



RIGHTS WHISPER



www.rights-whisper.eu

RIGHTS WHISPER

D2.1: GUIDANCE DOCUMENT: LINKING DIRECTIVE 2019/1937 WITH CHARTER RIGHTS

CERV-2025-CHAR-LITI

Project number: 101293231



TRANSPARENCY
INTERNATIONAL
SLOVENIA



TRANSPARENCY
INTERNATIONAL
BULGARIA



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.



Contents



Executive summary	06
Introduction	08
• 1.1 Why we connect the Directive with fundamental rights	09
• 1.2 Who is the handbook for?	09
• 1.3 Scope and limitations	09
Part I — Legal framework	10
2. Directive (EU) 2019/1937 briefly	10
• Why a common EU standard was needed	10
• 2.1 What the Directive covers	11
• 2.2 What might this mean in practice?	11
• 2.3 Who may qualify for protection?	11
• 2.4 Reporting channels	13
• 2.5 Public disclosure, or when to go to the media?	13
• 2.6 Protecting the reporting person's identity	14
• 2.7 Protection against retaliation and support for reporting persons	14
• 2.8 Penalties	14
• 2.9 What about fields that already had their own rules?	15
3. The Charter of Fundamental Rights of the European Union: Why does it matter for reporting persons?	16
• 3.1 How may Charter rights be limited?	17
• 3.2 The Charter before national courts	17
Part II — Article-by-article analysis	18



Contents



4. Article 11 — Freedom of expression and information	18
• 4.1 When a person decides to speak up...	18
• 4.2 Who may qualify for protection?	19
• 4.3 Must reporting persons prove that they are right, and what evidence do they need?	19
• 4.4 Confidentiality enables people to find the courage to speak up	20
• 4.5 What if a person wants to disclose information to the public?	21
• 4.6 What does this look like in practice?	21
5. Article 31 — Fair and just working conditions	22
• 5.1 They spoke up. What happens the next day?	22
• 5.2 What is retaliation?	23
6. Article 41 — Right to good administration	25
• 6.1 After submitting a report	25
• 6.2 Who handles the report?	26
7. Article 47 — Right to an effective remedy and to a fair trial	30
• 7.1 What if protection fails?	30
• 7.2 A real-world example	31
• 7.3 When a report concerns another person	31
• 7.4 What if protection of the reporting person fails?	31
8. How the four rights interact	32
• Article 11: Speak up about wrongdoing!	32



Contents



• Article 31: I must not become a target for speaking up!	32
• Article 41: Someone must handle my report properly and provide me with feedback!	32
• Article 47: If my rights are not protected after I speak up, there is a route to an effective remedy.	32
 9. Part III — Examples from everyday working life	 33
• 9.1 Suspected manipulation of a public procurement procedure	33
• 9.2 Environmental example BULGARIA and GREECE	34
• 9.3 Example from the pharmaceutical or financial sector	36
 10. Guidance for organisations: What must an organisation do to ensure that its internal reporting channel works in practice?	 38
• 10.1 Independence that must be tested, not merely stated	39
• 10.2 Documenting decisions	39
• 10.3 Training and awareness	39
• 10.4 How does an organisation know whether its system really works?	40
 11. What must a competent authority do to ensure that external reporting works in practice?	 40
• 11.1 Who can report externally, and when?	40
• 11.2 The channel must be accessible and confidential	41
• 11.3 What happens after a report is submitted?	41
• 11.4 What if the authority remains silent or closes the report without explanation?	41
• 11.5 External transparency	41



Contents



12. How do we know whether the system works at all?	43
• 12.1 What Member States must report to the European Commission	43
• 12.2 Which indicators show whether protection actually works?	44
• 12.3 The role of projects such as RIGHTS WHISPER	44
13. All in one place: Charter article, Directive provision and practical focus	44
14. Frequently asked questions	45
• Annex A — Checklist for organisations	46
• Annex B — A short guide for workers	47
• Annex C — Glossary and further resources	48
• Annex D — Model wording	48
SOURCES AND FURTHER READING	50

Executive summary



This guidance handbook is the first deliverable of Work Package 2 of the RIGHTS WHISPER project, led by Transparency International Slovenia. Its purpose is to explain, in clear and above all practical terms, the relationship between Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union.

The handbook is not intended to be yet another legal analysis of the Directive. It is intended for people and organisations that deal with reports of wrongdoing in practice: workers considering making a report; persons of trust and other people who receive and handle such reports; organisations establishing internal reporting channels; and competent authorities receiving external reports.

Why did we begin with the Charter of Fundamental Rights of the European Union, and what does it have to do with the Whistleblower Protection Directive?

The Charter of Fundamental Rights of the European Union had already been legally binding for ten years (since 2009) when the Whistleblower Protection Directive became legally binding in 2019. This matters because, a decade later, the Directive laid down its rules within a European legal order in which fundamental rights had already been codified. One point is essential to understanding this document.

‘The Charter sets out which right we protect, while the Directive translates that right into specific rules: how a person should report a breach, to whom, when they should expect a response, whether they will be protected, and whether they could lose their job.’

In this handbook, we examine in detail four provisions of the Charter that are particularly important for reporting wrongdoing (whistleblowing):



- Article 11 (freedom of expression and information),
- Article 31 (fair and just working conditions),
- Article 41 (right to good administration), and
- Article 47 (right to an effective remedy and to a fair trial).

Each of these rights corresponds to a particular stage or situation experienced by a reporting person. The first stage is the decision to speak up, followed by making a report within or outside their organisation, through to the point at which the reporting person may have to challenge retaliatory action before a court.

The handbook is therefore divided into three parts. First, we present the basic legal framework: an accessible overview of the Directive's scope, reporting routes and protective mechanisms, followed by an introduction to the Charter and to the general principle recognised both by the Court of Justice of the European Union and by the European Commission itself—namely, that whistleblower protection is, at its core, a matter of fundamental rights. The second part analyses each of the four Charter articles listed above, explaining them through narratives and examples from different countries. The third part translates the analysis into practice, with separate guidance for organisations required to operate internal reporting channels and for competent authorities receiving external reports. Our concern is not merely whether a reporting channel exists in a particular company or organisation, but whether it enables individuals to report safely, ensures that their reports are handled appropriately, and protects them against retaliation.

The document also includes two practical tools for everyday use: a two-page checklist enabling an organisation to assess, article by article, whether its whistleblowing policy respects the underlying fundamental rights rather than merely the letter of national law; and a two-page short guide written directly for workers, explaining in plain language what protection they are entitled to and where it comes from. A short glossary and a list of further resources conclude the document.

It is important to note that these guidelines do not replace legal advice or country-specific analysis, which is being prepared under Task T2.2 (national implementation of reporting channels), nor do they replace the case-law analysis under Task T2.4 (cases of retaliation). Their role is narrower but, in the project consortium's view, fundamental: to provide all subsequent RIGHTS WHISPER deliverables with a shared vocabulary grounded in European rights, enabling us to discuss not only what whistleblower protection requires, but also why it matters.

Introduction



At first sight, Directive (EU) 2019/1937 is a rather technical document. Over several dozen pages, it explains why the European Union needed common rules for whistleblower protection, who may qualify for protection, which breaches may be reported and which reporting options must be available. Behind the legal language, however, lies a fairly simple question: **‘What should people do when, in the course of their work, they notice something that is not right and decide to speak up about it?’**

They may notice suspected corruption in a public procurement procedure, a dangerous product, a breach of environmental rules, the misuse of EU funds, or another breach covered by the Directive, and decide to report it. It is not the reporting person’s task to investigate the wrongdoing themselves and gather all the evidence. What matters is that they have information acquired in a work-related context and reasonable grounds to believe that it was true at the time of reporting. Once they decide to speak up, very practical questions arise. To whom can they report the wrongdoing? Must they first inform their employer, or can they approach the competent authority directly? Who may learn their identity? What happens if their report is subsequently not substantiated? Above all, who will protect them if they lose their job, position or responsibilities because of the report, or if they face pressure or other forms of retaliation?

This handbook seeks to answer these questions as clearly as possible.

We will therefore not present the Directive solely article by article. We will examine what its rules mean in real life, both for a person wishing to report wrongdoing and for the organisation or competent authority receiving the report. We will pay particular attention to the reporting person’s fundamental rights mentioned above.

In Slovenia, there have been cases in which reporting persons said that their written reports had been forwarded directly to managing directors and that they had not been protected but had instead faced retaliation.

Organisations therefore often set up an email address and an online form without ensuring confidentiality, the proper handling of reports, or protection against retaliation. If protection fails, reporting persons must be able to enforce their rights effectively.

The Member States have transposed the European Directive into their national legislation, and individual rules may therefore vary from country to country. This handbook consequently focuses not on the legislation of any one country, but on the common European rules and rights arising from the Directive and the Charter. Specific examples will help demonstrate how these rules operate in practice.

For the RIGHTS WHISPER project, such a common European framework is also important because it will form the basis for subsequent national reports, training and awareness-raising materials in the partner countries.

1.1 Why we connect the Directive with fundamental rights

The RIGHTS WHISPER project requires us to examine whistleblower protection through the lens of four fundamental rights enshrined in the Charter of Fundamental Rights of the European Union: freedom of expression and information under Article 11; fair and just working conditions under Article 31; the right to good administration under Article 41; and the right to an effective remedy and to a fair trial under Article 47. Put as simply as possible, these Charter articles can be summarised as follows:

- Article 11: Speak up about wrongdoing!
- Article 31: I must not become a target for speaking up!
- Article 41: Someone must handle my report properly and provide me with feedback!
- Article 47: If my rights are not protected after I speak up, there is a route to an effective remedy.

This explanation is easy to remember. To understand the relationship, however, it is worth reiterating that the Whistleblower Protection Directive was adopted a decade after the EU Charter of Fundamental Rights became legally binding and builds on those rights. Why do we mention, combine and cross-reference the two, and why do we seek to understand them together?

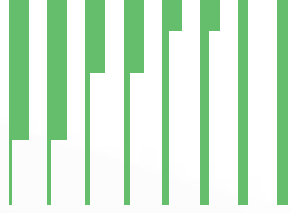
The Charter therefore helps us understand which fundamental right we are protecting, while the Directive is concrete: it tells us how a person who reports a breach should be protected in practice.

1.2 Who is the handbook for?

This guidance handbook is written for employees who are considering speaking up about wrongdoing; designated persons responsible for receiving and following up reports and for the day-to-day operation of internal reporting channels; legal and human resources professionals who advise organisations on whistleblowing policies; staff of competent public authorities that manage external reporting channels under national legislation transposing the Directive; and civil society organisations, trade unions and providers of free legal assistance that support workers who are considering making a report or have already done so.

1.3 Scope and limitations

This document addresses fundamental rights and the Directive at EU level. It does not provide a country-by-country overview of transposition;



that analysis is being prepared separately as D2.2 (national implementation of reporting channels) and D2.5 (consolidated transnational comparative report). Part II also uses real, non-anonymised cases involving reporting persons. These cases have already received public or media attention. We chose this approach because we did not want a purely theoretical document, but real examples that reveal something a dry explanation alone cannot: what the decision to speak up means in practice for a particular person and what a reporting person may face in real life. The stories are not intended to discourage reporting. On the contrary, some occurred before the Directive became applicable and demonstrate why its adoption by the Member States was important. Real-life stories allow workers and prospective reporting persons to understand the Directive through a person's experience, from the moment they noticed wrongdoing to the moment they first thought they might need protection. It is important to add that the purpose of using these examples is not to assess the guilt of the individuals or organisations concerned by the reports, but solely to illustrate the challenges reporting persons face.



Part I — Legal framework

2. Directive (EU) 2019/1937 briefly

Why a common EU standard was needed

It may be helpful to begin with a figure illustrating why directives of this kind are needed to encourage individuals to report suspected wrongdoing. According to the 2025 Eurobarometer survey, as many as 69% of EU citizens believe that corruption is widespread in their country. The European Commission estimates that corruption costs the EU between EUR 170 billion and EUR 990 billion each year.

