFEU and breaches falling within the scope of Council Regulation (EC) No 1/2003 and Council Regulation (EU) No 2015/1589;

c) breaches affecting the financial interests of the Union as defined by Article 325 TFEU and as further specified, in particular, in Directive (EU) 2017/1371 and Regulation (EU, Euratom) No 883/2013;

d) breaches relating to the internal market, as referred to in Article 26(2) TFEU, as regards acts which breach the rules of corporate tax or arrangements whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

2. ~~Where specific rules on the reporting of breaches are provided for in sector-specific Union acts listed in Part 2 of the Annex, those rules shall apply. The provisions of this Directive shall be applicable for all matters relating to the protection of reporting persons not regulated in those sector-specific Union acts.~~

Article 1bis

Relationship with other Union acts and national provisions

1. Where specific rules on the reporting of breaches are provided for in sector-specific Union acts listed in Part 2 of the Annex, those rules shall apply. The provisions of this Directive shall be applicable ~~for all matters relating to the protection of reporting persons~~ **to the extent that a matter is not regulated** in those sector-specific Union acts~~, in particular the provisions relating to the protection of reporting persons~~.

1bis. This Directive shall not affect the responsibility of Member States to ensure national security.

2. **This Directive shall not affect the application of Union or national law on:**

a) **the protection of classified information;**

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

c) **the secrecy of judicial deliberations; and**

d) **rules on criminal procedure.**

3. **This Directive shall not apply to cases in which persons registered as informants in national databases report breaches to law enforcement authorities, against reward or compensation, pursuant to procedures that aim at ensuring their anonymity and physical integrity.**

Article 2

Personal scope

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

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

b) persons having the status of self-employed, with**in** the meaning of Article 49 TFEU;

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

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

1bis. **This Directive shall apply to reporting persons also where they report or disclose information acquired in a work-based relationship which has since ended.**

2. This Directive shall also apply to reporting persons whose work-based relationship is yet to begin in cases where information concerning a breach has been **lawfully** acquired during the recruitment process or other pre-contractual negotiation.

Article 2bis

Conditions for protection of reporting persons

1. **Persons reporting information on breaches falling within the scope of this Directive shall qualify for protection provided that:**

a) **they had reasonable grounds to believe that the information reported was true at the time of reporting and that the information fell within the scope of this Directive; and**

b) **they reported internally in accordance with Article 3bis and/or externally in accordance with Article 5bis or publicly disclosed information in accordance with Article 12bis of this Directive.**

2. **Reporting persons who later cease to have a reasonable belief that the information reported was true may not qualify for protection from subsequent retaliation unless they report this new information in due time.**

3. **Without prejudice to existing obligations to provide for anonymous reporting by virtue of Union law, this Directive does not affect the power of Member States to decide whether public entities and competent authorities shall or shall not accept and follow-up on anonymous reports of breaches. Persons who reported or publicly disclosed information anonymously but were subsequently identified shall nonetheless qualify for protection in case they suffer retaliation, provided that they meet the conditions laid down in paragraph 1.**

Article 2ter

Breaches exclusively affecting individual rights

Member States may provide that information on breaches exclusively affecting the individual rights of the reporting person shall not be reported under the procedures of this Directive, but under other available procedures, unless that information reveals a wider pattern of breaches.

Article 3

Definitions

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

(1) 'breaches' means ~~actual or potential~~ unlawful **acts or omissions** ~~activities~~ **that relate** ~~relating~~ **to the Union acts and areas falling within the scope referred to in Article 1 and in the Annex** or **that defeat the object or the purpose of the rules in these Union acts and areas** ~~abuse of law relating to the Union acts and areas falling within the scope referred to in Article 1 and in the Annex~~;

~~(2) 'unlawful activities' means acts or omissions contrary to Union law;~~

~~(3) 'abuse of law' means acts or omissions falling within the scope of Union law which do not appear to be unlawful in formal terms but defeat the object or the purpose pursued by the applicable rules;~~

