Whistleblower Protection Compliance Tool

EU Directive Compliance (EUDC)

A

99%

The highest possible score, indicating full to almost full compliance with the requirements outlined in the EU Directive.

Section Scores (Uncapped)

What is covered?	23/23 (100%)
Who is covered?	19.5/19.5 (100%)
Reporting Channels	43/44 (98%)
Support and Legal Protections	36/36 (100%)
Review and Evaluation	13/13 (100%)

International Standards Conformance (ISC)

B

52%

The proposed draft covers most of the elements recommended in international best practice standards. Consider review of the legislative proposal to meet those standards in full.

Section Scores (Uncapped)

What is covered?	8/14 (57%)
Who is covered?	6.5/14 (46%)
Reporting Channels	9/21 (43%)
Support and Legal Protections	12.5/17.5 (71%)
Review and Evaluation	3/8 (38%)

COVID-19 Whistleblower Scenarios

D

67%

The proposed draft would fail to protect whistleblowers in many of our scenarios.

Section Scores (Uncapped)

COVID-19 Scenarios	4/6 (67%)

Results Key

After each answer is *[survey_name] (question_score) {caps}*

- survey_name
  - EUDC = EU Directive Compliance (EUDC)
  - ISC = International Standards Conformance (ISC)
  - COVID = COVID-19 Whistleblower Scenarios
- question_score
  - The value the answer contributes to the total score. The value could be negative.
- caps
  - The ID of any caps on the overall result that have been triggered.

What is covered?

Is it clear that a whistleblower can make a report about any of the following subjects?

- [x] Public procurement *[EUDC] (1)*
- [x] Financial services *[EUDC] (1)*
- [x] Money laundering *[EUDC] (1)*
- [x] Terrorist financing *[EUDC] (1)*
- [x] Product safety and compliance *[EUDC] (1)*
- [x] Transport safety *[EUDC] (1)*
- [x] Nuclear safety and radiation protection *[EUDC] (1)*
- [x] Environmental protection *[EUDC] (1)*
- [x] Food and feed safety *[EUDC] (1)*
- [x] Animal health and welfare *[EUDC] (1)*
- [x] Public health *[EUDC] (1)*
- [x] Data protection *[EUDC] (1)*
- [x] Network security *[EUDC] (1)*
- [x] Misuse of EU funds *[EUDC] (1)*
- [x] Competition rules *[EUDC] (1)*
- [x] Tax avoidance *[EUDC] (1)*
- [x] Working conditions *[ISC] (1)*
- [x] Health and safety at work *[ISC] (1)*
- [x] Education *[ISC] (1)*
- [ ] Policing *[ISC] (1)*
- [ ] Defence *[ISC] (1)*
- [ ] Intelligence *[ISC] (1)*
- [ ] Anything else *[ISC] (1)*

EUDC Feedback

The EU Directive adopts a broad, horizontal approach that ties whistleblower protection to the working of the Single Market and matters affecting the financial interests of the Union. This means that the Directive comes close to covering everything the EU could legislate on.

See Directive 2(1)

ISC Feedback

Issues outside of EU competence are not covered by the Directive, and the decision to extend reportable wrongdoing on other matters is reserved to EU Member States. The Directive includes an explicit carve out for national security matters. Nevertheless, the Directive is clear that it should be regarded as a minimum standard and that Member States can provide stronger and more expansive protections if they wish.

Best practice is to ensure that all whistleblowers, including in the national security, police and intelligence sectors, do have some form of recourse, whether that be to a specialised internal mechanism or to an oversight institution.

See Directive 2(2), 3(2), 3(3)

Can a whistleblower report a breach of any of the following?

- [x] EU regulations that apply directly on the national level *[EUDC] (1)*
- [x] National laws or regulations that give effect to EU Directives *[EUDC] (1)*
- [x] National laws on subjects covered by EU Directives that go beyond what the EU requires *[ISC] (1)*
- [x] Other national laws *[ISC] (1)*
- [ ] Codes of ethics, professional guidelines and other rules of conduct *[ISC] (1)*
- [x] Local or regional laws *[ISC] (1)*
- [x] International law *[ISC] (1)*

EUDC Feedback

To look at the limits of the Directive from another angle, strictly speaking it covers only EU regulations and those Directives which have been applied in national law.

See Directive 2(1)

ISC Feedback

The Directive encourages Member States to go over and above what is required. In order to ensure that the scope of whistleblower protections are intelligible to non-specialists, they should be extended to cover matters covered in national legislation only.

Member States may also wish to consider whether whistleblower reports about breaches of ethics codes and similar standards that do not have legal status should be protected.

Which of the following constitutes a breach?

- [x] Illegal acts *[EUDC] (1)*
- [x] Legal acts that go against the purpose of a law/regulation *[EUDC] (1)*
- [x] Not complying with the law *[EUDC] (1)*
- [x] Mismanagement that undermines an organisation's mission *[EUDC] (1)*
- [ ] Waste or incurring unnecessary costs *[ISC] (1)*
- [x] Attempts to conceal any of the above *[EUDC] (1)*

EUDC Feedback

The Directive defines a breach as an act or omission that is either unlawful or defeats the object or purpose of the law. Omissions in this sense should include purposeful omissions (not enforcing regulations) as well as non-purposeful ones (negligence). Protection extents to information on potential breaches or efforts to cover them up.