This handbook is therefore one of the measures intended to encourage and empower individuals to report suspected wrongdoing instead of simply turning a blind eye. Before 2019, whistleblower protection varied across the European Union and was, above all, fragmented. Only a small number of countries had comprehensive, cross-sectoral legislation; in most, protection was scattered across different laws, if it existed at all. The European Parliament had called for uniform legislation for more than a decade before the Commission prepared its proposal. Another impetus for regulating this field came from media investigations in individual countries that exposed corruption and breaches of law in areas such as taxation, financial supervision and environmental non-compliance.

The European Parliament and the Council adopted the Directive on 23 October 2019, with an overwhelming majority in the plenary vote. It entered into force twenty days after its publication in the Official Journal.

Member States were required to transpose it into national law by 17 December 2021, with an additional two-year transitional period, until December 2023, for private-sector entities with between 50 and 249 workers to establish internal reporting channels. Transposition proceeded unevenly: several Member States missed the initial deadline by a considerable margin, and the European Commission opened infringement proceedings against some of them. By the time of the Commission's 2024 implementation report, transposition had been completed in all twenty-seven Member States, albeit with varying degrees of fidelity to the Directive's minimum standards.

2.1 What the Directive covers

The Directive lays down specific rules to protect people who encounter or learn of a breach of EU law in the course of their work and wish to report it. A breach does not mean only conduct that is manifestly unlawful. It may also involve suspected infringements of rules in certain areas of EU law. The Directive refers, among others, to public procurement, financial services, public health, food safety, consumer protection and the protection of personal data. It also covers breaches affecting the European Union's financial interests and certain internal-market rules. The Directive does not, however, limit Member States in this regard. They may extend whistleblower protection to other areas not covered by the Directive itself. Several countries chose to do precisely this when transposing the Directive into national law.

2.2 What might this mean in practice?

In public procurement, this means that a report might concern a tender tailored to a particular bidder or the artificial splitting of contracts to avoid public-procurement rules. In financial services, it might concern the concealment or manipulation of transactions. In product safety, a report might concern a non-compliant product that a company nevertheless places on the market. In transport, an employee might draw attention to the concealment of maintenance data; in environmental protection, to illegal dumping; and so forth.

Where the EU's financial interests are concerned, possible examples include fraud, corruption and the misuse of EU funds or subsidies. In the field of the internal market, a report might concern, for example, cartel arrangements, abuse of a dominant position or breaches of State-aid rules.

2.3 Who may qualify for protection?

Protection is not intended solely for permanent employees. The Directive emphasises that individuals may have various types of relationship with an organisation and still qualify for protection. They may be self-employed persons, shareholders, members of administrative and supervisory bodies, volunteers, trainees or subcontractors. Crucially, protection is not tied to a current employment relationship: a person may report wrongdoing after leaving the organisation or even during a recruitment process.

In addition to reporting persons themselves, the Directive takes account of people around them. Protection may extend to a person who assisted them with the report, as well as to colleagues or relatives who might themselves face retaliation because of their connection with the reporting person. Under certain conditions, protection also extends to legal entities that the reporting person owns, works for or is otherwise connected with in a work-related context. This is particularly important because, in real life, the consequences of reporting are not always confined to the person who made the report.



Selected areas covered by the Annex to the Directive	Examples of relevant breaches
Public procurement	Tailored tender procedures, conflicts of interest in the award of contracts, and circumvention of public-procurement thresholds.
Financial services, prevention of money laundering and terrorist financing	Inadequate customer due diligence, concealment of suspicious transactions, and market abuse.
Product safety and compliance	Placing non-compliant or dangerous products on the market, and falsified compliance documentation.
Transport safety	Concealment of safety-critical defects, and falsification of inspection or maintenance records.
Environmental protection	Illegal discharge of substances, falsified emissions data, and unlawful waste management.
Public health	Breaches of pharmacovigilance obligations, unlawful marketing of medicinal products, and counterfeit products.
Consumer protection	Unfair commercial practices and misleading claims concerning safety or quality.
Protection of privacy and personal data; security of network and information systems	Unlawful processing of personal data, failure to report significant personal-data breaches, and non-compliance with cybersecurity requirements.
The Union's financial interests	Fraud, corruption or misuse of EU funds and subsidies.
Internal-market rules, including competition and State aid, and national corporate-tax rules	Cartels, abuse of a dominant position, unlawful State aid, and aggressive tax structuring contrary to national implementing rules.



2.4 Reporting channels

Larger private companies with more than 50 employees must establish and operate internal channels for reporting suspected wrongdoing. This rule also applies to the public sector, although the Directive allows certain exceptions for smaller municipalities. Internal channels must enable secure reporting. This means protecting the reporting person's identity and ensuring that unauthorised staff cannot read or access the information. The organisation must designate an impartial person or department to handle the report and communicate with the reporting person.

External channels exist alongside internal ones. Member States must designate competent authorities to receive and handle such reports. Their channels must be independent and autonomous.

A reporting person is not required to use an internal channel first. They may decide to report wrongdoing directly to the competent external authority. The Directive nevertheless encourages internal reporting where the breach can be addressed effectively within the organisation and the reporting person considers that there is no risk of retaliation.

The Directive also sets deadlines. As a rule, the reporting person must receive an acknowledgement of receipt within seven days. For an internal report, they must generally receive feedback no later than three months. The deadline for an external report is likewise three months, although in duly justified cases it may be extended to six months.

2.5 Public disclosure, or when to go to the media?

In some cases, reporting persons may decide to disclose wrongdoing to the media and the public. It is important to emphasise that, before doing so, they should ensure that they have reported the wrongdoing through the usual channels and retain evidence that no response was received.



The Directive also provides for cases in which a person approaches the media first because they consider that there would otherwise be an imminent danger to the public interest. In other words, they decide to go public after learning that something dangerous to health, the general public or the environment is about to occur. They may likewise opt for public disclosure if they believe there is a risk of retaliation.

‘Public disclosure is not the first route; it is an exception.’

2.6 Protecting the reporting person’s identity

Individuals must be protected after reporting suspected wrongdoing. Their identity must be carefully safeguarded, and only persons authorised to receive and handle reports may access their name and personal details. Moreover, a person authorised to handle reports may not disclose the reporting person’s identity without their consent, except where an exception applies—for example, in judicial proceedings or where disclosure is required by law. The reporting person must be informed in advance of such disclosure.

2.7 Protection against retaliation and support for reporting persons

A reporting person must not be punished or placed at a disadvantage because they made a report. This means more than prohibiting dismissal by the employer. Retaliation may also include:

- transfer to a less favourable position,
- denial of promotion opportunities,
- an adverse performance assessment and denial of promotion,
- intimidation, harassment or discrimination,
- termination of a contract or damage to reputation

Covert forms of pressure that are difficult to detect are likewise prohibited, even though the reporting person can see and feel the changes in the working environment. Examples include changing their working hours, omitting them from invitations to important meetings, isolating them, assigning less important duties and removing more significant responsibilities. The Directive also assists reporting persons in these situations. If, for example, a reporting person is transferred to a less favourable position, the person who took that measure must prove that the transfer was not prompted by the report of wrongdoing. Reporting persons must also be able to obtain independent information about their rights, available protection and procedures, including legal and psychological assistance.

2.8 Penalties

Whistleblower protection would mean little if breaches of that protection had no consequences. The Directive therefore requires Member States to provide for penalties against those who hinder or attempt to hinder reporting, retaliate against reporting persons, bring vexatious proceedings against them, or disclose their identity in breach of the rules. Penalties are also envisaged for anyone who knowingly reports or publicly discloses false information.



An important distinction must be made here: reporting persons are not penalised merely because their information subsequently proves incorrect. If they had reasonable grounds to believe that the information was true when they reported it, they may still qualify for protection. It is entirely different when someone knows that information is untrue but nevertheless deliberately reports it or publicly discloses it as true. The Directive provides for penalties in such cases.

2.9 What about fields that already had their own rules?

The Whistleblower Protection Directive was not the first piece of European legislation to regulate the reporting of wrongdoing. In certain fields, specific rules existed even before its adoption in 2019. Such arrangements apply, for example, to financial services and certain areas of transport and aviation.

Those specific rules did not disappear with the new Directive. Where specific European rules on reporting wrongdoing already exist for a particular field, they continue to apply.

It is therefore particularly important for reporting persons to know that, in addition to the Directive's general rules, specific rules may apply to their field. The fundamental rights discussed in this handbook are important irrespective of the field in which the wrongdoing occurred. Freedom of expression, fair working conditions, the proper handling of reports and access to legal remedies are relevant not only to reporting persons in a particular sector, but form the broader framework for their protection.



3. The Charter of Fundamental Rights of the European Union: Why does it matter for reporting persons?



The EU Charter of Fundamental Rights is the document that laid the foundations for rights in the European Union. To give a brief historical overview, the Charter of Fundamental Rights of the European Union was proclaimed in 2000 and acquired the same legal value as the EU's founding Treaties when the Treaty of Lisbon entered into force on 1 December 2009. It is divided into six substantive titles—Dignity, Freedoms, Equality, Solidarity, Citizens' Rights and Justice—which bring together civil, political, economic and social rights in a single instrument.

The rights of greatest relevance to our handbook and guidelines include freedom of expression, the right to fair working conditions and the right to judicial protection. The Whistleblower Protection Directive is itself part of EU law. When Member States transposed the Directive's rules into national law, they were required to respect fundamental rights. This does not, however, mean that the Charter may be invoked in connection with every instance of wrongdoing. Where national whistleblower-protection legislation is unclear, the Charter assists by serving as a standard for interpretation. Where a provision implementing the Directive cannot be reconciled with a Charter right, the Charter takes precedence. In legal terms: 'Under Article 51(1) of the Charter, its provisions are addressed to the institutions and bodies of the European Union and to the Member States only when they are implementing Union law. Since Directive (EU) 2019/1937 is itself an act of Union law, and national transposition measures implement that Directive, the Charter applies in full when national whistleblower-protection legislation is interpreted and applied.'

This is not a peripheral technical detail. It means that, where national whistleblower-protection legislation is unclear or a public authority or national court has discretion in applying it, the Charter serves as a binding standard of interpretation. Where a provision of national law implementing the Directive cannot be reconciled with a Charter right, the Charter takes precedence.



Professionals advising on whistleblowing matters therefore have a direct interest in understanding not only what national transposition legislation provides, but also which Charter right underpins it. The Directive and the Charter are fully aligned in respect of the four articles explained here. The Charter provided their foundation, while the Directive gives them concrete effect.

3.1 How may Charter rights be limited?

Charter rights are not absolute, since whistleblower protection sometimes requires different interests to be balanced. On one side are the rights of reporting persons; on the other are rights arising from the protection of trade secrets and personal data, the right to a good name and reputation, and the rights of those concerned by complaints or suspicions. To illustrate: an employer may require an employee to protect confidential information or trade secrets. This could be used as a pretext to silence someone who believes that such ‘confidential information’ reveals wrongdoing. The same applies to retaliation. The fact that someone has reported wrongdoing does not mean that the employer may never again transfer them, remove or add duties, or give them a poorer assessment. The principle of proportionality requires different rights and legitimate interests to be balanced. The same is true of the right to judicial protection: it does not guarantee that a person will win in court, but it does guarantee them the opportunity to defend themselves and obtain legal protection.

3.2 The Charter before national courts

What happens if the protection of a reporting person fails and the case ends up in court? May the reporting person rely on the EU Charter, or only on the national law transposing the Directive? As noted above, the answer is not always the same. Nevertheless, where a matter falls within the scope of EU law, the Charter is a document that national courts must take into account. Courts must interpret the rights under the Directive in accordance with EU law and Charter rights. Where a question of interpretation arises, it may be referred to the Court of Justice of the European Union, which will guide the national court towards the correct interpretation.

Part II — Article-by-article analysis

4. Article 11 — Freedom of expression and information

Charter of Fundamental Rights of the European Union, Article 11(1)

Everyone has the right to freedom of expression. This right includes freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

4.1 When a person decides to speak up...

Article 11 of the Charter of Fundamental Rights of the European Union guarantees freedom of expression and information. Among other things, this encompasses an individual's right to receive information and ideas and to impart them to others.

But what does this right have to do with reporting persons?

Imagine an employee of Slovenia's largest motorway company (DARS) who discovers in the course of their work that controversial contractual addenda worth millions are being signed and that tender procedures have allegedly been tailored to a particular bidder for this purpose. The employee decides to speak up, but asks: Should I speak up? Is it right to do so? Am I allowed to speak up? To whom should I communicate the information?