(4) 'information on breaches' means ~~evidence~~ **information or reasonable suspicions** about actual ~~breaches as well as reasonable suspicions about~~ **or** potential breaches**,** ~~which have not yet materialised~~ **and about attempts to conceal breaches which occurred or are very likely to occur in the organisation at which the reporting person works or has worked or in another organisation with which he or she is or was in contact through his or her work;**

(5) 'report' means the provision of information **on breaches;** ~~relating to a breach which has occurred or is likely to occur in the organisation at which the reporting person works or has~~

~~worked or in another organisation with which he or she is or was in contact through his or her work;~~

(6) 'internal reporting' means provision of information on breaches within a public or private legal entity;

(7) 'external reporting' means provision of information on breaches to the competent authorities;

(8) '**public** disclosure' means making information on breaches ~~acquired within the work-related context~~ available to the public domain;

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

(10) 'work-related context' means current or past work activities in the public or private sector through which, irrespective of their nature, persons may acquire information on breaches and within which these persons may suffer retaliation if they report them.

(11) 'concerned person' means a natural or legal person who is referred to in the report or disclosure as a person to whom the breach is attributed or with which he or she is associated;

(12) 'retaliation' means any ~~threatened or actual~~ act or omission **which occurs in a work-related context,** prompted by the internal or external reporting~~,~~ **or by public disclosure,** ~~which occurs in a work-related context~~ and **which** causes or may cause unjustified detriment to the reporting person **or to a third person connected with or having supported the reporting person, in particular a relative or a trusted person, or to a legal entity connected with the reporting person;**

(13) 'follow-up' means any action taken by the recipient of the report **or any competent authority**, ~~made internally or externally,~~ to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including **through** actions such as internal enquiry, investigation, prosecution, action for recovery of funds and closure;

(13bis) 'feedback' means providing to the reporting persons information on the action envisaged or taken as follow-up to their report and on the grounds for such follow-up.

(14) 'competent authority' means any national authority entitled to receive reports in accordance with Chapter III **and give feedback to the reporting persons** and**/or** designated to carry out the duties provided for in this Directive, in particular as regards the follow-up of reports**;**

(14bis) 'trusted persons' means persons such as trade union representatives designated by private or public entities with a view to providing confidential advice to reporting persons and those considering reporting.

CHAPTER II

INTERNAL REPORTING AND FOLLOW-UP OF REPORTS

Article 3bis

Reporting through internal channels

Without prejudice to Articles 5bis and 12bis, reporting persons shall first provide information on breaches falling within the scope of this Directive using the channels and procedures provided for in Chapter II.

Article 4

Obligation to establish internal channels ~~and procedures for reporting and follow-up of reports~~

1. Member States shall ensure that legal entities in the private and in the public sector establish internal channels and procedures for reporting and following up on reports, following consultations with social partners, if appropriate.

2. Such channels and procedures shall allow for reporting by employees of the entity. They may allow for reporting by other persons who are in contact with the entity in the context of their work-related activities, referred to in Article 2(1)(b),(c) and (d), but the use of internal channels for reporting shall not be mandatory for these categories of persons.

3. The legal entities in the private sector referred to in paragraph 1 ~~are~~ **shall be** those~~the following:~~

~~a) private legal entities~~ with 50 or more employees.

~~b) private legal entities with an annual business turnover or annual balance sheet total of EUR 10 million or more;~~

~~c) private legal entities of any size operating in the area of financial services or vulnerable to money laundering or terrorist financing, as regulated under the Union acts referred to in the Annex.~~

3bis. Reporting channels may be operated internally by a person or department designated for that purpose or provided externally by a third party, provided that the safeguards and requirements referred to in Article 5(1) are respected.

3ter. This Directive shall not affect the obligation to establish internal channels imposed on private legal entities by virtue of Union acts referred to in Part II of the Annex.

4. Following an appropriate risk assessment taking into account the nature of activities of the entities and the ensuing level of risk, Member States may require ~~small~~private legal entities~~, as defined in Commission Recommendation of 6 May 2003[41], other than those referred to in paragraph 3(c)~~ **with less than 50 employees** to establish internal reporting channels and procedures.