See Directive 5(1), 5(2)

ISC Feedback

Waste and inefficiencies do not necessarily result from negligence and are an example of issues that may well form the subject matter of valuable reports but are not explicitly covered by the Directive. This may be an area where Member States or individual organisations wish to expand on the Directive standards.

In any case, the Directive provides that a whistleblower is entitled to protection if they had reasonable grounds to believe that their report was within the scope of the Directive.

See Directive 6(1)(a)

Can a whistleblower make a report about something that happened in another country?

- (●) Yes *[ISC] (1)*
- ( ) No *[ISC] (0)*

ISC Feedback

While there is no explicit language in the Directive about reports with cross border implications, it is clear from implication that these should be covered, at least where the other country is also an EU Member State.

See Directive 6(4), 20(1)(c), 27(3)

Who is covered?

Would any of the following be protected for making a whistleblowing report, regardless of whether they work in the public or private sector?

- [x] Employees *[EUDC] (1)*
- [x] Self-employed contractors *[EUDC] (1)*
- [x] Shareholders *[EUDC] (1)*
- [x] Members of an organisation's supervisory or management body *[EUDC] (1)*
- [x] Non-executive directors *[EUDC] (1)*
- [x] Volunteers *[EUDC] (1)*
- [x] Trainees *[EUDC] (1)*
- [x] Subcontractors and anyone working under their supervision *[EUDC] (1)*
- [x] Suppliers and anyone working under their supervision *[EUDC] (1)*
- [x] Former employees *[EUDC] (1)*
- [x] People going through a recruitment process *[EUDC] (1)*
- [x] Journalists and media organisations *[EUDC] (1)*
- [x] Public service users *[ISC] (1)*
- [x] Relatives of public service users *[ISC] (1)*
- [ ] Members of the public *[ISC] (1)*

EUDC Feedback

The personal scope of the Directive is very broad and covers anyone who acquires information on breaches in a work-related context – that includes shareholders, former employees, volunteers and those going through a recruitment process. "Work-related context" should be interpreted broadly: it does not matter what the nature of those activities are.

See Directive 4(1), 4(2), 5(9)

ISC Feedback

The requirement for information to have been acquired in the context of work activities does, nevertheless, means that the Directive falls short of protecting all citizens. A hospital patient would not be covered, nor someone who witnesses a wrongful arrest. Some proposals recommend extending coverage in this area. Whistleblowing schemes that are open to the public already exist in some EU Member States, such as France and Spain.

France: Loi Sapin II https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033558528&categorieLien=id

Spain: Ley, de la Generalitat, de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana / General Law on the Antifraud Agency of the Community of Valencia https://www.antifrau.cat/sites/default/files/noticies/20161118-agencia-prevencio-contra-frau-valencia.pdf

Does a whistleblower have to be in a working relationship with the subject of their report?

- ○ Yes *[ISC] (0)*
- ◉ No *[ISC] (1)*

ISC Feedback

The Directive requires that someone making a report should have acquired that information in the course of their work-related activities and that the information concerns an organisation they are or have been in contact with.

There is no requirement for a whistleblower to be in a direct working relationship with the subject of their report, or to have been in one in the past.

See Directive 5(2), 5(9)

Which of the following should be the case in order for a whistleblower to be protected?

- [ ] They are acting in good faith *[EUDC] (-1)*
- [x] Their motive is irrelevant *[EUDC] (1)*
- [x] They have reasonable grounds to believe the information they are reporting is true *[EUDC] (1)*
- [x] They have reasonable grounds to believe they are reporting evidence of alleged misconduct *[EUDC] (1)*
- [ ] They can prove their allegations *[EUDC] (-1)*

EUDC Feedback

Good faith requirements are onerous for whistleblowers and their absence from the Directive is deliberate. Neither are whistleblowers required to establish their allegations to a legal standard of proof.

A whistleblower is required only to have reasonable grounds to believe that the information in their report is true. If an investigation later determines that a report is not well-founded, the person who made that report does not lose their entitlement to protection.

Knowingly false reports or public disclosures are not protected by the Directive and may be subject to penalties.

See Directive 6(1), 23(2)

See Directive Recital 32

Is a whistleblower protected if have to they break the law in order to make their report?

- Yes *[ISC] (1)*
- No *["EUDC","ISC"] (0)*
- Partly *["EUDC","ISC"] (0.5)*

ISC Feedback

Whistleblowers who are entitled to protection under the Directive rules can seek dismissal of legal proceedings on a range of grounds, including defamation, breach of copyright, data protection and disclosure of trade secrets.

The situation is slightly more complicated when it comes to criminal liability. The Directive provides that there is an exemption to general immunity from prosecution if the acquisition or access of information does not constitute a "self-standing criminal offence."

This clause provides a potential of legal uncertainty. It is not uncommon for the acquisition of internal information a whistleblower relies on in their report to be characterised as theft. Preventing these kinds of legal vexatious proceedings was, in fact, one of the inspirations behind the Directive.

The Directive recitals clarify the situation somewhat, specifying physical trespass and computer misuse as examples where national criminal law should apply. Nevertheless, care should be taken here too.