This is precisely where the Charter and the Whistleblower Protection Directive meet.

The Charter guarantees the fundamental right to freedom of expression and information. In the context of reporting certain breaches of EU law, the Directive lays down specific rules that enable people to communicate information through safer channels and, where the relevant conditions are met, to be protected when doing so.

This is the essence of the relationship between Article 11 of the Charter and the Directive.

The right to speak up is not sufficient in itself: freedom of expression can readily be guaranteed on paper, but in real life the decision whether to speak up about wrongdoing is often far more difficult. Our employee therefore legitimately asks who will learn of the report, whether that person will tell their manager, and what happens if the manager is involved in transactions worth millions and the manipulation of tender procedures. Can the report be sent to someone outside the organisation? Could the employee lose their job for drawing attention to corruption? Without safe reporting channels, such a person may remain silent.

Here, the Directive complements the right under Article 11 with a concrete system of whistleblower protection. It specifies who may qualify for protection, provides for internal and external reporting routes, safeguards the confidentiality of the reporting person's identity, prohibits retaliation and, under specific conditions, also protects a person who publicly discloses information.

Freedom of expression thus acquires a very practical dimension: a person needs not only the right to say something, but also: **a safe route through which to communicate the information.**



4.2 Who may qualify for protection?

The Directive does not restrict protection to employees with permanent contracts. Various people who acquire information about breaches in a work-related context may qualify for protection. They include employees, self-employed persons, shareholders, members of administrative or supervisory bodies, volunteers and trainees, and people working for contractors, subcontractors and suppliers.

Protection may also be important for someone who no longer works for the organisation, or for a person who acquired information about a breach during a recruitment process or other pre-contractual negotiations.

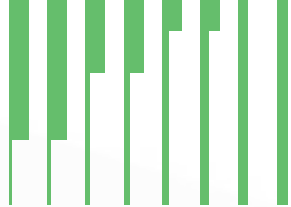
This is also important from the perspective of freedom of expression. If protection were restricted to a narrow group of employees, people whose work gives them access to important information about breaches could be left unprotected.

4.3 Must reporting persons prove that they are right, and what evidence do they need?

A person who notices wrongdoing often does not have access to all the information. They may see part of the story, but not necessarily the whole picture. They are not an investigative journalist who has been able to obtain responses from all sides. In a system with 2000 or more employees, they may simply have no access to the answer. It is therefore possible that they believe a tender procedure was tailored to a particular bidder, only for it later to emerge that this was not the case. The Directive does not require them to conduct their own investigation and conclusively prove the breach before reporting it. It requires something else: at the time of reporting, they must have reasonable grounds to believe that the information concerning the breach is true and falls within the scope of the Directive.

This is an important distinction.

In the case of our DARS employee, where public procurement procedures with a combined value of approximately EUR 9 billion are involved, an employee named Peter Verbič was dismissed after he began drawing attention to irregularities. Management consistently denied his allegations.



He did not initially enjoy protection under this Directive. Had he been protected, however, he would not automatically have lost that protection under the Directive if his suspicions had not been substantiated. What matters is that, at the time of reporting, he had reasonable grounds to believe that the information was true. But what if our reporting person lied, deliberately spread false information, or simply made a mistake? The distinction is clear. The Directive seeks to protect people who, acting in good faith or on the basis of the information available to them at the time, raised suspicions of wrongdoing even if those suspicions were not subsequently substantiated. It does not protect individuals who knew that information was untrue but reported it nevertheless. Member States must provide for effective, proportionate and dissuasive penalties in such cases. This is important because a person may suffer consequences as a result of a false report. That person, too, has the right to the presumption of innocence, the right of defence, and the right to an effective remedy and a fair trial.

A reporting person may be protected if they were mistaken. They are not protected so that they may knowingly lie.

At the next stage, our reporting person asks where they may submit information about the suspected wrongdoing. The Directive establishes two basic routes:

- internal reporting,
- and
- external reporting.

With internal reporting, a person communicates the information within the organisation. If the organisation gives its system sufficient attention, it can learn of a problem early and address it before greater harm occurs. Internal reporting is not always the most appropriate option, however. Returning to our employee Peter Verbič at the motorway company, he opted to report internally. At the time, he did not know that the service designated for whistleblowers was connected to management. The Directive encourages internal reporting where a breach can be addressed effectively within the organisation, and the reporting person considers that there is no risk of retaliation. However, it does not make protection conditional on a person always reporting within the organisation first. Reporting persons may also report information directly to the competent external authority.

This is an important way in which the Directive supports a person's ability to communicate information in practice. If only an internal route existed, people might find themselves required to report a breach to the very individuals they suspect of involvement. In Slovenia, Peter Verbič was dismissed from DARS after speaking up. [Source](#):

4.4 Confidentiality enables people to find the courage to speak up

One of the greatest barriers to reporting is the fear that the reporting person's identity will be disclosed. The Directive therefore specifically protects the confidentiality of their identity. Without their explicit consent, their identity must generally not be disclosed to anyone who is not authorised to receive reports or follow up on them. The Directive permits certain exceptions required by law, for example where disclosure is a necessary and proportionate obligation in the context of an investigation or judicial proceedings.

Why does this matter for Article 11? Because people cannot easily communicate information freely if they must also assume that their name will be disclosed unnecessarily to those concerned by the report.

Confidentiality is therefore not merely a technical rule on handling reports. It helps create an environment in which people have the courage to speak up in the first place.

4.5 What if a person wants to disclose information to the public?

In addition to internal and external reporting, the Directive also regulates the public disclosure of information—in other words, the decision to bring the story to light with the help of the media. Stricter conditions apply in this context.

A person may qualify for protection if they first used the appropriate reporting channels but no appropriate action was taken within the prescribed time limits.

In certain circumstances, they may also qualify for protection when making a direct public disclosure. This may be possible, for example, if they have reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest, or if, in the event of external reporting, the particular circumstances create a risk of retaliation or a low prospect of the breach being effectively addressed. This is an important boundary on freedom of expression within the framework of the Directive. The Directive does not provide that every public disclosure of any information is automatically protected. For protection to apply to a public disclosure, the conditions laid down in the Directive must be met.

4.6 What does this look like in practice?

As noted above, Peter Verbič observed that tender procedure worth millions had been tailored to a particular bidder. He could report his observations through the internal reporting channel. If he did not trust that channel, the Directive would allow him to report the matter to the competent external authority—in Slovenia, the Commission for the Prevention of Corruption. His identity must not be disclosed arbitrarily in the process.

If he decided to provide the information to the media or otherwise disclose it publicly, it would be necessary to determine whether the conditions for protection in the case of a public disclosure were met. Under certain conditions, the Directive also protects a reporting person who provides information directly to the media. This is possible even without prior internal or external reporting where, for example, the reporting person has reasonable grounds to believe that there is an imminent or manifest danger to the public interest, that external reporting would expose them to a risk of retaliation, or that the breach would be unlikely to be addressed effectively.

I would then add another short paragraph, as it provides a very good link to Article 11 of the Charter: The connection with freedom of expression is particularly evident here. The Directive expressly emphasises the importance of whistleblowers as sources for investigative journalists and the importance of protecting them so that investigative journalism can fulfil its watchdog role in a democratic society. From the discussion above, we can identify what the Directive does on the basis of the Charter, which was adopted 10 years earlier.



In the field of whistleblower protection, the Directive makes the rules considerably more concrete. It specifies who may qualify for protection and under which conditions, how information may be reported within or outside an organisation, how the reporting person's identity must be safeguarded, and when protection may also apply to a public disclosure.

The relationship between Article 11 and the Directive is therefore not merely theoretical. It can be summarised as follows.

The Charter protects a person's right to receive and impart information. The Directive helps create the conditions in which a reporting person can actually communicate certain information about breaches more safely.

In practice, this is one of the ways in which the Directive supports the exercise of freedom of expression and information in the field of whistleblower protection.

Example from national implementation — Slovenia:

Slovenia transposed Directive (EU) 2019/1937 through the Reporting Persons Protection Act (ZZPri), which regulates internal and external reporting routes and the conditions for public disclosure. For external reporting, a reporting person approaches the competent authority designated for the field in which the breach occurred. The Commission for the Prevention of Corruption (KPK) also plays an important role in implementing the reporting-person protection system.

5. Article 31 — Fair and just working conditions

Charter of Fundamental Rights of the European Union, Article 31

1. Every worker has the right to working conditions which respect his or her health, safety and dignity. 2. Every worker has the right to limitation of maximum working hours, to daily and weekly rest periods and to an annual period of paid leave.

5.1 They spoke up. What happens the next day?

As a rule, a reporting person who has reported wrongdoing must return to work the next day. They must face the same colleagues and the same managers about whom they may have reported, and they must continue doing their job. They may also have to work with the people concerned by their report. It is precisely then that a new question arises: what will happen to me because I spoke up?

Article 31 of the Charter provides the broader framework for protecting people in the workplace. The Directive lays down a very specific rule for reporting persons: they must not be subjected to retaliation because they made a report or public disclosure, as happened to our employee at the motorway company, who was dismissed (and did not have whistleblower protection).

This is one of the most important aspects of whistleblower protection.



5.2 What is retaliation?

Retaliation is most easily understood as a punishment or detrimental consequence that a person experiences because they spoke up. In our case, it took the form of dismissal; in someone else's case, it may take another form. The Directive lists possibilities including demotion or withholding of promotion, transfer to another position, reduction in wages, changes in working hours, withholding of training, a negative performance assessment, disciplinary measures, intimidation, harassment, exclusion, discrimination, unfair treatment, early termination of a fixed-term contract, damage to reputation, and financial loss. The list is not limited to these examples. This matters because retaliation may be far less visible than dismissal. A person may still sit at the same desk, receive the same pay and officially hold the same position, while their actual situation has changed completely following the report. Employers will often say that 'they did not dismiss the person; they merely transferred them.' Imagine an employee who has managed important projects for several years. After the employee reports wrongdoing, the employer does not terminate their contract. Instead, the employer takes away their projects, excludes them from meetings and transfers them to a role with less responsibility. Formally, the person remains employed. Does this mean that no retaliation occurred? Not necessarily. This is precisely why the Directive frames the prohibition broadly. Article 19 prohibits not only dismissal but 'any form of retaliation, including threats of retaliation and attempts of retaliation'. In practice, therefore, we must consider the wider picture.

What happened to the employee before the report? What changed afterwards? Is there a comprehensible and demonstrable reason for the change in their situation, or did the less favourable treatment begin precisely after they raised concerns about wrongdoing?

This clearly demonstrates the link with Article 31 of the Charter. It is not enough to enable a person to make a report. If they can then be punished for doing so through demotion, isolation, poorer working conditions or dismissal, their protection is very weak in practice. An employer may, however, make legitimate decisions.



This does not mean that a reporting person becomes untouchable after making a report, and it is important to say so clearly. If an employee breaches their employment obligations, performs poorly, or there are other legitimate grounds for an employer's decision, the Directive does not in itself prevent the employer from taking action against them merely because they once made a report. The crucial question is different: Was the detrimental measure taken because of the report? The Directive does not grant reporting persons general immunity from the ordinary rules governing the employment relationship. It protects them against being placed at a disadvantage because of a report or public disclosure. This distinction is extremely important for both the reporting person and the employer.

Proving retaliation

This brings us to one of the Directive's strongest protective mechanisms. Retaliation is often very difficult to prove. An employer will almost never write in a notice of dismissal: 'We are dismissing you because you reported wrongdoing.' It will cite another reason.

In the case of our employee Peter Verbič, the employer abolished his position and gave 'dismissal on business grounds' as the reason. How, then, is a reporting person to prove that their report was the real reason? Verbič is currently seeking to prove this in court because he wants his position back. Article 21 of the Directive therefore lays down a special rule for proceedings before a court or another authority. If a reporting person establishes that they made a report or public disclosure and subsequently suffered detriment, it is presumed that the detriment was imposed in retaliation for the report.

The person who took the detrimental measure must then prove that it was based on duly justified grounds. Put simply:

“The reporting person does not have to prove the employer’s entire underlying motive. Once the report and the detriment have been established, the burden of proving that the measure was duly justified shifts to the other party.”

