
COMMENTS ON 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

JORGETE VITORINO CLARINDO DOS SANTOS, TANIA NEMER***

KEYWORDS

Compliance, Whistleblowing Channel, Protection, Whistleblower, Directive European Union, U.S. DOJ

ABSTRACT

Without some of the important information brought into light by whistleblowers, many current scandals would not have occurred. It is undeniable that whistleblowing brought into the public domain can insert a previously unforeseen and incorrigible milestone in the biography of whistleblowers, which can lead to financial loss, loss of work, affect private life, and even health. Even in situations where the whistleblower acts in good faith, he runs the risk of being publicly judged and having his reputation tarnished by lack of protection. Reporting persons may even be driven to complete isolation or pay with their lives or that of their families. In view of this, the European Union has foreseen in a new directive a better protection for whistleblowers, through the implementation of a trilateral whistleblower system.

The main new feature of the European Whistleblower Protection Directive is the obligation to establish internal whistleblower channels for legal entities in the public and private sectors with at least 50 or more employees. In the public sector, Member States may exempt cities with fewer than 10,000 inhabitants or fewer than

* Director Compliance Officer at Infineon Technologies AG in Munich, Germany, E-mail: internationalcompliance@gmail.com

** Community Outreach Prosecutor at the Summit County Prosecutor's Office in Ohio, U.S.A. The authors thank Steve Herbes for his valuable comments and proofreading. This work reflects only the personal opinion of the authors and not necessarily of the company or institution for which they work.

50 employees working in the public body from the obligation to establish whistleblowing channels. If the report to the company or public body is not successful, the whistleblower may report to the press.

European legislators have until December 2021 to transpose the provisions of this directive into national whistleblower protection regulations.

I. INTRODUCTION

The 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 (the “Directive”)¹ was published on November 26, 2019 and went into effect in December of the same year.² European legislators have two years³ at the national level to incorporate the provisions of this Directive into national whistleblower protection regulations.⁴

The inclusion of whistleblower reporting channels in compliance programmes is not new and has long been considered an essential element in the structural framework of an effective compliance programme.⁵

Work with whistleblowers in multinational companies is multifaceted and unique, either by virtue of the subject matter itself (i.e., the allegations and the analysis and investigation by the local compliance officer), or the diverse cultures to which whistleblowers belong, or the number and quality of functions of the people involved in the report (which often requires time in preparing and conducting interviews), or the impact caused, or that may be caused, by the complaint submitted by the whistleblower in relation to the company.

With regard to the identification of risks, whistleblowing reporting channels are a means of helping to identify corporate wrongdoing.⁶ Thus, it is recommended that all companies, even those governed by a corporate legal form that dispenses

¹ Union Law is understood as European Union law.

² The Directive went into effect on December 16, 2019.

³ By December 17, 2021, all European Union countries must have incorporated the provisions of the Directive into their national legal systems.

⁴ Resolution 2399, 2019, Improving the Protection of Whistleblowers All Over Europe: All EU member countries will be legally required to incorporate this Directive into their national law within two years from its effective date. However, the member states of the Council of Europe that are not, or not yet, members of the EU also have a strong interest in drawing on the draft Directive with a view to adopting or updating legislation in accordance with the new European standards.

⁵ Vitorino Clarindo dos Santos, Jorgete. *Rechtsfragen der Compliance in der internationalen Unternehmensgruppe*, 2013, P. 58.

⁶ Kremer/ Klarhold, ZGR 2010, P. 113, 132.

with the establishment of a compliance system and independent of the new Directive, establish whistleblower reporting channels, whether they are overseen by human resources, the legal department, the audit division, or a supervisory board, or placed under the direction of the works council, an ombudsman, or the compliance department itself.⁷

Whistleblowing reporting channels may allow the employee to raise a concern by telephone, e-mail, online (i.e., through the whistleblowing reporting channel established on the company's internet and/or intranet), or written mail, or the employee may be allowed to raise a concern directly with his or her superior, the compliance officer of the subsidiary in question, the chief compliance officer, or an ombudsman (if one exists), or the employee may contact the employee responsible for receiving the whistleblowing report in a department different from his or her own.