Computer misuse laws are typically expansive and lack a public interest test. It is likely that many disclosures related to data protection or network security – both areas that are explicitly covered by the Directive – could also constitute technical breaches of computer crimes statutes.

If immunity is not to be extended to these areas, then national courts should carefully consider the necessity and proportionality of such actions in relation to the report or public disclosure at issues.

See Directive 21(3), 21(4), 21(7)

See Directive Recital 92

Third parties are also involved in the whistleblowing process and can experience retaliation themselves. Are any of the following explicitly granted protection?

- [x] Relatives of the reporting person *[EUDC] (1)*
- [x] Colleagues of the reporting person *[EUDC] (1)*
- [x] Facilitators assisting in the reporting process *[EUDC] (1)*
- [x] Legal entities the whistleblower owns or works for *[EUDC] (1)*
- [x] Media organisations *[ISC] (1)*
- [x] Individual journalists *[ISC] (1)*
- [x] NGOs *[ISC] (1)*
- [ ] Community groups *[ISC] (1)*
- [ ] Professional bodies *[ISC] (1)*
- [ ] Lawyers *[ISC] (1)*
- [ ] Trades unions (if they are not also workers) *[ISC] (1)*
- [ ] Anyone suspected of blowing the whistle *[ISC] (1)*
- [ ] Anyone else *[ISC] (1)*

EUDC Feedback

The Directive recognises that not only do whistleblowers often seek the assistance of third parties, those individuals and organisations can themselves become the subject of retaliation. Relatives and colleagues of the whistleblower and legal entities directly connected to the whistleblower are entitled to all the protections the Directive provides.

There is also a provision for the protection of "facilitators", who are defined as natural persons who "assist a reporting person in the reporting process" in a confidential manner.

See Directive 4(4), 5(8)

ISC Feedback

The facilitators provision excludes legal entities, but it is open to Member States to improve on the baseline protections in the Directive. Consideration could be given to whether legal entities – such as media organisations, NGOs and professional organisations should also be granted protection.

Reporting Channels

Can a whistleblower make their first report to any of the following places?

- [x] The organisation concerned *[EUDC] (1)*
- [x] An external regulator competent to hear whistleblower complaints *[EUDC] (1)*
- [x] Law enforcement *[EUDC] (1)*
- [x] A trade union *[EUDC] (1)*
- [x] A political representative *[ISC] (1)*
- [x] A journalist or media organisation *[EUDC] (1)*
- [ ] A civil society organisation *[ISC] (1)*
- [x] A dedicated whistleblower authority *[EUDC] (1)*

EUDC Feedback

The ability of whistleblowers to make a choice about where to make a report – whether to their employer, to an external regulator or, in more limited circumstances, to the media – is a key feature of the Directive.

Mandatory internal reporting – an obligation for a whistleblower to make a report to their employer before having recourse anywhere else – was a contentious issue while the Directive was being concluded. It was ultimately rejected.

While the overwhelming majority of whistleblowers - over 90% - will typically make an internal report first, the ability to have initial recourse to a regulator is critical in the minority of cases where an employer is likely to disregard a report or, worse, penalise the whistleblower and destroy evidence when alerted to wrongdoing.

The Directive allows Member States to encourage internal reporting, but not at the expense of providing full information about when a whistleblower might choose to go elsewhere.

Meeting the required standard in this area of the Directive is an essential part of an effective transposition.

The US experience showed that the absence of mandatory internal channels overloads competent authorities with false or irrelevant reports.

See Directive 7, 10, 15

ISC Feedback

The Directive also regulates the creation and functioning of external channels, typically defined as Competent authorities.

Some reporting routes are not explicitly mentioned in the Directive, for instance national governmental or representative bodies. Given that recourse to EU institutions or agencies is defined as external reporting in the Directive, there may be merit in defining a similar situation for domestic institutions in national law.

Existing rights to go to law enforcement or trades unions should not be affected by the Directive.

See Directive 3(4), 6(4)

Do whistleblowers have legal protection if they make a report in the normal course of their work and not through the designated internal channel?

- (●) Yes *[ISC] (1)*
- ( ) No *[ISC] (0)*

ISC Feedback

A large number of whistleblowing cases involve individuals being penalised for communicating information as part of their normal work duties. This is particularly the case for those in compliance, audit and health and safety roles. Creating a specific protected channel for whistleblower disclosures should not leave work-related speech that happens elsewhere vulnerable to retaliation. While the Directive's recitals state that duty speech is protected, member states may want to ensure this is explicit in transposition.

See Recital 62

Which of the following has to provide an internal reporting channel for whistleblower reports?

- [ ] Private sector organisations employing less than 50 people *[ISC] (1)*
- [x] Private sector organisations employing between 50 and 249 people *[EUDC] (1)*
- [x] Private sector organisations employing 250 people or more *[EUDC] (1)*
- [ ] Public sector organisations employing less than 50 people *[ISC] (1)*
- [x] Public sector organisations employing between 50 and 249 people *[EUDC] (1)*
- [x] Public sector organisations employing 250 people or more *[EUDC] (1)*
- [ ] Non-profit organisations employing less than 50 people *[ISC] (1)*
- [x] Non-profit organisations employing between 50 and 249 people *[EUDC] (1)*
- [x] Non-profit organisations employing 250 people or more *[EUDC] (1)*
- [x] All organisations in the financial sector, regardless of how many people they employ *[EUDC] (1)*

EUDC Feedback

One of the most significant provisions of the Directive is the obligation it places on employers to set up secure and confidential internal channels to handle whistleblowing reports.