Protection therefore does not simply mean prohibiting dismissal. In short, reporting persons must have access to information about the procedures, as well as to advice, legal assistance and protection against retaliation. Member States may also provide financial assistance and psychological support in the framework of legal proceedings. Article 21 requires access to remedies against retaliation, including the possibility of interim relief pending the resolution of proceedings, in accordance with national law. The Directive also requires access to legal remedies and full compensation for damage caused by retaliation, in accordance with national law. This matters because a prohibition on paper is not enough in itself. If someone loses their job because they made a report and then has to wait several years for court proceedings to conclude without access to effective interim relief, the damage may already have been done. After losing their job, an individual will often lack the resources to pursue legal proceedings. This is why the Directive provides for legal protection.



6. Article 41 — Right to good administration



Charter of Fundamental Rights of the European Union, Article 41(1)

Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union.

6.1 After submitting a report



Under Article 11, we followed a reporting person who had decided to speak up. Under Article 31, we looked at how the system must protect them against retaliation. Now let us consider what happens to the report itself once the reporting person has written it. Peter Verbič publicly stated that he had used the internal reporting channels of the Motorway Company in the Republic of Slovenia (DARS). He knew who would receive the report, but hoped that the person was trustworthy. What if they were not? Would they bury his report in a drawer or actually deal with it? What if it reached someone connected to the people concerned by the report? Above all, would anyone deal with the report at all?

A reporting channel is not simply an email address to which an employee/reporting person/whistleblower sends a report. There must be a procedure for handling that report. The Directive lays down several basic rules.

Someone must receive the report, protect its confidentiality, handle it impartially, take appropriate action and provide feedback to the reporting person. This is precisely where the Directive sets out in very concrete terms how the system must operate. For internal reporting channels, the Directive requires, among other things, a secure channel that safeguards the confidentiality of the reporting person's identity, acknowledgement of receipt within seven days, the designation of an impartial person or department competent for follow-up, diligent follow-up and, as a rule, feedback to the reporting person no later than three months.



Article 41 of the Charter concerns impartial, fair and timely handling. In the field of reporting breaches, the Directive establishes highly specific procedural requirements that help translate those values into the operation of reporting channels. Seven days is not an insignificant deadline. Someone may have spent months summoning the courage to report; when they finally do so, they may then wait and wait. Someone may have buried the report in a drawer, and the reporting person does not know whether it was even received or is being handled. This is precisely why the Directive provides that, for internal reporting, the reporting person must generally receive an acknowledgement of receipt within seven days. An acknowledgement may appear to be a minor administrative detail. For the reporting person, however, it means something very concrete:

“Someone has received my report, and the procedure has begun.”

A similar rule applies to external reporting. As a rule, the competent authority must acknowledge receipt within seven days. There are, however, two exceptions: where the reporting person expressly requests otherwise, or where the competent authority reasonably believes that acknowledging receipt would jeopardise the protection of the reporting person’s identity.

Even this small example shows how the Directive seeks to strike a balance between an effective procedure and the protection of the individual.

6.2 Who handles the report?

Once the report has been received, the work has only just begun. The Directive uses the term “follow-up”. An impartial person must be designated to handle the report; throughout the procedure, that person must remain in contact with the reporting person and may ask them for further clarification and information.

Let us return to our reporting person, Verbič. As he told the media, after reporting through the internal channel he discovered that the channel was not independent of the people concerned by the report. For internal reporting, the Directive requires the designation of an impartial person or department competent for following up on reports. That person or department must maintain communication with the reporting person, request further information from them where necessary, and provide feedback. For external reporting, the Directive requires independent and autonomous external reporting channels. In Slovenia, this is the Commission for the Prevention of Corruption. Once the competent authority receives a report, its task is not complete; it must also keep a record of it.



The allegations in the report must be properly examined and the necessary follow-up assessed. The Directive requires diligent follow-up to reports made through both internal and external channels. During the procedure, the reporting person may also receive questions or a request for further information. The Directive envisages communication between the person handling the report and the reporting person. A reporting person will often know only part of the story. During its examination, the authority or organisation may find that it needs additional clarification: where the reporting person saw the document, which event it concerns, who was present, or which contract they are drawing attention to. In summary, the important point here is that, under the Directive, a reporting person must feel that the system has heard them.

If, under Article 11, we said:

- **“A person must be able to speak up”,**

and, under Article 31:

- **“They must not become a target for doing so”,**

then, under Article 41, we can say:

“When a person speaks up, there must be someone on the other side who truly listens and handles their report fairly, impartially and promptly.”

A reporting channel without meaningful follow-up is merely an address to which a person sends their story. The Directive seeks to ensure that there is also a procedure behind that address.

Example from national implementation :

In Bulgaria, the Commission for Personal Data Protection is the designated institution for handling reports.

In Bulgaria, the Commission for Personal Data Protection (CPDP) is the central body responsible for the external reporting channel and for providing protection to reporting persons under the Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches, (Whistleblower Protection Act). Depending on the subject matter of a report, the CPDP may transmit it to the relevant competent authority for follow-up.

The Ombudsman is the institution tasked with monitoring how the CPDP handles reports, including overall effectiveness of the procedure. This monitoring, alongside the yearly auditing reports published by the Ombudsman on the functioning of the CPDP as an external reporting channel, are an example of good practice of the application of Art. 41 of the Charter.

Under Ordinance No. 1 of 27 July 2023, every report reaching CPDP through the external channel must be logged and assigned a unique identification number (UIN) within seven days of receipt, which is the same acknowledgment deadline as set by the Directive. This way, the reporting person is given confirmation that their report has actually entered the system.

Internally, this used to involve a screening step: staff from the relevant directorate passed each incoming report to the director, who assessed whether it fell within the scope of Art. 3 of the Whistleblowing Act and whether the sender qualified as a reporting person under Art. 5, before an identifying number was generated. This screening step has now been removed. Every incoming report is now registered and assigned an identifying number directly. Once registered, cases are distributed automatically and at random among staff of the directorate within CPDP responsible for the external reporting channel through a dedicated case-management system. The assigned officer must complete a regularity, admissibility, credibility and plausibility check within seven days.

In the case of Nataliya Stancheva, a nurse at the Kozloduy Nuclear Power Plant whose case we will explore in further detail in the following sections of this document, a case expert was assigned promptly and formal confirmation of her protection status was issued within 13 days, which is within statutory window.

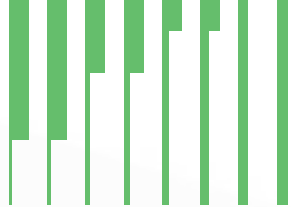
The Ombudsman's two most recent audits however found that this level of responsiveness is not consistent.

Reports sent to CPDP's general mailbox are frequently misdirected internally to the case registrar's personal inbox rather than the dedicated directorate's mailbox, producing registration delays in at least eight reviewed cases as of 2025. Another example is that of a case, when a report was automatically assigned to a staff member who had left the institution eight months earlier. It took nine days for this error to be corrected.

Beyond intake, the audits of the Ombudsman also found no systematic mechanism for verifying whether retaliation follows a protected report, and no remedial measure had been applied in a single case in the three years since the Act entered into force.

These findings suggest that on paper, the registration architecture is procedurally sound: the seven-day deadlines, the system generating unique identification numbers automatically, as well as the randomized case assignment. Its reliability in practice however still depends heavily on many additional and manual in-between steps (for example, the general mailbox handoff, staff-record maintenance to ensure assignment to a working staff member) that sit outside the formal procedure and are where most of the observed failures occur.

One more weak point explored in the audits of the Ombudsman is the communication and overall dynamic between an obliged entity's internal channel (whether it be public or private) and CPDP as the external authority for reporting breaches.



In at least seven reviewed cases, a report submitted through the internal channel of a competent authority under Art. 20.1 of the Whistleblowers Protection Act reached CPDP only after a significant delay in forwarding.

For example, a report submitted through an administration's internal reporting channel failed to reach CPDP due to a technical email-forwarding fault. Despite indications that the transmission had failed, the officer responsible for the internal channel made no follow-up contact with the CPDP to confirm receipt. The report arrived 14 days later. In the meantime, the reporting person was dismissed and was initially unable to invoke the protections available under the Whistleblowing Act.

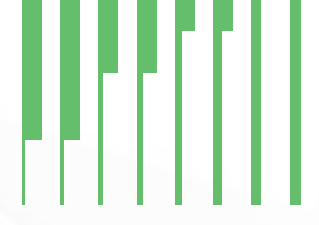
Another report illustrated in one of the audit reports of the Ombudsman showcased another example of delays. A report submitted to a public body was forwarded to CPDP 22 days after receipt, which is well outside the seven-day forwarding deadline set by Art. 12.1 of Ordinance No. 1. CPDP took no apparent action in response to the delay, despite the risk this created for the reporting person's rights and protection.

Both of these examples point to the same structural gap: the seven-day forwarding deadline depends entirely on the internal channel operator recognising a failed or delayed transmission and proactively confirming receipt with CPDP. From merely a technical fault, as is the case with an email that did not reach the intended addressee within the legal deadline, this translates directly into added vulnerability to the reporting person and uncertainty when it comes to their rights and their protection.

While court rulings on the topic of whistleblowing are still scarce in Bulgaria, one such case illustrates how good administration includes judicial interpretation granting protection to whistleblowers and those related to them rather than strictly sticking to the wording in the law alone. An employee at a commercial company was dismissed in May 2024, shortly after being reassigned to a newly created position that was eliminated only a few weeks later. After being dismissed from her position, her former husband, who was then a member of the company's board, filed a report under the Whistleblowing Act and sent it to the Commission for Personal Data Protection as the responsible external reporting channel. In his report, he included information on the creation of the post she was moved to before being made redundant, in addition to a documented conflict between him and the company's management which took place prior to her dismissal.

What the court found was that although the redundancy was genuine in its formality, the employer had exercised in bad faith its right to restructure. The employee was the sole staff member of the position created specifically for her. This move is seen as specifically and directly aiming to terminate her employment alone rather than genuinely restructuring and reorganizing the company. Through these actions, the employee became an indirect casualty of the documented conflict between her former husband and the company's board, as documented in the court ruling.

A crucial element of this ruling is the fact that it was not the employee herself who filed the report under the Whistleblowing Act but rather her former husband. She qualified for protection as a person connected to the reporting person. The court explicitly extended the law's protective scope to include her in the labour dispute. The reading was reinforced with two rulings of the Supreme Court of Cassation from 2024.



Rather than confining itself to only the formal legality of the dismissal, the court went further and did a comprehensive examination of the employer's purpose and manner of conducting the dismissal. This resulted in the court ordering an annulment of the dismissal, reinstatement to the employee's previous post despite it no longer existing, in addition to compensation for the period of unemployment. This comprehensive review conducted by the courts is what turns legal obligations into truly effective protection and remedy as per Art. 41 of the Charter.

GREECE

The external reporting channel in Greece (Articles 11–12, Law 4990/2022)

Law 4990/2022 (Government Gazette Á 210/11.11.2022) transposed Directive (EU) 2019/1937. It established internal channels (mandatory for public bodies and for private companies with 50+ employees, and for firms in finance, transport and environment regardless of size) and a single external channel: the National Transparency Authority (EAD), an independent authority created by Law 4622/2019 (which consolidated the former General Inspector of Public Administration, several inspectorate corps, and the General Secretariat for Anti-Corruption).

Article 11 designates the EAD as the competent authority to receive, manage and monitor external reports; its staff are specially trained and dedicated to report handling. Article 12 sets the procedure and timelines:

- Reports may be submitted in writing, orally (telephone or voicemail), or via the accessible electronic platform, and by in-person meeting on request.
- Acknowledgment of receipt within 7 working days (unless the reporter requests otherwise or acknowledgment would jeopardise the protection of their identity).
- Prioritisation of serious violations or breaches of essential provisions.
- Archiving where the report discloses no EU-law breach, is manifestly minor/trivial, or is repetitive without significant new information.
- Transfer to competent national/EU bodies where the EAD lacks competence, with notification to the reporter.
- Feedback to the reporter within a reasonable period not exceeding 3 months, or 6 months in duly justified cases.
- Communication of the final outcome of any investigation triggered by the report.