The explanatory memorandum to the proposed Directive lists several positive economic effects of the inclusion of whistleblower protection rules. Studies carried out by the European Commission in 2017 found that, in the field of public procurement alone, the annual loss of potential benefits for the proper functioning of the single market would be in the range of 5.8 to 9.6 billion euros.⁸ Moreover, just with regard to the impact on the EU budget allocated to preventing fraud and corruption, the current risk of lost revenue is estimated to be between 179 and 256 billion euros per year.⁹ Whistleblower protection should also contribute to more effective taxation in the EU by combatting tax avoidance. The latter results in tax revenue losses for Member States and the Union of around 50 to 70 billion euros per annum.¹⁰ As provided for in the Directive, protection for whistleblowers is instrumental in preventing the diversion of firearms, their parts, components and ammunition, as well as defence-related products, since it will encourage the reporting of violations of Union law, such as document fraud, altered marking and fraudulent acquisition of firearms within the Union, where breaches often imply a diversion from the legal to the illegal market.¹¹ Also, with regard to product manufacturing companies, the European Union estimates that

⁷ In some countries and cultures, whistleblowing reporting channels can also be viewed suspiciously, since the nature of the whistleblowing disclosure by one co-worker to another takes away the trust that must exist for their usefulness in discovering and subsequently handling corporate wrongdoing effectively. In this regard: Deiseroth/ Derleder, *Whistleblower und Denunziatoren*, ZRP 2008, P. 248; Mahnhold, "Global Whistle" oder «deutsche Pfeife» - Whistleblower-Systeme im Jurisdiktionskonflikt, NZA 2008, P. 737 et seq.

⁸ Milieu, *Estimating the economic benefits of whistleblower protection in public procurement*, 2017.

⁹ Directive, P. 8.

¹⁰ Directive, P. 8.

¹¹ *Exposition of reasons to the European Directive on the protection of whistleblowers*, 2019, P. 18.

they are the main source of uncovering unfair or illegal activities, with the result that whistleblowers' reports from these companies have a high added value, given their function in identifying possible unfair or illegal practices in the manufacturing, importing or distribution of products.¹²

Regarding the budgetary impact of the implementation of the whistleblower system in the public sector, the European Union foresees costs of more than 204.9 million euros in one-time costs and 319.9 million euros in annual operating costs.¹³ For medium and large companies in the private sector, costs are expected to be over 542.9 million euros in one-time costs and annual operating costs around 1,016.6 million euros.¹⁴

To ensure that the positive effects of implementing an European whistleblowing system are realised, the European Union has defined a set of common minimum legal standards that provide protection against acts of retaliation against whistleblowers, without the latter having to bear any disadvantages, whether personal or economic.¹⁵ It is undeniable that public disclosure of an anonymous whistleblower's identity can have a previously unforeseen and often irreversible effect on the reputation of the whistleblower. Not only Edward Snowden¹⁶, but also Margrit Herbst¹⁷, Chelsea Manning¹⁸,

¹² Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 18.

¹³ Directive, P. 8.

¹⁴ Directive, P. 8.

¹⁵ Cf. Council of Europe Recommendation CM/Rec (2014) of April 30, 2014, on the protection of whistleblowers; Council of Europe Parliamentary Assembly Resolution 2171 (2017) of June 27, 2017.

¹⁶ Edward Snowden is currently the world's best-known American whistleblower: While employed by an outside consulting firm in the service of the NSA intelligence agency, he uncovered and made public U.S. government surveillance via the internet. In 2020, a U.S. Federal Court ruled that the U.S. intelligence phone surveillance programme Snowden denounced was illegal. See link.

¹⁷ Margrit Herbst is a German veterinarian, who in 2001 received the whistleblower award from the association of German scientists, after having discovered and denounced the beginning of the BSE scandal (bovine spongiform encephalopathy, known as mad cow disease) in Germany during the 1990s. Margrit identified several suspected cases in 1994. However, her superiors not only ignored her, they released the infected animals for slaughter and their infected meat entered the market. When the number of cattle with suspected cases of the disease increased and the company continued to ignore the facts, the doctor gave a television interview in which she made the BSE cases public. See link.