Private and public sector organisations employing 50 or more people are obliged to set up these channels. This does not override existing obligations for companies in some sectors (such as financial services) where these are more onerous.

Member States have the option of exempting municipalities with less than 10,000 inhabitants from these requirements.

Organisations in the private sector employing fewer than 250 people are allowed to share resources for the receipt and investigation of reports, as long as all the requirements for internal channels are met.

See Directive 8(1, 3-6, 9)

ISC Feedback

Member States have the option of extending these requirements to private sector entities employing fewer than 50 people. The Directive suggests this may be appropriate for the management of risks to public health and the environment in particular organisations.

Where Member States wish to extend internal channel obligations in this way, they are obliged to notify the Commission with their reasons and criteria relied on in their risk assessment.

Non-profits are not specifically mentioned in the Directive but might be best considered as a subset of legal entities in the private sector.

See Directive 8(7-8)

Are private sector organisations allowed to contract third parties to receive and investigate their internal reports?

- (●) Yes *[EUDC] (1)*
- ( ) In some circumstances *[EUDC] (0.5)*
- ( ) No *[EUDC] (0)*

Are there minimum requirements for these third parties to avoid conflicts of interest?

- ( ) Yes *[ISC] (1)*
- (●) No *[ISC] (0)*

EUDC Feedback

Private sector organisations are allowed to contract third parties to operate internal reporting channels on their behalf. Identical standards apply to those third parties as they do to organisations operating their own channels.

See Directive 8(5)

ISC Feedback

Where whistleblowing channels are contracted out to third parties, there is the potential for conflict of interest and detriment caused to whistleblowers as a result. Consideration should be given to whether minimum standards should be set down in law, as they are in the Netherlands.

Netherlands: Wet Huis voor klokkenluiders https://wetten.overheid.nl/BWBR0037852/2018-06-13

Do the requirements for internal channels include the following:

- [ ] Being open to individuals not directly employed by the organisation, such as contractors, volunteers and shareholders *[ISC] (1)*
- [x] Receiving and investigating reports being made the responsibility of a specific person or department *[EUDC] (1)*
- [x] Being designed in a secure way so that reports cannot be accessed by non authorised persons *[EUDC] (1)*
- [x] Training for those receiving or investigating reports *[ISC] (1)*
- [x] Specific protections from retaliation for those receiving or investigating reports *[ISC] (1)*
- [x] Reports can be made in writing, by phone or in person *[EUDC] (1)*
- [x] Reports can be made electronically *[ISC] (1)*
- [x] Reports can be made anonymously *[ISC] (1)*
- [x] The ability to communicate with a whistleblower after they have made their report *[EUDC] (1)*
- [x] Acknowledgement of reports within 7 days *[EUDC] (1)*
- [x] The diligent investigation of reports *[EUDC] (1)*
- [x] Responding to a report with feedback within 3 months *[EUDC] (1)*
- [x] Documenting reports so that they can be investigated *[EUDC] (1)*
- [x] Keeping records of the number of reports received and outcome of investigations *[ISC] (1)*
- [x] Providing clear information about how to access relevant external reporting channels *[EUDC] (1)*
- [ ] Allowing the whistleblower access to the investigative file *[ISC] (1)*
- [ ] Allowing the whistleblower to comment on a draft report *[ISC] (1)*

EUDC Feedback

The Directive sets out some specific requirements for how internal channels should operate. They are supposed to be designed with confidentiality in mind and made the specific responsibility of an individual or department.

There must be scope for reports to be made in writing, orally and in person, if that is requested.

Those charged with operating the channel are expected to keep communication with the whistleblower open. A reporting person is entitled to have their report acknowledged within seven days and receive feedback within three months.

See Directive 9

ISC Feedback

Internal channels must be open to employees, but organisations have the option of opening their whistleblowing to others who do have been in contact with it in the course of their working activities. This includes volunteers, contractors and shareholders.

Facilitating anonymous reporting is suggested as an option in the

Directive. The use of online dropboxes allows for anonymous reporting that maintains a means of communication between the whistleblower and the person receiving the report.

Training for those operating internal channels is not required under the Directive but, given that it is mandatory for those operating external channels, it should be regarded as best practice.

Similarly, while there is a requirement for those operating internal channels to keep records for the purpose of investigating reports, there is no obligation to maintain or publish statistics on the number of reports received and outcome of investigations. Employers may wish to consider doing so as a means of showing that their measures are working as intended.