7. Article 47 — Right to an effective remedy and to a fair trial

Charter of Fundamental Rights of the European Union, Article 47(1)–(2)

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal ... Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law.

7.1 What if protection fails?

Article 47 provides that everyone whose rights and freedoms guaranteed by European Union law have been violated has the right to an effective remedy before a tribunal.

It also guarantees the right to a fair and public hearing within a reasonable time before an independent and impartial tribunal, and the possibility of being advised, defended and represented. Subject to certain conditions, legal aid must also be made available to people who lack sufficient resources where such aid is necessary to ensure effective access to justice.

7.2 A real-world example

Slovenia has also had the case of one of its best-known whistleblowers, Ivan Gale, who spoke out in 2020 during the epidemic about alleged corruption in the procurement of protective equipment and lost his job and income. Because the story received exceptional media attention, many prominent lawyers offered him free legal assistance. This is not always the case, however. Verbič, for example, did not have that option. If he had been required to wait until the proceedings were finally concluded, with no possibility of interim relief, he could in the meantime have lost his income and professional standing and suffered substantial harm. Even if he had won in court several years later, it might not have been possible simply to erase all the consequences. Article 47, however, also raises another question: what are the rights of the person accused of breaches? That person, too, has the right to an effective remedy and a fair trial. The Directive is clear:

The Directive makes clear that Member States must ensure that persons concerned fully enjoy, in accordance with the Charter, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of defence, including the right to be heard and the right to access their file. This is an important balance: a reporting person must be able to raise suspicions of a breach safely, but the report itself does not mean that the person concerned is guilty.

7.3 When a report concerns another person

We have already addressed this point. In protecting the reporting person, we must not forget the person concerned by the report. That person also has rights and, above all, benefits from the presumption of innocence. A report in itself may amount to a serious allegation, but it does not prove that the person committed the breach. The Directive's task is therefore clear: to protect both sides. It protects the reporting person against retaliation, while the person concerned has the right to a fair procedure and is presumed innocent until a court determines their guilt. It is also important to protect that person's identity while the procedure is under way.

One further point about the procedure is important. The fact that a reporting person reports suspicions of wrongdoing does not mean that they will ultimately be proved right. Nor does the Directive require the reporting person to prove the breach when making the report. What matters for protection is that, at the time of reporting, they had reasonable grounds to believe that the information was true. A reporting person does not lose protection if it later emerges that they were mistaken. The situation is, of course, different where someone knowingly disseminates falsehoods or reports something they know to be untrue.

7.4 What if protection of the reporting person fails?

Despite all the rules, a reporting person may still be subjected to retaliation, the most serious form of which is losing their job. The Directive prohibits such conduct, but some people will still act unlawfully because they are counting on lengthy litigation, or perhaps on no longer being in office by the time the matter is decided and leaving the problem to someone else.



The reporting person must therefore be able to defend themselves. This is where Article 47 of the Charter, which guarantees the right to an effective remedy and a fair trial, becomes important. The Directive makes that protection more concrete. The most important issue is proving retaliation. Imagine that a worker, like Peter Verbič in our example, reports wrongdoing and is dismissed a month later. They will find it difficult to prove the causal link to the actions of management or the director. The Directive therefore provides that, where a reporting person suffers a detriment after reporting, it is presumed to have occurred in retaliation for the report. The reporting person must also have access to remedies, interim relief, advice and coverage of costs. Court proceedings can take several years.

The reporting person must also have access to remedies against retaliation. Interim relief must be available during court proceedings. This is particularly important because proceedings can take a long time, while the consequences for the reporting person arise immediately. The Directive also enables reporting persons to claim full compensation for damage and to have continuing access to information.

8. How the four rights interact

The four Charter articles discussed in Part II do not concern four separate areas. They interconnect sequentially, and often simultaneously, throughout the course of an individual case. Understanding this interaction helps practitioners see why a problem at one stage will usually deepen the problems at the next.

Stage of the reporting procedure	Charter right(s) primarily at issue
Deciding whether and how to report	Article 11 — Is reporting protected, and which route should I take?
Submitting a report and awaiting acknowledgement of receipt	Article 41 — Is the report being handled with the diligence, impartiality and timeliness required by good administration?
Continuing to work during and after the handling of the report	Article 31 — Are the reporting person's dignity, health and safety at work being safeguarded?
Challenging a failure of protection	Article 47 — Is an effective and timely remedy available before an independent tribunal?



In informal language, we can summarise the articles as follows:

- Article 11: Speak up about wrongdoing!
- Article 31: I must not become a target for speaking up!
- Article 41: Someone must handle my report properly and provide me with feedback!
- Article 47: If my rights are not protected after I speak up, there is a route to an effective remedy.

9. Part III — Examples from everyday working life

Although we have already used real cases along the way to explain how the system operates, this chapter examines the subject in greater detail.

9.1 Suspected manipulation of a public procurement procedure

The Slovenian mask scandal

In spring 2020, during the emergency, Slovenia rapidly purchased face masks, ventilators and other protective equipment outside the usual public procurement procedures. Ivan Gale was Head of General Affairs at the Agency of the Republic of Slovenia for Commodity Reserves. When its director, Anton Zakrajšek, fell ill with COVID-19 in March 2020, Gale stood in for him and identified suspected manipulation of a public procurement procedure in favour of one bidder in the procurement of medical equipment. He recorded statements made by the minister and decided to take the evidence to the media.

The case is important because, when raising concerns, a reporting person often does not have all the evidence and cannot know what an investigation will reveal. The Directive therefore makes protection dependent on whether, at the time of reporting, the person had reasonable grounds to believe that there was a genuine breach falling within the scope of the Directive — not on whether every allegation is subsequently substantiated. In November 2020, following its review of the procurement procedures, the Commission for the Prevention of Corruption (KPK) identified corruption risks at every stage of the procedures and opened 21 investigations into eight public officials. Gale, however, was dismissed after appearing on television. On 9 October 2020, the Agency of the Republic of Slovenia for Commodity Reserves summarily dismissed him on the grounds that he had falsified a business document; a criminal complaint followed. Gale challenged the dismissal as an act of retaliation, and the dispute ended in a court settlement in April 2022 (a payment of approximately EUR 54,000 gross). Interestingly, he was later himself investigated by the KPK — confirming that the question of his protection must be assessed separately from whether all his allegations were ultimately substantiated in full. This is precisely why the Directive prohibits retaliation — not only dismissal, but also the removal of duties, an adverse performance assessment, intimidation and exclusion.

If the case were assessed under the Slovenian Reporting Persons Protection Act, two questions would therefore be examined separately: (1) whether he had reasonable grounds for suspicion when he reported, and (2) whether his subsequent dismissal — which followed relatively soon after his television appearance — was connected with the report.



Gale spoke out in 2020, before the Slovenian Act was adopted in 2023, so his position at the time cannot be assessed under today's rules. His case — involving dismissal, litigation and settlement — nevertheless clearly illustrates the central question: can an employee raise a suspicion without having to prove the whole case themselves, and what happens to them when they speak up?

9.2 Environmental example BULGARIA and GREECE

In Bulgaria there haven't been any whistleblowing cases in an environmental context as of yet. The closest are environmental NGOs issuing complaints directed at the European Commission, which does not qualify as a relevant and appropriate example for the purposes of this deliverable.

The Bulgarian experience offers a relevant perspective on the relationship between environmental reporting, public-interest disclosures and protection against retaliation. Although the available publicly documented examples do not readily establish a post-2023 case that can be presented as a complete application of the whistleblower protection framework in the environmental sector, earlier cases involving employees raising concerns about environmental and public-safety risks illustrate the importance of the safeguards subsequently introduced by Directive (EU) 2019/1937 and the Bulgarian Whistleblower Protection Act.

One such example is the case concerning the storage of carbon disulfide at the former "Himko" chemical plant in Vratsa, where an environmental inspector raised concerns about the risks associated with the substance and subsequently faced adverse employment measures. The case illustrates the importance of effective protection for persons who report environmental risks in the context of their work.

Environmental whistleblowing: the Asopos River / Oinofyta chromium scandal



The Asopos river in Boeotia/Attica became one of Greece's most notorious cases of industrial pollution. After Oinofyta was designated an industrial zone, hundreds of factories discharged untreated waste, and the aquifer and drinking water in Oinofyta, Dilesi and the wider Oropos area were contaminated with hexavalent chromium (Cr-VI), a carcinogen.

In 2007 Greece's Ministry of Environment, Regional Planning and Public Works imposed fines on 20 industries for discharging waste with high levels of hexavalent chromium into the Asopos river (documented in Linou et al., Environmental Health 2011). The environmental inspectorate reported carrying out more than 150 inspections and proposing fines totalling around €3.28m (per the head of inspectors, I. Dermitzakis). In July 2013 the National Technical University of Athens (LIFE-CHARM programme) measured Cr-VI concentrations up to 7,200 µg/L; these studies were classified as confidential despite their public-health significance. More recent NGO monitoring (PAKOE, 2024) and a 2020 University of Athens study on PFAS contamination — which the regional authority reportedly withheld — show the pollution and information-suppression problems persist.

The public-health dimension was documented by Professor Athena Linou (University of Athens Medical School). Her peer-reviewed study — Linou et al., "Oral ingestion of hexavalent chromium through drinking water and cancer mortality in an industrial area of Greece," Environmental Health 2011;10:50 — found a Standardized Mortality Ratio for primary liver cancer of 1104 (95% CI 405–2403, $p < 0.001$), roughly 11 times the reference rate, among Oinofyta residents (1999–2009) compared with the Voiotia prefecture, alongside elevated kidney and other cancers. In 2008 the Municipality of Oinofyta was convicted by the Thebes Court of First Instance (case handled by EKPOIZO legal counsel Dimitris Spyarakos) and ordered to supply safe drinking water.

This case predates Law 4990/2022 but illustrates precisely why the Directive was needed: those who exposed the contamination (inspectors, scientists, local activists) faced obstruction and the suppression of official studies, with no dedicated whistleblower protection regime in place. It is best framed as a citizen/inspector/scientist exposure case rather than a single-employee workplace whistleblower case.

9.3 Example from the pharmaceutical or financial sector

In the healthcare sector, an important whistleblowing real-world case which gained traction and popularity in Bulgaria is that of Nataliya Stancheva - a nurse who filed numerous requests to the Kozloduy Nuclear Power Plant, her employer, for access to public information related to the Power Plant's medical center and activities. She did so under the Access to Public Information Act, which came into effect in 2022. Mrs. Stancheva also filed such requests to other institutions, including the Ministries of Health, Labour, Environment and Waters, as well as the Regional Health Inspectorate in Vratsa, among others. What she was concerned about more specifically was the fact that the occupational medicine office on the premises of the Nuclear Power Plant was operating as an unregistered medical facility and providing medical services to employees. After receiving the requested public information, she sent several alerts to different institutions, including the Ministry of Health and the Regional Health Inspectorate in Vratsa.

After inspections by several regulators, including the National Center for Radiobiology and Radiation Protection, the Medical Supervision Agency, and the Regional Health Inspectorate in Vratsa, the facility was closed (though reopened briefly afterwards). Their inspections resulted in the issuing of notes that the medical facility was not registered under the Law on Medical Facilities. As retaliation, her employer - the Kozloduy Power Plant - pursued a compensation claim against her in July 2023 amounting to 500 000 BGN (approximately 255,000 EUR). The Power Plant claimed that Mrs. Stancheva had disseminated false information, acted in bad faith, as well as abused rights - specifically Art. 45 and 56 of the Constitution. This was characterized as a SLAPP case by several non-governmental organizations. It took serious public pressure, including protests and several statements by civil society organisations, and a new management of the Power Plant for the claim to be withdrawn in January 2024. Mrs. Stancheva was also then reinstated to her post after having been fired following her filing the public information requests.

At the beginning of 2024, Mrs. Stancheva decided to approach the Commission for Personal Data Protection - the national external reporting channel and competent authority under the Whistleblowing Act. Shortly after approaching the Commission, Mrs. Stancheva was assigned a case expert. She also received a formal letter by the Chairman of the Commission for Personal Data Protection confirming her protection status within 13 days. It is important to note that her husband also received protection a few days after her. All of these actions and the rapidity of the responses indicates that the CPDP as an external reporting channel is technically capable of sustaining follow-through.