¹⁸ Chelsea Manning released war reports, classified military documents, and diplomatic dispatches from Afghanistan and Iraq to the WikiLeaks platform in 2013, making public the war crimes committed by the U.S. military. Found guilty of espionage, she spent seven years in prison, before then-President Barack Obama commuted much of her sentence. See link.

Daniel Ellsberg¹⁹, and Miroslav Strecker²⁰, among many others, are examples of the media exposure and public notoriety that often follows when the whistleblower's identity is revealed to the public. Public reactions can have a great impact on whistleblowers, including financial and job losses, and can affect the whistleblower's private life and even health. Even in situations where the whistleblower acts in good faith, he or she runs the risk of being publicly judged and having his or her reputation tarnished by lack of legal protection. He or she may even be driven to complete isolation, have his or her life ruined, and pay with his or her own life or that of his or her family. In view of this, the European Union has attempted in the new Directive to establish better protections for whistleblowers through the implementation of a trilateral whistleblower system.

This work analyses the major changes affecting whistleblowers in international companies, including the personal and legal scope of the new European Directive, the obligation to establish internal and external whistleblower reporting channels, and its equal use, confidentiality, and specific whistleblower protection measures. Further, the procedure for receiving and handling internal whistleblower complaints is also part of this paper. Additionally, a chapter is dedicated to the position of the U.S. Department of Justice (DOJ) in evaluating the effectiveness of compliance programmes, though a comparison of both European and American legal frames is not in scope. An outlook and last considerations finalise the article.

International and doctrinal (black-letter law) as well as legal interdisciplinary research in the field were the major types of legal research used in this work.

II. CONTENT OF THE DIRECTIVE

The main objective of the Directive is to protect whistleblowers who report violations in good faith. To achieve this objective, the Directive provides for the following safeguards: (i) ensuring the protection of the identity of the whistleblower; (ii) if the identity of the whistleblower is known, the Directive provides measures to protect the whistleblower in such a way that he or she

¹⁹ Daniel Ellsberg made public in 1971 the so-called Pentagon Papers, which revealed numerous untruths that the American public had heard about the Vietnam War and the war aims of various U.S. governments. Ellsberg, economist and peace activist, is now 90 years old. See movie.

²⁰ Miroslav Strecker revealed in 2007 that certain beef of lower standard than was allowed for consumption had been relabeled and declared as food. During the scandal it was discovered that the company, which was later closed down, had sold 105 whole tons of waste meat to Döner (meat kebab) manufacturers in Berlin. See link.

should not fear reprisals in his or her professional environment; and (iii) the Directive protects the whistleblower from liability or punishment.²¹

2.1. Personal Scope

The European legislature has demonstrated its commitment to ensuring the broadest possible protection for whistleblowers.

According to the European standard, almost any type of natural person can fall under the legal definition of Article 5 (7), provided they satisfy the prerequisite of an employment relationship with a company or the state.²² The effective application of Union law requires that protection be granted to the broadest possible range of categories of persons, regardless of whether they are citizens of the Union or third-country nationals, who by virtue of their professional activities, regardless of the nature of such activities and whether they are remunerated or not, have privileged access to information on violations, whose reporting is in the public interest and who may suffer acts of retaliation, if they report them.²³

As far as personal treatment is concerned, in accordance with Article 4 (2) of the Directive, the Directive also protects whistleblowers who, in the public or private sector, report or divulge information about breaches they have become aware of during the course of a working relationship that has since ended. The Directive also applies to those whistleblowers whose employment relationship has not yet begun, in cases where information about violations has been obtained during the recruitment process or other stages of pre-contractual negotiations.

Personal scope is not limited to active employees, according to Article 45 of the Treaty of the Functioning of the European Union (TFEU), but also encompasses atypical working conditions such as that of temporary workers, self-employed persons, holders of shareholdings, persons belonging to the administrative, management or supervisory bodies of undertakings, including non-executive members, as well as volunteers, applicants for vacancies, trainees whether paid or unpaid, any persons working under the supervision and direction of contractors, subcontractors and suppliers. Also included in this list are facilitators (natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential), third parties who are connected to whistleblowers and who could be subject to retaliation in a

²¹ Garden/ Hiéramente, BB 2019, P. 963 - 965.