5. Any decision taken by a Member State ~~pursuant to paragraph 4~~ **to require the private legal entities to establish internal reporting channels pursuant to paragraph 4** shall be notified to the Commission, together with a justification and the criteria used in the risk assessment. The Commission shall communicate that decision to the other Member States.

6. The legal entities in the public sector referred to in paragraph 1 shall be **all the branches of State power at all territorial levels, including entities owned or controlled by the State.** ~~the following:~~

~~a) state administration;~~

~~[41] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises OJ L 124, 20.5.2003, p. 36.~~

~~b) regional administration and departments;~~

~~c) municipalities with more than 10 000 inhabitants;~~

~~d) other entities governed by public law.~~

Member States may exempt from the obligation referred to in paragraph 1 municipalities with less than 10 000 inhabitants or less than 50 employees, or other public entities with less than 50 employees.

Member States may provide that internal reporting channels are shared between municipalities, or operated by joint municipal authorities established by law, provided that the shared internal channels are distinct and autonomous from the external channels.

Article 5

Procedures for internal reporting and follow-up of reports

1. The procedures for reporting and following-up of reports referred to in Article 4 shall include the following:

   a) channels for receiving the reports which are designed, set up and operated in a manner that ensures the confidentiality of the identity of the reporting person and prevents access to non-authorised staff members;

   b) the designation of a person or department competent for following up on the reports **which may be the same person or department as the one receiving the reports; additional persons such as trade union representatives may be designated as trusted persons**;

   c) diligent follow-up to the report by the designated person or department;

   d) a reasonable timeframe, not exceeding three months following the report, to provide feedback to the reporting person about the follow-up to the report;

   e) clear and easily accessible information regarding the procedures and information on how and under what conditions reports can be made externally to competent

authorities pursuant to Article **5bis** ~~13(2)~~ and, where relevant, to **institutions,** bodies, offices or agencies of the Union.

1bis. **Member States may provide that, in the event of high inflows of reports, the designated persons or departments may deal with reports on serious breaches or on breaches of essential provisions falling within the scope of this Directive as a matter of priority.**

2. The channels provided for in point (a) of paragraph 1 shall allow for reporting in **writing and/or orally, through telephone lines, and, upon request, by means of a physical meeting within a reasonable timeframe.**

~~all of the following ways:~~

~~(a) written reports in electronic or paper format and/or oral report through telephone lines, whether recorded or unrecorded;~~

~~(b) physical meetings with the person or department designated to receive reports.~~

~~Reporting channels may be operated internally by a person or department designated for that purpose or provided externally by a third party, provided that the safeguards and requirements referred to in point (a) of paragraph 1 are respected.~~

3. ~~The person or department referred to in point (b) of paragraph 1 may be the same person who is competent for receiving the reports. Additional persons may be designated as "trusted persons" from whom reporting persons and those considering reporting may seek confidential advice.~~

CHAPTER III

EXTERNAL REPORTING AND FOLLOW-UP OF REPORTS

Article 5bis

Reporting through external channels

1. **A person who reports externally information on breaches shall qualify for protection if one of the following conditions is fulfilled:**

a) **he or she first reported internally but no appropriate action was taken in response to the report within the reasonable timeframe referred in Article 5;**

b) **internal reporting channels were not available for the reporting person or the reporting person could not reasonably be expected to be aware of the availability of such channels;**

c) **the use of internal reporting channels was not mandatory for the reporting person, in accordance with Article 4(2);**

d) **he or she could not reasonably be expected to use internal reporting channels in light of the particular circumstances of the case, in particular, the high risk of retaliation or the low prospect of the breach being effectively addressed in that case;**

e) **he or she had reasonable grounds to believe that the use of internal reporting channels could jeopardise the effectiveness of investigative actions by competent authorities;**

f) **he or she was entitled to report directly through the external reporting channels to a competent authority by virtue of Union law;**

g) **he or she was under an obligation to report directly through the external reporting channels to a competent authority by virtue of Union or national law.**