Mrs. Stancheva's case should not be however mistaken for evidence that the reporting system and architecture put in place in Bulgaria delivers effective protection overall. Independent audits of the CPDP's practice as an external reporting channel, carried out by the Ombudsman for 2024 and 2025, tell a more cautious story.

The 2025 audit found progress on the disclosure of reporting persons' identities, which had effectively been the rule rather than the exception, is now being limited through a newly introduced protection certificate. But it also found that protection tends to end once a certificate is issued, which should be rather when protection begins. There is no risk assessment and no mechanism to check whether retaliatory action has actually been taken against the protected person, and there is no coordinated response among the institutions involved.



More than three years after the law entered into force, the audit found that remedial measures had not been applied in a single case, which it attributes to the absence of any clear procedure or shared understanding among the competent authorities. The mechanism meant to restore the rights of someone who has already suffered retaliation are malfunctioning. Support to reporting persons also remains largely administrative, mostly referrals, notifications and provision of standard information. There is no individualised assessment of what a given person needs. Additionally, despite being one of the most consistently cited gaps, there is still no dedicated free legal aid for whistleblowers. Mrs. Stancheva, for example, accrued 25 000 BGN (around 12 500 EUR) for a lawyer in relation to the case pursued by her employer. The Supreme Court of Cassation did not recognize the full cost incurred by Mrs. Stancheva, instead awarding her only 10 000 BGN (about 5 000 EUR) of the full amount. Civil society organizations started a fundraising campaign to help the medical nurse cover the remaining costs.

Greece

Pharmaceutical whistleblowing: the Novartis scandal

The Novartis Greece case is Greece's most prominent whistleblowing scandal and a paradigmatic example of retaliation. Between roughly 2006 and 2015, Novartis was alleged to have bribed Greek doctors and officials to boost sales and inflate drug prices; Greek prosecutors estimated the price-fixing cost the country around €3 billion. The case surfaced through two tracks:

- **US enforcement:** In June 2020 Novartis AG and two subsidiaries agreed to pay the DOJ and SEC US\$346.7 million in penalties and disgorgement to settle Foreign Corrupt Practices Act charges — comprising a US\$225m DOJ criminal penalty on Novartis Hellas S.A.C.I. and over US\$112m in SEC disgorgement and interest (DOJ/SEC press releases, 25 June 2020). The DOJ stated Novartis Greece "conspired...to bribe employees of state-owned and state-controlled hospitals and clinics in Greece." The US whistleblowers (identities confidential) were represented by Kohn, Kohn & Colapinto and the Greek firm Pavlos K. Sarakis & Associates; at one point a suspected whistleblower and the Greek lawyers were assigned state bodyguards owing to the intensity of attempts to unmask and retaliate against them.

- Greek protected witnesses: Two protected witnesses, initially under the pseudonyms "Aikaterini Kelesi" and "Maximos Sarafis," were later identified as Maria Marangeli (a former secretary to the Novartis CEO in Greece, protected witness from 2017) and Philistor Destempasides (a former Novartis manager, from 2018). They alleged around 10 politicians — including two former prime ministers (Antonis Samaras, Panagiotis Pikrammenos), ministers (Adonis Georgiadis, Andreas Loverdos, Evangelos Venizelos, Dimitris Avramopoulos and others) and Bank of Greece Governor Yiannis Stournaras — took bribes.

Outcomes and retaliation:

- Greek investigating magistrates found insufficient evidence against the politicians; charges were dropped and several were cleared (four former Novartis executives and a politician cleared in 2023).
- The whistleblowers' protected status was lifted by the financial crimes prosecutor; a legislative amendment in force from 1 May 2025 allowed disclosure of their identities.
- In September 2025 an Athens court convicted both former protected witnesses of false accusation and repeated false testimony: Destempasides received 25 months and Marangeli 33 months, both sentences suspended for three years (GreekReporter and Balkan Insight, 15 September 2025).
- Chief anti-corruption prosecutor Eleni Touloupaki, who led the investigation, was removed from the case after the 2019 change of government, then prosecuted for abuse of power / dereliction of duty (and initially criminal-organisation charges); she was acquitted. Testifying before Deputy Supreme Court Prosecutor Evangelos Zacharis in June 2020, she said she was the victim of "a coordinated attempt at moral extermination," denying charges of abuse of power, dereliction of duty and making false statements.
- Journalists who reported on the case were also charged with criminal-organisation membership; those charges were later dropped.

The Novartis case shows the two-sided nature of the "whistleblower" question in Greece: while US law protected and vindicated the FCPA whistleblowers, the Greek protected witnesses were ultimately discredited and convicted, and the officials who investigated were themselves pursued — feeding a rule-of-law critique (voiced in the European Parliament and by OCCRP) that Greece went after the investigators, journalists and witnesses rather than the alleged corruption. The report should present both the FCPA settlement and the Greek convictions as facts, without asserting that the bribery allegations against Greek politicians were proven.

10. Guidance for organisations: What must an organisation do to ensure that its internal reporting channel works in practice?

We have already covered most of this chapter in Chapter 2. Let us look at a few further essential details that must not be overlooked. The Directive requires reporting channels to be accessible orally as well as in writing; this means that a meeting must be arranged within a reasonable timeframe.



This reflects precisely the point made earlier: an email address is not enough. A person who is afraid to put something in writing, does not want to leave a digital trail, or perhaps has no computer because of the physical nature of their work must be able to report orally, by telephone or at an in-person meeting.

Good practice: On its front page, a company should explain how to report any wrongdoing identified and present all three options on an equal footing.

10.1 Independence that must be tested, not merely stated

We have already established that the person handling reports must be impartial. The remaining question is: how does an organisation know that this independence holds up in practice? Anything can be written on paper; only when a report concerns someone influential does it become clear whether the system really works.

Good practice: An organisation should test at least once whether a report concerning senior management would in fact be routed around them, rather than waiting until this happens for the first time in a real case.

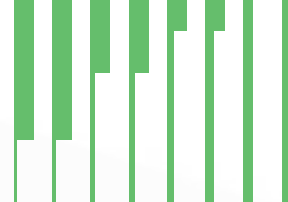
10.2 Documenting decisions

When, after a report has been made, an organisation takes a decision that places the reporting person in a different position — transferring them, changing their duties or excluding them from consideration for promotion — it may later be difficult to prove that the reason was unrelated to the report if nothing was recorded at the time of the decision.

Good practice: The organisation should set out in writing the reasons for every decision that could be perceived as connected with a report at the time the decision is taken, rather than only when it must be defended before a court.

10.3 Training and awareness

Even the best-designed channel has little value if employees do not know that it exists, do not know who receives reports, or do not trust that person.



An organisation therefore needs more than a policy and an email address. People need to know where they can report wrongdoing, how their identity will be protected, what will happen after they report, and that they may also approach the competent external authority. The people who receive and handle reports require specialised training. Managers must understand that retaliation is not limited to dismissal, but may also take far less obvious forms.

Good practice: An organisation should not inform employees about the channel only once, when it is established. Information and training should be refreshed periodically, particularly when new employees, managers or people responsible for handling reports join the organisation.

10.4 How does an organisation know whether its system really works?

An organisation's compliance with formal requirements says little about how the system operates in practice. It is therefore useful to review some basic data periodically: how many reports were received; whether receipt was acknowledged on time; how long they took to handle; how they were concluded; and whether any suspected retaliation arose. Care must be taken throughout to ensure that aggregated data do not reveal reporting persons' identities. If, for example, several reports in succession concern the same department, or many reports are closed without further action, this does not in itself prove that something is wrong with the system — but it may give the organisation a reason to examine what is happening.

Good practice: An organisation should also periodically examine something that statistics cannot reveal: whether employees know where they can report wrongdoing and whether they believe they will be safe if they do.

11. What must a competent authority do to ensure that external reporting works in practice?

As we have seen, Peter Verbič first chose to report internally. But what if he does not trust the internal channel? What if there is no such channel at all? The Directive then provides a second route: the reporting person may approach the competent external authority directly — in Slovenia, the Commission for the Prevention of Corruption (KPK). The organisation itself operates the internal channel, which is why the previous chapter discussed what the organisation must do. The external channel, by contrast, is operated by the State — more specifically, by the competent authority designated by the State. The questions here are much the same as for an internal channel: who receives the report, how the reporting person's identity is safeguarded, what happens after the report is submitted, and what happens if the authority does not act.

11.1 Who can report externally, and when?

A reporting person is never required to use the internal route first. They may decide, precisely because of a lack of trust, to go directly to the competent external authority, even where their organisation has an internal channel.

The Directive encourages internal reporting where the breach can be addressed effectively within the organisation and the reporting person does not expect retaliation, but this is not a condition for protection. The same applies to Peter Verbič: if he does not trust the internal channel because he suspects that it is connected with the people concerned by the report, the Directive does not require him nevertheless to wait for a response from that channel.

11.2 The channel must be accessible and confidential

As with the internal channel, the reporting person must be able to report in writing or orally and, upon request, at an in-person meeting within a reasonable timeframe. The confidentiality of their identity must be safeguarded in the same way as for internal reporting: only staff authorised to handle reports within the authority may access information identifying the reporting person.

Staff who handle reports within the competent authority must be trained and must have no conflict of interest in relation to the matter they are handling.

11.3 What happens after a report is submitted?

As with the internal channel, the seven-day rule applies: the competent authority must generally acknowledge receipt of the report within seven days. It must then diligently follow up on the report and provide feedback to the reporting person within three months on what is happening with it. In duly justified cases, this period may be extended to six months.

This is the same rule that applies to internal channels — and that is no coincidence. At this point, the Directive makes no distinction between a report handled by an organisation and one handled by the State. The same principle applies in both cases: the reporting person must not be left uncertain as to whether their report has even been received or whether anything is being done about it.

11.4 What if the authority remains silent or closes the report without explanation?

This is not merely a theoretical question. Silence on the part of the competent authority has consequences that extend beyond the report itself. If the reporting person receives no response from the authority within a reasonable period, this is one of the grounds on which the Directive may, exceptionally, permit a public disclosure — the route otherwise described as a last resort. In other words, if the external route does not work, the reporting person has little choice but to consider the next step.

Silence or an unexplained decision to close a report is therefore not merely a matter of good practice on the part of the authority — it affects which options remain available to the reporting person.

11.5 External transparency

A reporting person considering whether to approach the competent authority often asks a simple question: will this make any difference, or will my report simply disappear into a void? Trust in the external route is also built when the authority explains regularly and clearly what it does with reports, how many it receives, how many lead to follow-up action, and how long they take on average.

Example from national implementation

Bulgaria

In Bulgaria, external reports are received by the Commission on Personal Data Protection - the designated authority for handling these reports. According to the Bulgarian Act on the Protection of Persons who Report or Publicly Disclose Information on Breaches, whistleblowers may report first to an internal channel within their organisation, or directly to the external one (CPDP) in case there is a risk of retaliation, discriminatory actions. They may also report to the external channel if no effective measures will be taken to deal with the violation internally. After signalling institutions and the wider public via the Access to Public Information Act, Mrs. Stancheva turned to the CPDP and was granted protection status, along with her husband.

Greece

How the EAD handles reports in practice (Greece)

Under Article 11 of Law 4990/2022, the National Transparency Authority (EAD — Εθνική Αρχή Διαφάνειας) is the single designated external reporting channel in Greece. Reports are handled by a dedicated unit within the EAD's Inspections and Controls Division (Μονάδα Επιθεωρήσεων και Ελέγχων, Τομέας Διαχείρισης Καταγγελιών), whose staff receive specialised training in report handling.

How to submit a report

A report can be submitted through four channels:

- the EAD's dedicated secure online platform (aead.gr → "Υποβολή Καταγγελίας" → "Εξωτερική αναφορά")
- by sealed post to EAD headquarters (195 Lenorman & Amfiaraou St., 10442 Athens), marked "Εξωτερικός Δίαυλος Whistleblowing"
- by telephone (2132129900, Mon–Fri 09:00–14:00), including voicemail
- in person, by appointment on request

No supporting documents are required and the service is free of charge.