See Directive 8(2)

Do the requirements for external reporting channels include the following:

- [x] Authorities operating these channels to be named by government and properly resourced *[EUDC] (1)*
- [x] Handling and investigating reports being made the responsibility of a specific person or department *[EUDC] (1)*
- [x] Being designed in a secure way so that reports cannot be accessed by non authorised persons *[EUDC] (1)*
- [x] Training for those receiving or investigating reports *[EUDC] (1)*
- [x] Specific protections from retaliation for those receiving or investigating reports *[EUDC] (1)*
- [x] Reports can be made in writing, by phone or in person *[EUDC] (1)*
- [x] Reports can be made electronically *[ISC] (1)*
- [x] Rules for what happens if a report is received, but not through the regular channel *[EUDC] (1)*
- [x] Reports can be made anonymously *[ISC] (1)*
- [x] The ability to communicate with a whistleblower after they have made their report *[EUDC] (1)*
- [x] Acknowledgement of reports within 7 days, unless this would put the reporting person at risk *[EUDC] (1)*
- [x] The diligent investigation of reports *[EUDC] (1)*
- [x] Obligation to respond to a report and provide feedback within 3 months, or 6 months in "duly justified" cases *[EUDC] (1)*
- [x] Secure storage of reports for the purposes of investigation *[EUDC] (1)*
- [x] Keeping records of the number of reports received and outcome of investigations *[EUDC] (1)*
- [x] Providing clear information online about whistleblowers' legal rights, recourse and the response they can expect *[EUDC] (1)*
- [x] Receiving and investigating reports being made the responsibility of a specific person or department *[EUDC] (1)*
- [ ] Allowing the whistleblower access to the investigative file *[ISC] (1)*
- [ ] Allowing the whistleblower to comment on a draft report *[ISC] (1)*

EUDC Feedback

Requirements for external channels under the Directive are similar to those for internal channels, but more onerous in some respects. This reflects not only that external channels are likely to handle the most serious initial reports and those escalated from internal channels.

Those operating external channels are expected to provide training to those dealing with whistleblower complaints and have set procedures for transmitting reports to those best placed to investigate them. Those procedures need to be set up in specified manners regarding the granting of confidentiality of personal data, reporting and accessibility.

Member States are granted significant freedom in the institutional design of external whistleblowing schemes and may explicitly consider the introduction of dedicated independent oversight.

EU regulators have included "relevant institutions, bodies, offices or agencies of the Union" as eligible recipients for external reports, which suggests national agencies should be treated in the same way.

See Directive 11,12

Does a public report have to be made via a journalist?

- (●) Yes *[ISC] (0)*
- ( ) No *[ISC] (1)*

ISC Feedback

What constitutes a public disclosure for the purposes of the Directive is not defined. While much discussion of public reporting focuses on the relationship between whistleblowers and journalists, there is nothing that says that journalists necessarily have to be involved in such disclosures.

Direct publication, for instance the publication of an op-ed, a blog or a post on social media, should also be understood as types of public reporting.

See Directive 15

Is public reporting protected in the following circumstances?

- [x] The person has reasonable grounds to believe that the report concerns and immediate and obvious danger to the public interest *[EUDC] (1)*
- [x] The person has reasonable grounds to believe that it is unlikely the report will be addressed in any other way *[EUDC] (1)*
- [x] The person has reasonable grounds to believe that using another reporting channel would be likely to result in retaliation *[EUDC] (1)*
- [x] Other channels were used and the time limit for a response has passed without appropriate action being taken *[EUDC] (1)*
- [ ] The report concerns public health or the environment *[ISC] (1)*
- [ ] The ability to go to the media is protected under existing national law *[EUDC] (1)*
- [x] Public reporting allowed unless the information is marked classified or release is specifically prohibited by statute *[EUDC] (1)*
- [ ] Any other circumstance *[ISC] (1)*

EUDC Feedback

While whistleblowers are able to make their report public in the first instance, the Directive sets a high bar for this. A report must either "constitute an imminent or manifest danger to the public interest" with the risk of emergency or serious damage, or the whistleblower has reason to believe that using other channels will be fruitless or risky.

Public reporting is also protected in situations where other reporting channels have been tried and no appropriate action has been taken in the given timeframe. The Directive recitals clarify that this covers situations where investigations have been conducted but appropriate remedial action has not been taken. If a report has been wrongly assessed as being of minor importance, the recitals suggest this may be a reason to go public.

Where national laws already offer greater protections – for instance in Sweden, where source protection is guaranteed at a constitutional level – these are not affected by the Directive.

See Directive 15

See Directive Recital 79

ISC Feedback

Courts are likely to interpret "imminent or manifest danger" narrowly. Member states may therefore wish to consider whether the Directive's treatment of public reporting offers effective protection to whistleblowers who have information on issues of considerable public importance. To strengthen legal certainty, clear definitions of what constitutes imminent or manifest dangers to the public interest should be included.

Support and Legal Protections

Can whistleblowers make anonymous disclosures?

- [x] Yes, there is an obligation to provide ways of making anonymous reports *[ISC] (1.5)*
- [ ] Yes, there is the option of providing ways of making anonymous reports *[ISC] (1)*
- [x] There is an obligation to investigate anonymous reports if received *[ISC] (1)*
- [x] Whistleblowers who make a report anonymously are entitled to protection on the same basis as others if their identity becomes known *[EUDC] (1)*
- [ ] Anonymous reports are not possible *[EUDC] (0)*

Which channels are covered by the obligation to provide ways of making anonymous reports?

- ( ) Internal *[ISC] (1)*
- ( ) External *[ISC] (1)*
- (•) Both *[ISC] (2)*

EUDC Feedback

Notwithstanding the prominence of anonymous disclosures in public debates around whistleblowing, the provision of anonymous reporting channels was a contentious issue during Directive negotiations.