2. **A person reporting to relevant institutions, bodies, offices or agencies of the Union on breaches falling within the scope of this Directive shall qualify for protection as laid down in this Directive under the same conditions as a person who reported externally in accordance with the conditions set out in paragraph 1.**

Article 6

Obligation to establish external reporting channels and to follow-up on reports

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

2. Member States shall ensure that the competent authorities:

   a) establish independent and autonomous external reporting channels, which are both secure and ensure confidentiality, for receiving and handling information provided by the reporting person;

   abis) promptly acknowledge, as provided for in national procedural rules, the receipt of written reports to the postal or electronic address indicated by the reporting person, unless the reporting person explicitly requested otherwise or the competent authority reasonably believes that acknowledging receipt of a written report would jeopardise the protection of the reporting person's identity;

   ater) follow-up on the reports by taking the necessary measures and investigate, to the extent appropriate, the subject-matter of the reports;

   b) give feedback to the reporting person about the follow-up of the report within a reasonable timeframe not exceeding three months or six months in duly justified cases. **The competent authorities shall communicate to the reporting person the final outcome of the investigations, in accordance with the procedures provided for under national law;**~~;~~

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

3. ~~Member States shall ensure that competent authorities follow-up on the reports by taking the necessary measures and investigate, to the extent appropriate, the subject-matter of the reports. The competent authorities shall communicate to the reporting person the final outcome of the investigations.~~

4. ~~Member States shall ensure that any authority which has received a report but does not have the competence to address the breach reported transmits it to the competent authority~~

~~and that the reporting person is informed.~~ **Member States may provide that, in the event of high inflows of reports, competent authorities may deal with reports on serious breaches or breaches of essential provisions falling within the scope of this Directive as a matter of priority.**

5. **Competent authorities may close the procedure regarding repetitive reports whose substance does not include any new meaningful information compared to a past report that was already closed, unless new legal or factual circumstances justify a different follow-up. In such a case, they shall inform the reporting person about the grounds f or their decision, which shall be subject to judicial review.**

6. **After having duly reviewed the matter, competent authorities may decide that a reported breach is clearly minor and does not require follow-up measures pursuant to this Directive. This shall not affect other obligations or other applicable procedures to address the reported breach, or the protection granted by this Directive in relation to reporting through the internal and/or external channels. In such a case, the competent authorities shall notify their decision and its grounds to the reporting person. This decision shall be subject to judicial review.**

7. **Member States shall ensure that any authority which has received a report but does not have the competence to address the breach reported transmits it to the competent authority and that the reporting person is informed.**

Article 7

Design of external reporting channels

1. ~~Dedicated e-~~ **E**xternal reporting channels shall be considered independent and autonomous, if they meet all of the following criteria:

~~a) they are separated from general communication channels of the competent authority, including those through which the competent authority communicates internally and with third parties in its ordinary course of business;~~

~~b~~**a**) they are designed, set up and operated in a manner that ensures the completeness, integrity and confidentiality of the information and prevents access to non-authorised staff members of the competent authority;

b~~c~~) they enable the storage of durable information in accordance with Article 11 to allow for further investigations.

2. The ~~dedicated~~**external** reporting channels shall allow for ~~at least all of the following ways:~~ **reporting in writing and orally through telephone lines, and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe.**

~~a) written report in electronic or paper format;~~

~~b) oral report through telephone lines, whether recorded or unrecorded;~~

~~c) physical meeting with dedicated staff members of the competent authority.~~

3. Competent authorities shall ensure that a report received by means other than ~~dedicated~~ **the** reporting channels referred to in paragraphs 1 and 2 is promptly forwarded without modification to the ~~dedicated~~ staff members **responsible for handling reports.** ~~of the competent authority by using dedicated communication channels~~.

4. Member States shall establish procedures to ensure that, where a report being initially addressed to a person who has not been designated as responsible handler for reports that person is refrained from disclosing any information that might identify the reporting or the concerned person.