What happens after submission

- Within **7 working days**: the EAD acknowledges receipt (unless the reporter has requested no acknowledgment, or acknowledgment would jeopardise confidentiality of identity).
- The EAD then assesses whether the report falls within the scope of Law 4990/2022 (i.e. concerns a breach of EU law in one of the covered sectors). Reports that are incomprehensible, abusive, or manifestly outside scope are archived, with the reporter notified.
- Reports that fall outside the EAD's own competence are transferred to the relevant national or EU body, again with notification to the reporter.
- Within a maximum of **3 months** (6 months in duly justified cases): the reporter receives feedback on the measures taken or planned and the reasons for them.
- The EAD reviews the effectiveness of its procedures at least every three years (Article 11(4)).

Relationship with internal channels

A reporter may bypass the internal channel and go directly to the EAD where there is risk of retaliation, where the internal channel has failed to act, or where a competent authority is involved. Where a report is first submitted through an internal channel and not effectively addressed, the reporter may resubmit it directly to the EAD.

Slovenia

Role of the Commission for the Prevention of Corruption (KPK)

The KPK is one of the authorities designated to receive external reports under the ZZPri. It also acts as the fallback authority: if no external reporting authority is competent for the area of the reported breach, the whistleblower reports to the KPK.

Within the Commission, external reports are handled by designated officials of the Whistleblower Protection Centre. A report to the KPK can be submitted by email, by telephone, through an electronic form on the eGovernment portal (eUprava), or in person by prior arrangement.

The external reporting authority must protect the identity of the whistleblower. Information identifying the whistleblower is protected, and documents relating to the report are subject to special confidentiality rules. Unlawful attempts to identify or disclose the identity of a whistleblower, facilitator or connected person may constitute a minor offence (prekršek) under the ZZPri.

The KPK also has a central role in monitoring how the Slovenian whistleblower protection system works. Organisations operating internal reporting channels and authorities receiving external reports must submit annual statistical data to the KPK by 1 March for the previous year. Reporting is mandatory even if no reports were received. For external reports, the data include the number of reports received, anonymous reports and substantiated reports, breaches handled, measures taken, retaliation cases handled and, where established, financial damage and recovered amounts.

12. How do we know whether the system works at all?

In the previous chapter, we noted that an organisation can itself check whether its internal channel is actually working by examining how many reports it receives, how quickly it responds, and whether employees even know that the channel exists. The same question should also be asked more broadly: how do we know whether the protection of reporting persons in a particular country, or across the European Union, actually works rather than existing only on paper?

12.1 What Member States must report to the European Commission

Member States must report regularly to the European Commission on how they are implementing the Directive. On the basis of these reports, the Commission prepared the first comprehensive report on implementation of the Directive across the Union in 2024; that report has already been mentioned in this handbook. Reports of this kind show whether Member States met the deadline for transposing the Directive, how closely national rules follow its minimum standards, and where gaps remain.

For an individual reporting person, this may seem remote from their everyday experience. Yet these reports show whether the protection promised by law is genuinely accessible — or remains merely a fine promise on paper.

12.2 Which indicators show whether protection actually works?

Some indicators are the same as those proposed to organisations in the previous chapter, except that this time they are considered at national level: how many reports the competent authorities receive each year; how many were acknowledged within the prescribed period; how many lead to follow-up action; and how many cases of retaliation were reported and how they ended.

None of these data tells the whole story in isolation. A low number of reports may mean that there is simply no wrongdoing, but it may also mean that people do not trust the system enough to speak up. It therefore makes sense to read these data together rather than individually.

12.3 The role of projects such as RIGHTS WHISPER

This is where the project under which this handbook is being produced also comes into play. Across three countries — Slovenia, Bulgaria and Greece — RIGHTS WHISPER not only explains what the Directive requires, but also monitors how it is implemented in practice: where national laws follow the Directive's minimum standards, where gaps remain, and how courts perform when adjudicating cases involving retaliation. This work is being carried out primarily under Tasks T2.2 (national implementation of reporting channels) and T2.4 (cases of retaliation and case-law), whose findings will supplement this handbook.

13. All in one place: Charter article, Directive provision and practical focus

If it seems that this handbook has repeatedly interwoven the Charter and the Directive, you are quite right — that was the intention. The table below summarises where each Charter article intersects with a provision of the Directive and what deserves particular attention in practice.

Charter article	What the Directive provides	Key point to remember
Article 11 — Freedom of expression and information	Internal and external reporting; public disclosure subject to conditions; protection regardless of the outcome of the investigation.	The reporting person does not have to prove the breach; it is sufficient that they had reasonable grounds to believe that the information was true at the time of reporting.
Article 31 — Fair and just working conditions	Prohibition of retaliation, including covert forms; reversal of the burden of proof.	Retaliation is not limited to dismissal; it also includes less obvious forms of pressure.



Charter article	What the Directive provides	Key point to remember
Article 41 — Good administration	Deadlines for acknowledgement of receipt (7 days) and feedback (3 months); impartial handling.	The reporting person must know that the report has been received and what is happening with it.
Article 47 — Effective remedy	Access to legal and psychological counselling; the possibility of interim relief during proceedings.	Protection is not merely a prohibition on paper, but also a route to the effective enforcement of rights.

14. Frequently asked questions

To conclude, we have collected some of the questions most frequently asked by workers and persons designated to handle reports. The answers are brief; for a more detailed explanation, see the relevant chapter.

Do I have to be certain that my information is correct?

- No. It is enough that, at the time of reporting, you had reasonable grounds to believe that the information was true. If it later emerges that you made an honest mistake, you do not lose protection as a result.

Do I have to report within the organisation first?

- Not necessarily. The Directive encourages internal reporting where you believe that the organisation can address the problem effectively and that you are not at risk of retaliation. You may, however, also report directly to the competent external authority.

What if my report proves to be unfounded?

- If you acted in good faith and had reasonable grounds to believe that the information was true, you remain protected even if the investigation concludes without finding a breach. The situation is different if you knowingly reported something you knew to be untrue; the Directive provides for penalties in such cases.

Can I report anonymously?

- The Directive does not require organisations to accept anonymous reports, although many nevertheless offer this option. If you reported anonymously and your identity subsequently became known, you enjoy the same protection as if you had reported openly.

What counts as retaliation?

- Far more than simply losing your job. It also includes demotion, removal of duties, an adverse performance assessment, exclusion from meetings or denial of access to information, an unjustified change in working hours, and similar measures. If something of this kind happens shortly after you report and there is no understandable, unrelated reason for it, it may constitute retaliation.

Who must prove that the detrimental measure was not taken because of my report?

- Once you establish that you made a report and subsequently suffered a detriment, the detriment is presumed to have occurred in retaliation for the report. The other party must prove that its decision was based on other, duly justified grounds. You therefore do not have to prove the causal link; that burden rests with the other party.

Where can I get help if I am considering making a report?

- You can contact the person designated to handle reports within your organisation, the Commission for the Prevention of Corruption, a trade union, or a civil society organisation that provides legal assistance to reporting persons. You do not have to go through this alone.

Annex A — Checklist for organisations

This checklist summarises Chapter 10 in a form that allows an organisation to carry out a quick point-by-point check without rereading the entire text.

Channel design and accessibility

- The internal channel is accessible to employees and to other people connected with the organisation (volunteers, trainees, contractors and subcontractors).
- The organisation has considered whether it will also allow anonymous reporting.
- An alternative route has been determined in advance for every situation in which the person designated to handle reports might have a conflict of interest (for example, where a report concerns senior management).

Confidentiality

- Only authorised persons have access to information about the reporting person's identity.
- Employees who handle reports have been instructed not to discuss them with anyone who is not authorised to receive that information.
- Any exception involving disclosure of the reporting person's identity (for example, in court proceedings) is preceded by notice to the reporting person.

Handling a report

- As a matter of standard practice, and not merely by way of exception, an acknowledgement of receipt is sent within seven days.
- Feedback is provided to the reporting person no later than three months.
- The assessment of whether a reporting person remains protected is based on whether they had reasonable grounds to believe that the information was true, not on whether the report ultimately proved to be correct.



Preventing retaliation

- In addition to formal personnel decisions, less obvious signs of retaliation are monitored, including exclusion, removal of duties and changes in working hours.
- Every decision affecting a known reporting person is documented, at the time it is taken, with a clear reason unrelated to the report.

Awareness and training

- Employees know that the channel exists, who operates it, and that it is independent of their immediate manager.
- Staff who handle reports have received specialised training, which is refreshed periodically.
- Once a year, the organisation reviews basic data on reports (number, timeliness and outcome) without disclosing reporting persons' identities.

Annex B — A short guide for workers

This guide is intended specifically for you if you are considering reporting wrongdoing and would like to know what to do first.

Thinking of reporting wrongdoing? Here are five rules.

1. What do I want to report? Make a note of what you saw or learned and when it happened.
2. Do I have reasonable grounds to believe that the information is true? To qualify for protection, you do not have to prove the breach conclusively yourself.
3. Which channel can I use? Check whether your organisation has an internal channel and who operates it. You may also report directly to the competent external authority.
4. Is there a risk of retaliation? If so, consider whether the external route would be safer.
5. Where can I get help? Before taking the next step, consult someone independent: a trade union representative, a legal adviser or a civil society organisation. You can also call Transparency International in your country.

What is protected?

You are protected if, at the time of reporting, you had reasonable grounds to believe that the information was true, even if it later emerges that you made an honest mistake. You may report within the organisation or to the competent external authority and, under certain conditions, you may also make a public disclosure. Your identity must remain confidential and may be known only to authorised staff who handle the report.

What counts as retaliation?

Not only dismissal. It also includes demotion, an adverse performance assessment, exclusion from meetings, an unjustified change in working hours, harassment or damage to your reputation. If something of this kind happens after you report and there is no clear, unrelated reason for it, it may constitute retaliation.

Why does the burden of proof work in your favour?

If you establish that you made a report and subsequently suffered a detriment, the other party must prove that its decision was based on other, duly justified grounds. You do not have to prove the connection between the two events yourself.

Where can you get help?

Contact the person designated to handle reports within your organisation, the Commission for the Prevention of Corruption, Transparency International, a trade union, or a civil society organisation that provides legal assistance to reporting persons. You do not have to — and should not have to — deal with this alone.

Annex C — Glossary and further resources

Glossary

- Reporting person — a person who reports or publicly discloses information on a breach acquired in a work-related context.
- Internal reporting — reporting through a channel operated by the reporting person's own organisation.
- External reporting — reporting to a competent public authority designated by national law.
- Public disclosure — making information about a breach available in the public domain, most commonly through the media; protected only under specific conditions.
- Retaliation — any act or omission prompted by a report that causes or may cause detriment to the reporting person.
- Competent authority — a national authority designated to receive and handle external reports (in Slovenia, this includes the Commission for the Prevention of Corruption).

Further resources

- European Commission — overview of Directive (EU) 2019/1937 and its implementation in the Member States.
- EUR-Lex — full text of Directive (EU) 2019/1937 and the Charter of Fundamental Rights of the European Union.
- Eurobarometer (2025) — survey of EU citizens' perceptions of corruption.
- Commission for the Prevention of Corruption (KPK) — information on external reporting in Slovenia.
- RIGHTS WHISPER project results: D2.2 (national implementation of reporting channels), D2.4 (cases of retaliation and case-law), and D2.5 (consolidated transnational comparative report).
- Transparency International

Annex D — Model wording

Organisations may adapt the following short texts for their policies and correspondence. They are intended solely as a starting point and must be aligned with national law before use.

Model acknowledgement of receipt of a report

- **Model wording**

Thank you for your report, received on [date]. We hereby acknowledge its receipt within seven days, as required by law. Your report will be handled confidentially. You will receive feedback no later than three months.

Model clause on the standard of protection

- **Model wording**

Protection under this policy does not depend on whether the report subsequently proves to be correct. A worker who, at the time of reporting, had reasonable grounds to believe that the information was true remains protected even if the investigation does not substantiate the breach, unless the report was knowingly false.

Model non-retaliation clause

- **Model wording**

No worker who makes a report in accordance with this policy will be dismissed, demoted or otherwise placed at a disadvantage as a result. Every decision affecting a worker who is known to have made a report must be documented with reasons unrelated to the report.