²² European Directive on the protection of whistleblowers, art. 5. Definitions, 7) “Whistleblower” means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities.

²³ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 23 (37).

professional context, such as colleagues or family members of whistleblowers, as well as legal entities that are owned by whistleblowers, for whom the latter work or with whom they are connected in any way in a professional context. In situations where married persons work for the same employer and confirm that one of them is a whistleblower, the other person also enjoys legal protection if the whistleblower is fired or otherwise harmed by the employer.²⁴ Thus, the Explanatory Memorandum of EU Directive No. 81 makes it clear that persons who directly make a public disclosure should also benefit from protection if they have reasonable grounds for believing that, in the case of external whistleblowing, there is a risk of retaliation, or a prospect that evidence may be concealed or destroyed, or that an authority may be in collusion with the offender of the breach or involved in the violation itself.

The Directive also provides protection in Article 4 (4) (a) to the facilitator, who is defined as a natural person who assists a whistleblower in the complaint procedure in a professional context, and whose assistance must be confidential. The European norm also provides protection in Article 4 (4) (c) to legal entities that are owned by whistleblowers, for which they work or with which they are in any way connected in a professional context.

2.2. Legal Scope of Application

With regard to legal application, the Directive lists in an enumerative manner the legal areas in which the protection of whistleblowers is guaranteed, thus not fully harmonising the protection of whistleblowers.²⁵ The legal application of the Directive covers infringements within the scope of the EU acts listed in Article 2 (1) (a), which concern the following areas: public procurement, services, financial products and markets and prevention of money laundering and terrorist financing, product safety and compliance, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, protection of privacy and personal data, and network and information systems security. In addition, paragraph (b) provides protection in the case of offenses resulting from violations against the financial interests of the European Union, as referred to in Article 325 TFEU and specified in applicable Union measures. In addition, also listed under (c) are violations relating to the internal market, referred to in Article 26 (2) TFEU, including violations of Union competition and state aid rules, as well as violations relating to the internal market with respect to acts in violation of corporate tax

²⁴ European Directive on the protection of whistleblowers, art. 4.

²⁵ Dzida/ Granetzny, Die neue EU-Whistleblowing-Richtlinie und ihre Auswirkungen auf Unternehmen, 2020, P. 2.

rules or practices whose purpose is to obtain tax advantages contrary to the object or purpose of corporate tax law.

There is no whistleblower protection for complaints made about ethical issues or general breaches of contracts, nor about internal corporate guidelines, unless the breaches also constitute violations of laws listed in the Directive.²⁶

EU member states are permitted to extend protection under national law to areas or acts not covered by Article 2 of the Directive. This can be done by creating a national whistleblower protection law, which can also apply to internal reporting of violations.

III. REPORTING WHISTLEBLOWER CHANNELS AND THEIR OPERATING PRINCIPLES

3.1. Obligation to Establish Internal Whistleblower Reporting Channels

The main novelty that has been introduced with the effective date of the Directive is the obligation to establish internal whistleblower reporting channels. According to Article 8 of the Directive, legal entities in the public and private sectors with at least 50 or more employees are legally required to establish internal whistleblower reporting channels. The national legislators are free to require entities employing even fewer than 50 employees to establish such reporting channels. In view of the costs²⁷ and the complex administrative apparatus that whistleblowing reporting channels bring with them, the decision whether or not to follow the provisions of the Directive in the private sector should be proportionate to the size of the company and the risks that its activity presents to the public interest.²⁸ While Member States may encourage private sector legal entities with fewer than 50 employees to establish less prescriptive reporting channels than those set out in the Directive, the same channels should be able to ensure confidentiality and diligent investigation and follow-up of the initial complaint.

²⁶ Bachmann/ Kremer amongst others in Deutscher Corporate Governance Kodex (DCGK), Compliance Management System, Whistleblowing, 2021, Margin no. 28.

²⁷ Directive, 2018, P. 8: The costs of implementing whistleblowing channels for the private sector (medium and large enterprises) are expected to amount to €542.9 million one-time costs and €1,016.5 million annual operating costs. As for the public sector, implementation costs are expected to amount to €204.9 million one-time costs and €319.9 million annual operating costs.

²⁸ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 25 (48).