~~*Article 8*~~

~~**Dedicated s**~~**Staff members ~~responsible for handling reports~~**

5. Member States shall ensure that competent authorities have staff members **responsible for** ~~to~~ handling reports**, and ~~in particular for:~~** ~~Dedicated~~**Those** ~~staff members shall receive specific training for the purposes of handling reports.~~

~~Dedicated staff members shall exercise the following functions:~~

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

b) receiving and following-up reports;

c) maintaining contact with the reporting person for the purpose of ~~informing the reporting person of the progress and the outcome of the investigation~~**providing feedback**.

6. These staff members shall receive specific training for the purposes of handling reports.

Article 9

Procedures applicable to external reporting

1. The procedures applicable to external reporting shall provide for the following:

   a) the manner in which the competent authority may requ**est**~~ire~~ the reporting person to clarify the information reported or to provide additional information that is available to the reporting person;

   b) ~~a reasonable~~ **the** timeframe~~, not exceeding three months or six months in duly justified cases,~~ for giving feed-back to the reporting person ~~about the follow-up of the report~~ and the type and content of this feed-back;

   c) the confidentiality regime applicable to reports**.**~~,including a detailed description of the circumstances under which the confidential data of a reporting person may be disclosed.~~

2. ~~The detailed description referred to in point (c) of paragraph 1 shall include the exceptional cases in which confidentiality of personal data may not be ensured, including where the disclosure of data is a necessary and proportionate obligation required under Union or national law in the context of investigations or subsequent judicial proceedings or to safeguard the freedoms of others including the right of defence of the concerned person, and in each case subject to appropriate safeguards under such laws.~~

3. ~~The detailed description referred to in point (c) of paragraph 1 must be written in clear and easy to understand language and be easily accessible to the reporting persons.~~

Article 10

Information regarding the receipt of reports and their follow-up

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

a) the conditions under which reporting persons qualify for protection under this Directive;

b) the **contact details for using the external reporting channels as provided for under Article 7(2), in particular** ~~communication channels for receiving and following up the reporting:~~

~~i) the phone numbers, indicating whether conversations are recorded or unrecorded when using those phone lines;~~

~~ii)~~ **the** ~~dedicated~~ electronic and postal addresses, **and, where applicable, the phone numbers, indicating whether conversations are recorded or unrecorded when using those phone lines.**~~which are secure and ensure confidentiality, to contact the dedicated staff members responsible for handling reports~~;

c) the procedures applicable to the reporting of breaches referred to in Article 9;

d) the confidentiality regime applicable to reports, and in particular the information in relation to the processing of personal data in accordance with Article 13 of Regulation (EU) 2016/679, Article 13 of Directive (EU) 2016/680 and Article 11 of Regulation (EC) 45/2001, as applicable.

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

f) the remedies and procedures available against retaliation and possibilities to receive confidential advice for persons contemplating making a report;

g) a statement clearly explaining **the conditions under which** ~~that~~persons ~~making information available~~**reporting** to the competent authority ~~in accordance with this Directive~~**would** ~~are~~not **incur liability due to a breach of confidentiality as provided for in Article 15(4).** ~~considered to be infringing any restriction on disclosure of information imposed by contract~~

~~or by any legislative, regulatory or administrative provision, and are not to be involved in liability of any kind related to such disclosure.~~

Article 11

Record-keeping of reports received

1. Member States shall ensure that competent authorities keep records of every report received.

2. ~~Competent authorities shall promptly acknowledge the receipt of written reports to the postal or electronic address indicated by the reporting person, unless the reporting person explicitly requested otherwise or the competent authority reasonably believes that acknowledging receipt of a written report would jeopardise the protection of the reporting person's identity.~~

3. Where a recorded telephone line is used for reporting, subject to the consent of the reporting person, the competent authority shall have the right to document the oral reporting in one of the following ways:

   a) a recording of the conversation in a durable and retrievable form;

   b) a complete and accurate transcript of the conversation prepared by the ~~dedicated~~ staff members of the competent authority **responsible for handling reports**.

   The competent authority shall offer the possibility to the reporting person to check, rectify and agree the transcript of the call by signing it.