SOURCES AND FURTHER READING

European Union – Legal Framework

- European Union, **Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law:**
<https://eur-lex.europa.eu/eli/dir/2019/1937/oj>
- European Union, **Charter of Fundamental Rights of the European Union:**
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>
- European Commission, **Protection for whistleblowers:**
https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/protection-whistleblowers_en
- European Commission, **Report on the implementation and application of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law:**
https://commission.europa.eu/document/download/e43222b1-68be-4a0e-9d2f-45e0d7428a4a_en
- **Official Explanations relating to the Charter of Fundamental Rights** (2007/C 303/02) — the authoritative interpretive document [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007X1214\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007X1214(01))
- **FRA Charterpedia** <https://fra.europa.eu/en/eu-charter>
- **European Ombudsman — right to good administration (Article 41)**, European Code of Good Administrative Behaviour:
<https://www.ombudsman.europa.eu/en/home>
- **Council of Europe, Recommendation CM/Rec(2014)7** <https://rm.coe.int/16807096c7>

Case Law Databases

- **InfoCuria / Curia :**
<https://curia.europa.eu/juris/recherche.jsf?language=en>
- **HUDOC** <https://hudoc.echr.coe.int/eng>
- **ECTHR Guide on Article 10 of the Convention** https://ks.echr.coe.int/documents/d/echr-ks/guide_art_10_eng

EU Agencies

- **EU-OSHA** (European Agency for Safety and Health at Work) <https://osha.europa.eu/en>

SLOVENIA

Whistleblower Protection Act and Reporting System

- Republic of Slovenia, **Zakon o zaščiti prijaviteljev – ZZPri (Whistleblower Protection Act), Official Gazette of the Republic of Slovenia, No. 16/2023:**
<https://pisrs.si/pregledPredpisa?id=ZAKO8518>
- Ministry of Justice of the Republic of Slovenia, **Zaščita prijaviteljev – žvižgačev / Protection of Whistleblowers:**
<https://www.gov.si teme/zascita-prijaviteljev/>
- eUprava, **Prijava zaščenega prijavitelja glede kršitve predpisov v delovnem okolju / External reporting under the Whistleblower Protection Act:**
https://e-uprava.gov.si/si/podrocja/drzava-druzba/inspekcijski-postopki/zascita-prijaviteljev?lang=si&view_mode=0



- Labour Inspectorate of the Republic of Slovenia, **Zunanja prijava po Zakonu o zaščiti prijaviteljev / External reporting under the Whistleblower Protection Act:**
- <https://www.gov.si/novice/2023-05-22-zunanja-prijava-po-zakonu-o-zasciti-prijaviteljev/>
- Commission for the Prevention of Corruption (KPK), **Protection of Whistleblowers – detailed information:**
- <https://www.kpk-rs.si/sl/aktivnosti-komisije/zascita-prijaviteljev/podrobnosti-o-zasciti-prijaviteljev>
- Commission for the Prevention of Corruption (KPK), **Reporting persons / whistleblowers:**
- <https://www.kpk-rs.si/sl/prijavitelji-krsitev>
- KPK – External reporting under the ZZPri; <https://www.kpk-rs.si/sl/aktivnosti-komisije/zascita-prijaviteljev/zunanja-prijava>
- Transparency Slovenija: Whistleblower: <https://www.transparency.si/oznaka/zascita-zvizgacev/stran/2/>

Peter Verbič / DARS Case

Preiskovalno.si, “V Darsu sem opozarjal na korupcijo in dobil odpoved” – investigation concerning former DARS employee Peter Verbič and his allegations concerning procurement procedures and his subsequent dismissal: <https://preiskovalno.si/clanek/v-darsu-sem-opozarjal-na-korupcijo-in-dobil-odpoved/>

IVAN GALE / Slovenian Face-Mask Procurement Case

- Preiskovalno.si, “Ekskluzivno! Žvižgač Gale po petih letih dokazal ponaredek”, 5 March 2026:
- <https://preiskovalno.si/clanek/ekskluzivno-zvizgac-gale-po-petih-letih-dokazal-ponaredek/>
- Commission for the Prevention of Corruption (KPK), investigations concerning the procurement of protective equipment during the COVID-19 epidemic. Following its thematic review, the Commission initiated 21 investigations concerning suspected integrity violations involving eight public officials.
- Delo, “Žvižgač se je poravnal z nekdanjim delodajalcem” – report on the settlement between Ivan Gale and the Institute of the Republic of Slovenia for Commodity Reserves following the termination of his employment:
- <https://www.delo.si/novice/slovenija/ivan-gale-z-zavodom-za-blagovne-rezerve-sklenil-poravnavo>
- 24UR/STA, “Počivalšek in Rumpf napovedala sodelovanje s KPK: Nabava je potekala v ‘norih okoliščinah’”, 15 December 2020 – report on the 21 investigations opened by KPK following its review of protective-equipment procurement:
- <https://www.24ur.com/novice/slovenija/pod-drobnogledom-tudi-pocivalsek-in-gale-kpk-zaradi-nabave-zascitne-opreme-izvaja-21-preiskav.html>
- Commission for the Prevention of Corruption (KPK), subsequent decisions concerning investigations into COVID-19 protective-equipment procurement:
- <https://www.kpk-rs.si/>

BULGARIA

Sources:

- Commission for Personal Data Protection, Methodological Guidelines № 1 on receiving, registering and handling reports received at the obliged subjects under the Act on Protection of Persons, Reporting Information,



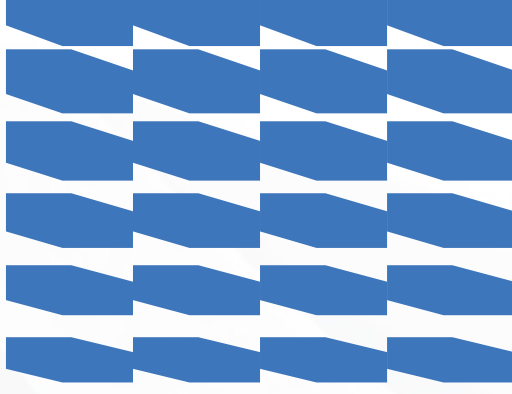
- **Ombudsman of the Republic of Bulgaria, Aud Reports:** <https://www.ombudsman.bg/?go=page&pagelid=596>
- **Act on the protection of persons who report or make public information on breaches:** <https://lex.bg/en/laws/ldoc/2137231156>
- **Court Ruling #6906:** <https://dela.bg/Acts/42f346b0-0532-403c-acfd-5cb75d80e2c1>
- **Btv news, The inspector who reported the toxic substances at “Himko” may be fired again:** <https://btvnovinite.bg/bulgaria/inspektorat-signaliziral-za-otrovite-v-himko-mozhe-otnovoda-bade-uvolnen.html>
- **Southeast Europe Coalition on Whistleblower Protection, The Bulgarian Nurse who Filled 300+ Freedom of Information Act Requests and Alerts** <https://see-whistleblowing.org/the-bulgarian-nurse-who-filled-300-freedom-of-information-act-requests-and-alerts/>
- **Access to Information Programme, Interview with Nataliya Stancheva:** https://www.aipbg.org/publications/%D0%91%D1%8E%D0%BB%D0%B5%D1%82%D0%B8%D0%BD/%D0%9D%D0%B0%D1%82%D0%B0%D0%BB%D0%B8%D1%8F_%D0%A1%D1%82%D0%B0%D0%BD%D1%87%D0%B5%D0%B2%D0%B0_%D0%9A%D0%BE%D0%B9%D1%82%D0%BE_%D1%82%D1%8A%D1%80%D1%81%D0%B8_%D0%BD%D0%B0%D0%BC%D0%B8%D1%80%D0%B0/102104/1000082701/
- **DW, Nataliya Stancheva and the Kozloduy Nuclear Power Plant: Standing Up to the Powerful:** <https://www.dw.com/bg/natalia-stanceva-i-aec-kozloduj-da-zastanes-sresu-silnia/a-68640109>
- **AEJ Bulgaria, a SLAPP case ended with 15,000 BGN of debt for an active citizen. AEJ launches a fundraising campaign:** <https://aejbulgaria.org/%D0%B4%D0%B5%D0%BB%D0%BE%D1%88%D0%B0%D0%BC%D0%B0%D1%80%D0%BF%D1%80%D0%B8%D0%BA%D0%BB%D1%8E%D1%87%D0%B8-%D1%81-15-000-%D0%BB%D0%B2%D0%B4%D1%8A%D0%BB%D0%B3-%D0%B7%D0%B0-%D0%B0%D0%BA%D1%82%D0%B8%D0%B2/>
- **Mediapool.bg, a SLAPP case ended with 15,000 BGN of debt for the nurse sued by the Kozloduy Nuclear Power Plant:** <https://www.mediapool.bg/delo-shamar-priklyuchi-s-15-000-lv-dalg-za-medsestrata-sadena-ot-aets-kozlodui-news365862.html>
- **Ombudsman of the Republic of Bulgaria, Aud Reports:** <https://www.ombudsman.bg/?go=page&pagelid=596>
- **Act on the protection of persons who report or make public information on breaches:** <https://lex.bg/en/laws/ldoc/2137231156>

GREECE

- Linos, A., Petralias, A., Christophi, C. A., Christoforidou, E., Kouroutou, P., Stolidis, M., Veloudaki, A., Tzala, E., Makris, K. C., & Karagas, M. R. (2011). Oral ingestion of hexavalent chromium through drinking water and cancer mortality in an industrial area of Greece: An ecological study. *Environmental Health*, 10(1), Article 50.
- EU Parliament question on Oinofyta chromium (2013): https://www.europarl.europa.eu/doceo/document/E-7-2013-014158_EL.html
- 2008 Oinofyta municipal conviction (Ta Nea): <https://www.tanea.gr/2008/07/16/greece/katadiki-toy-dimoy-oinofytw-n-gia-to-xrwmio-sto-nero/>
- Linou cancer findings (Ta Nea): <https://www.tanea.gr/2010/08/27/health/pethainontas-sta-oinofyta-2/>



- Inspectors' 150+ inspections / fines: <https://oinofyta.wordpress.com/>
- PFAS study withheld (Reporters United / Substack): <https://bersi.substack.com/p/pfas>
- PAKOE 2024 monitoring: <https://www.pakoe.gr/2024/02/26/>
- OCCRP (anonymity lifted): <https://www.occrp.org/en/news/greece-drops-anonymity-for-novartis-case-whistleblowers>
- OCCRP (Touloupaki acquitted): <https://www.occrp.org/en/news/greek-court-acquits-anti-corruption-prosecutor-eleni-touloupaki>
- Balkan Insight (2025 conviction): <https://balkaninsight.com/2025/09/15/greek-court-convicts-former-novartis-whistleblowers/>
- Neos Kosmos (conviction, Jan 2026 report):
<https://neoskosmos.com/en/2026/01/14/news/greece/two-ex-protected-witnesses-in-novartis-bribe-scandal-convicted-in-greece/>
- KKC case page: <https://kkc.com/whistleblower-case-archive/novartis-greece-bribery/>
- Financial Regulation International analysis:
<https://www.financialregulationintl.com/regulation/the-greek-novartis-scandal--whistleblowers-legal-retaliation-and-the-erosion-of-the-rule-of-law-159535.htm>
- EU Parliament question on prosecution of prosecutor/journalists:
https://www.europarl.europa.eu/doceo/document/E-9-2022-000694_EN.html
-
- Law 4990/2022, Articles 11–12: <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4990-2022/arthro-11-nomos-4990-2022-ethniki-arhi-diafaneias-os>
- EAD submission platform: <https://aead.gr/submit-complaint>
- MITOS (official administrative procedure register): <https://mitos.gov.gr> (search "Εξωτερική αναφορά Whistleblowing")



Thank you!

Thank you for taking the time to read this report. If you have any questions or would like to discuss our findings further, please don't hesitate to reach out to us.

Strengthening integrity and safeguarding human rights through robust whistleblower protection in Europe



RIGHTS WHISPER

www.rights-whisper.eu

RIGHTS WHISPER

D2.1: GUIDANCE DOCUMENT: LINKING DIRECTIVE 2019/1937 WITH CHARTER RIGHTS

CERV-2025-CHAR-LITI

Project number: 101293231



TRANSPARENCY
INTERNATIONAL
SLOVENIA



TRANSPARENCY
INTERNATIONAL
BULGARIA



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.