As far as the public sector is concerned, Member States may exempt municipalities with fewer than 10,000 inhabitants or fewer than 50 employees working in the public sector from the obligation to establish reporting channels. In addition, it is also possible to provide at the national level that whistleblowing reporting channels may be shared by common authorities, provided that the internally shared whistleblowing reporting channels are distinct and autonomous from the externally applicable whistleblowing reporting channels.

Empirical studies show that most whistleblowers tend to report internally, within the organisation in which they work.²⁹ Internal whistleblowing is also the best way to get information to the persons who can contribute to the early and effective resolution of risks to the public interest.³⁰

3.2. Obligation to Establish External Whistleblower Reporting Channels

The Directive in Article 10 mandates the creation of external whistleblowing reporting channels by the European Member States. The latter must designate competent authorities to receive, provide feedback and follow-up on complaints, and equip those authorities with adequate resources to accomplish those ends. The rule is silent on what “adequate resources” means. But fulfillment of the requirements referred to in the rule is only possible through the creation of an independent and autonomous organisational form within the organisation through the separation in the organisation of the authorities’ general information channels, ensuring the integrity and confidential treatment of the reports received, including their secure storage, as well as the creation of a comprehensive public information function with regard to the legal framework and general procedural references.³¹ Additionally, it is necessary for the competent authorities to designate specially trained personnel to deal with the handling of allegations, and in particular for the latter to be technically able to provide all persons concerned with information about the complaints procedures, receive and follow up on allegations, maintain contact with the whistleblower (for the purposes of providing feedback) and request additional information if necessary.³²

²⁹ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 23 (35).

³⁰ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 23 (35).

³¹ Dzida/ Granetzny, Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen, 2021, P. 3.

³² Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 29 (74): Staff members of the competent authorities who are responsible for handling reports should be professionally trained, including on applicable data protection rules, in order to handle reports and to ensure communication with the reporting person, as well as to follow up on the report in a suitable manner.

3.3. Equal Internal and External Reporting Channels

The Directive provides for equal use of internal and external whistleblowing reporting channels. The so-called third whistleblowing level – reporting to the public (e.g., to the press) – remains subsidiary to the two previously mentioned channels. The origin of this lies in the case law of the European Court of Human Rights (ECHR) on the protection of sources in the press. According to the ECHR, journalistic source protection is not simply a privilege, but an essential component of a free press. The protection of sources and the protection of whistleblowers are closely linked.³³ Thus, the Directive continues the ECHR's reasoning by weakening the need to initially offer the complaint to an internal channel.³⁴

According to Article 10 of the Directive, whistleblowers can report information about violations directly to the authorities without having first reported facts internally, for example in companies where they work or have worked. However, in accordance with Article 7 of the Directive, the rule is that the report should first be made to the internal channel, before proceeding to report through external channels, in all cases where the violation can be effectively resolved internally and where the whistleblower considers that there is no risk of retaliation. It is therefore up to Member States to encourage reporting through internal reporting channels.³⁵

One unresolved issue is how to harmonise the requirement to use an internal channel as a priority where there is no legal duty to do so. Legally, one could argue for the creation of legal standards of confidentiality of an even higher degree than those already in place at the European level for whistleblowers, as well as the extension (through the insertion of an amnesty rule) in the paragraph of the Criminal Code regulating the effects of the application of the sentence with regard to the contribution to the discovery of serious crimes, in the German law provided for in the Criminal Code (StGB) in Section 46b.³⁶ Taking Germany as an example, and without prejudice to other rules in other European legal systems, it would be necessary to compare the crimes covered by the Directive on the protection of whistleblowers and third parties with those provided for in Section

³³ EGMR, de 21.07.2011 - 28274/08.

³⁴ Jahn, NWJ-aktuell 20/2019, P. 20.

³⁵ This compromise formula stems from the fact that some member states, such as Germany and France, were in favor of a mandatory priority for internal denunciation but were not able to assert themselves in the formation of the agreement. In this sense Dzida/ Granetzny, Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen, 2021, P. 4.