4. Where an unrecorded telephone line is used for reporting, the competent authority shall have the right to document the oral reporting in the form of accurate minutes of the conversation prepared by the ~~dedicated~~staff members **responsible for handling reports**. The competent authority shall offer the possibility to the reporting person to check, rectify and agree with the minutes of the call by signing them.

5. Where a person requests a meeting with the ~~dedicated~~staff members of the competent authority for reporting according to Article 7(2)(c), competent authorities shall ensure, subject to the consent of the reporting person, that complete and accurate records of the meeting are kept in a durable and retrievable form. A competent authority shall have the right to document the records of the meeting in one of the following ways:

a) a recording of the conversation in a durable and retrievable form;

b) accurate minutes of the meeting prepared by the ~~dedicated~~ staff members of the competent authority **responsible for handling reports**.

The competent authority shall offer the possibility to the reporting person to check, rectify and agree with the minutes of the meeting by signing them.

Article 12

Review of the procedures by competent authorities

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

CHAPTER IIIBIS

PUBLIC DISCLOSURES

Article 12bis

Public disclosures

1. A person who publicly discloses information on breaches falling within the scope of this Directive shall qualify for protection under this Directive if one of the following conditions is fullfilled:

a) he or she first reported internally and/or externally in accordance with Chapters II and III but no appropriate action was taken in response to the report within the timeframe referred to in Articles 6(2)(b) and 9(1)(b); or

b) he or she had reasonable grounds to believe that:

(i) there is a low prospect of the breach being effectively addressed through the use of internal and/or external channels and the breach may constitute an imminent or manifest danger for the public interest or a risk of irreversible damage; or

(ii) the competent authority is in collusion with the perpetrator of the breach or involved in the breach.

2. Paragraph 1(a) shall not apply to public disclosures made after a competent authority has taken a decision pursuant to Article 6(7). This shall not affect the protection granted by this Directive against retaliation occurring prior to the public disclosure.

3. This Article shall not apply to public disclosures of information that constitute a serious threat to national security.

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

~~**CHAPTER IV**~~

~~**PROTECTION OF REPORTING AND CONCERNED PERSONS**~~

~~*Article 13*~~

~~**Conditions for the protection of reporting persons**~~

~~1. A reporting person shall qualify for protection under this Directive provided he or she has reasonable grounds to believe that the information reported was true at the time of reporting and that this information falls within the scope of this Directive.~~

~~2. A person reporting externally shall qualify for protection under this Directive where one of the following conditions is fulfilled :~~

~~a) he or she first reported internally but no appropriate action was taken in response to the report within the reasonable timeframe referred in Article 5;~~

~~b) internal reporting channels were not available for the reporting person or the reporting person could not reasonably be expected to be aware of the availability of such channels;~~

~~c) the use of internal reporting channels was not mandatory for the reporting person, in accordance with Article 4(2);~~

~~d) he or she could not reasonably be expected to use internal reporting channels in light of the subject-matter of the report;~~

~~e) he or she had reasonable grounds to believe that the use of internal reporting channels could jeopardise the effectiveness of investigative actions by competent authorities;~~

~~f) he or she was entitled to report directly through the external reporting channels to a competent authority by virtue of Union law.~~

~~3. A person reporting to relevant bodies, offices or agencies of the Union on breaches falling within the scope of this Directive shall qualify for protection as laid down in this Directive under the same conditions as a person who reported externally in accordance with the conditions set out in paragraph 2.~~

~~4. A person publicly disclosing information on breaches falling within the scope of this Directive shall qualify for protection under this Directive where:~~

~~a) he or she first reported internally and/or externally in accordance with Chapters II and III and paragraph 2 of this Article, but no appropriate action was taken in response to the report within the timeframe referred to in Articles 6(2)(b) and 9(1)(b); or~~

~~b) he or she could not reasonably be expected to use internal and/or external reporting channels due to imminent or manifest danger for the public interest, or to the particular circumstances of the case, or where there is a risk of irreversible damage.~~