The Directive contains one firm commitment on anonymity, to ensure that whistleblowers who make anonymous reports are not deprived of protections. Where the identity of someone who has made an anonymous report becomes known, they are entitled to the same duty of confidentiality and protections against retaliation as whistleblowers who have used other channels.

See Directive 6(2-3)

See Directive Recital 14

ISC Feedback

Beyond this commitment, the Directive suggests that Member States consider whether to require internal or external channels to facilitate and investigate anonymous reports.

Which of the following provisions are included for keeping the identity of a whistleblower confidential?

- [x] Only authorised staff should have access to information that identifies a whistleblower *[EUDC] (1)*
- [x] There are set procedures for what happens if non-authorised staff receive a report *[EUDC] (1)*
- [x] No personal data is collected or handled unless relevant to handling the report made. Accidentally collected data is to be deleted without undue delay *[EUDC] (1)*
- [x] Personal data relevant to the report is to be treated in accordance with data protection rules *[EUDC] (1)*
- [x] There are penalties for individuals or legal entities that breach their duty of confidentiality *[EUDC] (1)*
- [x] Whistleblowers can make a report without revealing their identity to anyone *[ISC] (1)*

EUDC Feedback

The duty of confidentiality is a key part of the Directive. A key characteristic of ineffective or compromised reporting channels is that they communicate the identity of a whistleblower to those who are the subject of their report.

The Directive therefore lays down detailed rules about the treatment of personal data and the need for this to be restricted to authorised persons. Those operating reporting channels have a responsibility to comply with data protection rules, with the purpose of information collection in this context to be to ensure that an investigation can be properly carried out.

Confidentiality applies not only to personal data, but also to other information from which the identity of the reporting person could be deduced.

There should be penalties for those who breach this duty of confidentiality.

See Directive 8(6), 9 (1), 12 (1), 13, 16, 23(1)(d)

ISC Feedback

An additional means of protecting against breaches of confidentiality is to allow whistleblowers to make their report anonymously. Member States should consider mandating the provision of options for anonymous reporting and ensuring that such reports are investigated.

Encrypted online drop-box systems allow for follow up of anomymous reports, which greatly assists investigation.

Under what circumstances can a whistleblower's identity be revealed?

- [x] If they grant their consent *[EUDC] (1)*
- [x] If it is "necessary and proportionate" to do so in the context of an investigation or judicial proceedings, and this is required by EU or national law *[EUDC] (1)*
- [x] If written permission has been granted in advance *[EUDC] (1)*
- [x] If the whistleblower has had the opportunity to challenge the decision *[EUDC] (1)*
- [ ] If original report was anonymous *[EUDC] (-1)*

Where it is "necessary and proportionate" to do so in the context of an investigation or judicial proceedings and this is required by EU or national law, are those legal obligations specified?

- (●) Yes *[ISC] (1)*
- ( ) No *[ISC] (0)*

EUDC Feedback

There are limited exemptions from the general duty of confidentiality, for the purpose of investigating a report or for judicial proceedings.

A whistleblower's identity may be disclosed if they give explicit consent or if it is assessed to be "necessary and proportionate" for investigation purposes, in the context of national law. Where this is the case, a whistleblower should be sent notification and an explanation in writing.

"Disclosure" in this context means disclosure to indivduals who are not authorised staff members, rather than disclosure to the public.

See Directive 16

ISC Feedback

The operation of these provisions depends to a great extent on national legal frameworks. Member states should refer to relevant legal obligations when putting these provisions into national law.

Is it clear that the following types of retaliation against a whistleblower are prohibited?

- [x] Suspension, lay-off, dismissal or equivalent measures *[EUDC] (1)*
- [x] Demotion or withholding of promotion *[EUDC] (1)*
- [x] Change in working conditions, place of work or working hours *[EUDC] (1)*
- [x] Reduction in salary *[EUDC] (1)*
- [x] Being given a negative reference *[EUDC] (1)*
- [x] Negative publicity or posts on social media *[EUDC] (1)*
- [x] Not being granted a full time or permanent contract *[EUDC] (1)*
- [x] Early termination, cancellation of contract for goods or services *[EUDC] (1)*
- [x] Cancellation of licences or permits *[EUDC] (1)*
- [x] Informal boycotting, or other actions which may make it hard for a reporting person to find new employment *[EUDC] (1)*
- [x] Harassment, being ostracised or other forms of social retaliation *[EUDC] (1)*
- [x] Medical or psychological referral *[EUDC] (1)*
- [x] Domestic legal proceedings *[EUDC] (1)*
- [ ] Extradition to face legal proceedings elsewhere *[ISC] (1)*

EUDC Feedback

All forms of retaliation, and attempts at retaliation, are prohibited under the Directive. The Directive text includes a non-exhaustive list of many types of retaliation and Member States should ensure that informal and social varieties of reprisal are encompassed in their definition.

See Directive 19

ISC Feedback

Notwithstanding that the Directive's list of examples is non-exhaustive, it is possible that some retaliatory measures are not recognised as such. Due to its cross-jurisdictional nature, extradition is not always understood as a variety of retaliation, despite increases in its use against both whistleblowers and journalists.

There is an allegation of employer retaliation against a whistleblower, who has already demonstrated that they made a report according to the rules. Whose responsibility it is to prove that the retaliatory action was - or was not – connected to the report?