CHAPTER IVBIS

PROTECTION OF REPORTING AND CONCERNED PERSONS

Article 13bis

Duty of confidentiality

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

2. **By derogation to paragraph 1, the identity of the reporting person and any other information referred to in paragraph 1 may be disclosed only where this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defence of the concerned person, or for the purposes of addressing an imminent or irreversible damage to the public interest. Such disclosures shall be subject to appropriate safeguards under the applicable rules. In particular, the reporting person shall be informed before his or her identity is disclosed, unless such information would jeopardise the investigations or judicial proceedings, where relevant.**

3. **Member States shall ensure that competent authorities receiving reports including trade secrets do not use or disclose them for other purposes beyond what is necessary for the proper follow-up of the reports.**

Article 13ter

Processing of personal data

Any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, shall be made in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Any exchange or transmission of information by Union institutions, bodies, offices and agencies should be undertaken in accordance with Regulation (EU) 2018/725. Personal data which are not relevant for following-up on a report or providing protection for the reporting person in a specific case shall be immediately deleted.

Article 14

Prohibition of retaliation against reporting persons

Member States shall take the necessary measures to prohibit any form of retaliation, **including threats and attempts of retaliation,** whether direct or indirect, ~~against reporting persons meeting the conditions set out in Article 13 or to third persons connected with or having supported the reporting persons, such as relatives or trade union representatives~~, including in particular in the form of:

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

b) demotion or withholding of promotion;

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

d) withholding of training;

e) negative performance assessment or employment reference;

f) imposition or administering of any discipline, reprimand or other penalty, including a financial penalty;

g) coercion, intimidation, harassment or ostracism at the workplace;

h) discrimination, disadvantage or unfair treatment;

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

j) failure to renew or early termination of the temporary employment contract;

k) damage, including to the person's reputation, or financial loss, including loss of business and loss of income;

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

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

n) cancellation of a licence or permit.

Article 15

Measures for the protection of reporting persons against retaliation

1. Member States shall take the necessary measures to ensure the protection of reporting persons meeting the conditions set out in Article ~~13~~**2bis** against retaliation. Such measures shall include, in particular, those set out in paragraphs 2 to 8.

2. Comprehensive and independent information and advice shall be easily accessible to the public, free of charge, on procedures and remedies available on protection against retaliation. **Member States may decide to extend such advice to legal counselling.**

3. Reporting persons shall have access to effective assistance from competent authorities before any relevant authority involved in their protection against retaliation, including, where provided for under national law, certification of the fact that they qualify for protection under this Directive.

4. **Without prejudice to Article 1bis (1bis) and (2), p**~~P~~persons **making a report** ~~reporting externally to competent authorities~~ or ~~making~~ a public disclosure in accordance with this Directive shall not be considered to have breached any restriction on disclosure of information, and **shall not** incur liability of any kind in respect of such **reporting or** disclosure, **provided that they had reasonable grounds to believe that the reporting or**

disclosure of such information was necessary for revealing a breach pursuant to this Directive.

Any other possible liability of the reporting person arising from the unlawful access to information related to the reporting or from acts or omissions which are unrelated to the reporting or are not necessary for revealing a breach pursuant to this Directive shall remain governed by applicable Union or national law.

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

6. Reporting persons shall have access to remedial measures against retaliation as appropriate, including interim relief pending the resolution of legal proceedings, in accordance with the national framework.

7. In ~~addition to the exemption from measures, procedures and remedies provided for in Directive (EU) 2016/943, in~~ judicial proceedings, including for defamation, breach of copyright, breach of ~~secrecy~~ **data protection rules, disclosure of trade secrets**, or for compensation requests based on private, public, or on collective labour law, ~~reporting persons~~ **persons reporting or making a public disclosure in accordance with this Directive** shall **not incur liability of any kind for that reporting or disclosure, and the case against them shall be dismissed, provided that they had reasonable grounds to believe that the reporting or disclosure was necessary for revealing a breach pursuant to this Directive. Where a person reports or publicly discloses information on breaches falling within the scope of this Directive which includes alleged trade secrets and meets the conditions of this Directive, such reporting or public disclosure shall be considered lawful under the conditions of Article 3(2) of the Directive (EU) 2016/943.**~~have the right to rely on having made a report or disclosure in accordance with this Directive to seek dismissal.~~