- The whistleblower has to show that the action taken against them was a consequence of their report *[EUDC] (0)*
- The person accused of retaliating has to show that the action taken against the whistleblower was not related to their report *[EUDC] (1)*

EUDC Feedback

Should a case involving a whistleblower end up in legal proceedings, it is for the employer to show that any action taken against a whistleblower was not as a consequence of their report.

This reversed burden of proof is an important clause in the Directive, which makes a significant difference for the ability of whistleblowers to receive the protections they are entitled to in law.

See Directive 21(5)

Are penalties established for the following actions?

- [x] Retaliating against a whistleblower *[EUDC] (1)*
- [x] Bringing vexatious legal proceedings against a whistleblower *[EUDC] (1)*
- [x] Obstructing, or attempting to obstruct a report *[EUDC] (1)*
- [x] Revealing a whistleblower's identity to a non-authorised person *[EUDC] (1)*

EUDC Feedback

The Directive requires Member States to introduce penalties for retaliating against or obstructing a whistleblower (or attempts to do so), breaching the confidentiality due to a whistleblower or for a whistleblower to make a knowingly false report or public disclosure.

The nature of these penalties is left up to the discretion of the Member States. It is important that a proportionate approach is taken, lest the overall objective of the legislation – to encourage whistleblowers to come forward – is compromised.

See Directive 23

ISC Feedback

The issue of penalties for making a knowingly false report are a case in point. Laws against defamation are likely to already be present in most EU jurisdictions.

Where a new course of action or criminal offence is proposed, this may impact freedom of expression rights as well as whistleblower protection. Such proposals require very careful examination.

Is it clear that whistleblowers' rights cannot be removed or modified in contracts, workplace policies, settlements or non-disclosure agreements?

- (●) Yes *[EUDC] (1)*
- ( ) No *[EUDC] (0)*

EUDC Feedback

Rights and remedies provided for in the Directive cannot be waived or abrogated in any kind of agreement, including settlements and non-disclosure agreements.

See Directive 24

What kinds of support are whistleblowers entitled to receive?

- [x] Free and independent advice on whistleblowing procedures, protections and remedies *[EUDC] (1)*
- [x] Certification of their status as a whistleblower *[ISC] (1)*
- [x] Access to a tribunal or administrative process *[ISC] (1)*
- [ ] The possibility of punitive damages *[ISC] (1)*
- [x] The ability for whistleblowers to recover legal fees and costs if they prevail *[ISC] (1)*
- [x] Legal aid both in criminal and civil proceedings *[EUDC] (1)*
- [ ] Health and psychological support *[ISC] (1)*
- [x] Financial assistance *[ISC] (1)*
- [x] Recourse to an independent whistleblowing authority *[ISC] (1)*
- [ ] Interim relief while their case is being considered *[ISC] (1)*

EUDC Feedback

Many kinds of support for whistleblowers are envisioned in the Directive, but most are optional and left up to the discretion of Member States to put into law.

Obligatory elements include the provision of free and independent advice. Internal channels must make information on how to make a report and methods of recourse available to employees. Operators of external channels must publish information online.

Member States are also obliged to provide legal aid to whistleblowers in criminal and cross-border civil proceedings.

See Directive 20(1)

ISC Feedback

Member States may wish to consider whether the compulsory legal aid requirement in the Directive is comprehensive enough to cover all the types of legal action a whistleblower might be subjected to. In particular, consideration should be given to the costs a whistleblower might encounter during employment and other civil proceedings.

Other types of support Member States may choose to provide include health and psychological support, interim relief and financial assistance. They may wish to introduce a certification scheme whereby a whistleblower can demonstrate their status pending investigation.

Member States may also establish a dedicated agency responsible for providing whistleblowers with information or support.

See Directive 20(2-3)

How are the rights of the individuals and entities that are the subject of reports protected?

- [x] Basic rights to fair procedure are not changed *[EUDC] (1)*
- [x] Penalties for making knowingly false reports *[EUDC] (1)*
- [x] Confidentiality rules also apply to those who are the subject of reports *[EUDC] (1)*
- [x] Identity of those in reports are kept confidential while an investigation is proceeding *[EUDC] (1)*
- [x] Access to effective remedial measures in cases of false or unjustified reports *[EUDC] (1)*

EUDC Feedback

The Directive includes an assertion of basic rule of law principles for those who are the subject of reports ("persons concerned"), including the presumption of innocence and a fair trial. There is a duty of confidentiality towards persons concerned as there is for whistleblowers.

See Directive 22

Is making a knowingly false report a criminal offence?

- Yes *[ISC] (0)*
- No *[ISC] (1)*

ISC Feedback

One area for remedy that requires careful consideration are penalties for those who use whistleblowing channels to make knowingly false reports, or disclose such information publicly.

Care should be taken to ensure that the approach taken here is proportionate and does not act as a disincentive to those who are considering making a report, as that would defeat the point of the Directive.

Laws against defamation are likely to already be present in most EU jurisdictions. Where a new course of action or criminal offence is proposed, this may impact freedom of expression rights as well as whistleblower protection. Such proposals require careful examination.

See Directive 23

Review and Evaluation

Which of the following kinds of information need to be kept by those operating reporting channels for record-keeping purposes?

- [x] Records of the original report, in audio recording or minuted form, while investigations are ongoing *[EUDC] (1)*
- [x] The number of investigations started *[EUDC] (1)*
- [ ] The reason for not launching an investigation *[ISC] (1)*
- [x] The outcome of an investigation *[EUDC] (1)*
- [x] Any corrective action taken as a result of an investigation *[EUDC] (1)*
- [x] Estimated financial damage related to the subject matter of the report *[EUDC] (1)*
- [x] Any funds recovered *[EUDC] (1)*

EUDC Feedback

The Directive establishes record-keeping duties for operators of internal and external channels in order to ensure that investigations can be conducted properly.

Operators of external channels are expected to keep records of the individual report, which can be inspected by the whistleblower on request, together with aggregated data on the total number of reports received, the outcome of investigations and the funds recovered as a result.

The standards for internal channels are less onerous and require only that proper records of reports be taken for the purposes of an investigation.

See Directive 18

ISC Feedback

Operators of internal channels may wish to consider keeping aggregated statistics on the number of records received and outcomes. There may be a reputational value in doing so, in addition to building confidence in the system.

We suggest that in addition to keeping records of investigation outcomes, operators of external channels record the reasons for not launching investigations. Large numbers of reports are being closed as trivial or repetitive may warrant further investigation.

Which of the following categories of information should be collated by central government?

- [x] The number of reports received by external channels *[EUDC] (1)*
- [x] The number of investigations launched by external channels *[EUDC] (1)*
- [ ] The reason for not launching an investigation *[ISC] (1)*
- [x] Estimated financial damage related to the subject matter of the report *[EUDC] (1)*
- [x] Total funds recovered *[EUDC] (1)*
- [x] Any corrective action required as a result of an investigation *[EUDC] (1)*
- [x] The number of legal proceedings related to reports, including proceedings for retaliation against a whistleblower and any proceedings related to knowingly false reports *[ISC] (1)*
- [ ] The outcome of any related legal proceedings *[ISC] (1)*

EUDC Feedback

The Directive mandates the collection of certain statistics on the national level. These include the total number of reports received by external channels and the number of investigations launched on the basis of those reports together with an estimate of the financial loss caused by the matters under discussion and any funds recovered.

See Directive 27

ISC Feedback

It may also be valuable to aggregate data on the outcome of reports and any legal proceedings initiated in relation to reports. This should include any proceedings for retaliation or for making a knowingly false report.

How will we know if the legislation is working?

- [x] National statistics are to be provided to the Commission annually *[EUDC] (1)*
- [x] National authorities are obliged to review external reporting mechanisms at least every three years *[EUDC] (1)*
- [x] National statistics are to be published annually *[ISC] (1)*
- [x] Public authority tasked with conducting regular review of the system *[ISC] (1)*
- [ ] Regular survey of whistleblower satisfaction with the system *[ISC] (1)*
- [ ] Implementation of an anonymous complaint mechanism for failures of the system ("whistleblowing on whistleblowing") *[ISC] (1)*

EUDC Feedback

The European Commission intends to conduct a review of how the legislation is operating after four years.

The Directive does not stipulate what review processes should take place at the national level, other than that certain statistics should be recorded and that a review of external channels needs to take place at least every three years.

In practice civil society plays an important role in reviewing how national systems are working and we can expect that to continue.

COVID-19 Scenarios

A care home worker is concerned about inadequate staffing levels at their place of employment, where they are charged with looking after a resident population who are particularly vulnerable to infection with COVID-19. Some have recently arrived after being discharged from hospital.

Concerned about the likely reception from their superiors, the worker makes a report to the industry regulator. Are they protected?

- (●) Yes *[COVID] (1)*
- ( ) No *[COVID] (0)*
- ( ) Not sure *[COVID] (0.5)*

There is a shortage of personal protective equipment in a hospital, meaning that medical staff are having to re-use equipment or improvise with home-made replacements. Knowing that she is also voicing the concerns of many of her colleagues, a nurse posts a video on her social media account where she expresses her fears and frustrations.

Is she protected from retaliation?

- Yes *[COVID] (1)*
- No *[COVID] (0)*
- Not sure *[COVID] (0.5)*

If the nurse discusses her plan with a colleague before posting a video, is that colleague also protected?

- Yes *[COVID] (1)*
- ◉ No *[COVID] (0)*
- Not sure *[COVID] (0.5)*

In circumstances of unprecedented demand, the market for masks, protective aprons and other PPE is fast moving and intensely competitive. A civil servant working in procurement is concerned about decisions made by a senior colleague but is equally worried about being identified.

Can they express their concerns anonymously?

- (●) Yes *[COVID] (1)*
- ( ) No *[COVID] (0)*
- ( ) Not sure *[COVID] (0.5)*

Will their report be ignored?

- ( ) Yes *[COVID] (0)*
- (●) No *[COVID] (1)*
- ( ) Not sure *[COVID] (0.5)*

A security researcher finds a critical security flaw in a “track and trace” app that allows users to alert others they have come into contact with, if they are diagnosed with COVID-19. The security flaw means that location data relating to a large number of people is easily accessible from the open internet. While it is not well secured, accessing this data would likely breach local computer crimes laws.

If they reported this security breach, would they be protected?

- (●) Yes *[COVID] (1)*
- ( ) No *[COVID] (0)*
- ( ) Not sure *[COVID] (0.5)*