8. In addition to providing legal aid ~~to reporting persons~~ in criminal and in cross-border civil proceedings in accordance with Directive (EU) 2016/1919 and Directive 2008/52/EC of the European Parliament and of the Council[42], and in accordance with national law, Member States may provide for further measures of legal and financial assistance and support for reporting persons in the framework of legal proceedings.

Article 15bis

Protection against retaliation of persons having consulted trade unions

The provisions of Articles 14 and 15 shall apply also to persons who consult their trade union in connection to reporting and suffer retaliation because of this consultation. In such cases, the conditions laid down in Article 2bis are not applicable.

Article 16

Measures for the protection of concerned persons

1. Member States shall ensure **in accordance with the Charter of Fundamental Rights of the European Union** that the concerned persons fully enjoy the right to an effective remedy and to a fair trial as well as the presumption of innocence and the rights of defence, including the right to be heard and the right to access their file, ~~in accordance with the Charter of Fundamental Rights of the European Union~~**without prejudice to Articles 13bis and 13ter**.

2. Where the identity of the concerned persons is not known to the public, competent authorities shall ensure that their identity is protected for as long as the investigation is ongoing.

3. The procedures set out in Articles 9 and 11 shall also apply for the protection of the identity of the concerned persons.

---

42 Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters (OJ L 136, 24.5.2008, p. 3).

Article 17

Penalties

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

   a) hinder or attempt to hinder reporting;

   b) take retaliatory measures against reporting persons;

   c) bring vexatious proceedings against reporting persons;

   d) breach the duty of maintaining the confidentiality of the identity of reporting persons.

2. Member States shall provide for effective, proportionate and dissuasive penalties applicable to persons **knowingly** making ~~malicious or abusive~~ **false** reports or **false public** disclosures, including measures for compensating persons who have suffered damage from ~~malicious or abusive~~ **such** reports or disclosures.

~~*Article 18*~~

~~**Processing of personal data**~~

~~Any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, shall be made in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Any exchange or transmission of information by competent authorities at Union level should be undertaken in accordance with Regulation (EC) No 45/2001. Personal data which are not relevant for the handling of a specific case shall be immediately deleted.~~

CHAPTER V

FINAL PROVISIONS

Article 19

More favourable treatment

Member States may introduce or retain provisions more favourable to the rights of the reporting persons than those set out in this Directive, without prejudice to Article 16 and Article 17(2).

Article 20

Transposition and transitional period

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by ~~15 May 2021~~**[2 years after adoption]**, at the latest. They shall forthwith communicate to the Commission the text of those provisions.

1bis **By derogation from paragraph 1, Member States may postpone the application of Article 4(3) and provide that the obligation therein shall only apply to legal entities in the private sector whose employees number between 50 and 249 from *[2 years after transposition].***

2. When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

Article 21

Reporting, evaluation and review

1. Member States shall provide the Commission with all relevant information regarding the implementation and application of this Directive. On the basis of the information provided, the Commission shall, by **[2 years after transposition]**~~15 May 2023~~, submit a report to the European Parliament and the Council on the implementation and application of this Directive.

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

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

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

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

3. The Commission shall, by **[4 years after transposition]**~~15 May 2027~~, taking into account its report submitted pursuant to paragraph 1 and the Member States' statistics submitted pursuant to paragraph 2, submit a report to the European Parliament and to the Council assessing the impact of national law transposing this Directive. The report shall evaluate the way in which this Directive has operated and consider the need for additional measures, including, where appropriate, amendments with a view to extending the scope of this Directive to further ~~areas or~~Union acts **or areas, in particular the improvement of the working environment to protect workers' health and safety and working conditions.**

Article 22

Entry into force

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

Article 23

Addressees

This Directive is addressed to the Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*