³⁶ Compare Hiéramente/ Ullrich, jurisPR-StrafR 25/2019 Anm. 1; zum Spannungsverhältnis zwischen DS-GVO-Auskunftsrechten und Whistleblowerschutz: Dzida, BB 2019, 3060, P. 3066 mit Verweis auf LAG Baden-Württemberg de 20.12.2018 - 17 Sa 11/18, NZA-RR 2019, P. 242 = NZA 2019, P. 711 Ls;

100 of the German Procedural Code (StPO), which are considered serious crimes, and ensure that these crimes also benefit from the guarantees provided by the new Guideline.

As for business practice, it is of the utmost importance that whistleblower reporting channels be publicised throughout the company or business group (in the case of business conglomerates) and to all employees, regardless of their position, in a clear and simple manner. Its use and rules must be available not only in internal company guidelines, but also on the intranet, on a dedicated internal page. In addition, the legitimacy and acceptance of the whistleblowing reporting channel starts with the “tone from the top”, in which the general management recognise the channel and promote it within the company in a positive and credible manner. Additionally, it is the duty of the compliance officer or the compliance area specialist to address the issue in employee training, but also through newsletters, internal competitions, tests, risk assessments, internal communication measures, and in the annual evaluation of employees as a condition for receiving part of the bonus, among other measures. Above all, it is necessary to make clear to the employees the confidential nature of the internal reporting channel, creating confidence in its use, as well as in the treatment of the allegations.³⁷ The greater their confidence in the confidentiality of the reporting channel and the thoroughness of the investigation, the greater the chance that it will be used. This may lead employees to prefer using the internal reporting channel before turning to external agencies.

There is an understanding in the literature that offering a financial advantage to the whistleblower may encourage him to “break the wall of silence” in favor of using the internal reporting channel.³⁸ However, this form of offering an advantage can create an atmosphere of mistrust, and is not very focused on business success, which is why it should not be followed.³⁹

Articles 13 and 15 of the Guideline regulate the protection of whistleblowers when they report to the public authorities and the press only as a last resort. According to what is prescribed, the person who makes a public allegation to the press benefits from protection if it turns out that he or she initially made an internal or external denunciation, without appropriate action having been taken

³⁷ For more information regarding the implementation of whistleblower systems in European companies, see the Swiss study on the practice of developing whistleblower protection procedures at: www.whistleblowingreport.de.

³⁸ Granetzny/ Krause, CCZ 2020, P. 29; Schmolke, NZG 2020, 5-11; Dzida, NZA Editorial 23/2012.

³⁹ In Germany there is no legal incentive to reward whistleblowers. The positive aspect generated by the financial side is to motivate the whistleblower to use the internal whistleblowing channel instead of turning to the external channel first. This is related to whistleblowers who no longer work for the company in which violation of an internal rule or law came to their attention during the period of their employment contract.

as a consequence of the allegation within the legal time limit. In addition, information about the violation must be published when there is reason to believe that the violation constitutes imminent or manifest danger to the public interest (in an emergency situation) or an irreversible risk, or that there is a risk of retaliation, diminished prospect that the violation will be resolved effectively, or in situations where evidence may be concealed or destroyed, or where an authority may be in collusion with or involved in the violation.

It is indisputable that with the insertion of the trilateral whistleblower system at the European level, the possibility of the whistleblower turning to the public body before reporting to the company brings enormous risks to the reputation of the latter. It appears to be doubtful whether the unconditional external possibility that the offering of allegations directly to public authorities will adequately balance the conflicting interests of the public interest in the process and the whistleblower's freedom of expression, on the one hand, and *pars pro toto*, the economic interests of the company, on the other.⁴⁰ In this sense, the lesson for the national legislator is, without a doubt, to ensure that there is sufficient support for internal whistleblowing reporting channels.

3.4. Confidentiality

The Directive requires Member States to establish reporting channels in such a way that they do not allow access by unauthorised personnel to receive the reports and they must ensure the confidentiality of the reporting person and third parties mentioned in the report.

As far as internal reporting channels are concerned, confidentiality is mandated and is directed mainly to the identity of the whistleblower and third parties mentioned in the complaint, in order to prevent access by unauthorised personnel, according to Article 9 of the European rule.

As for external channels, Article 12 states that they need to be designed, installed and operated so as to ensure the completeness, integrity and confidentiality of the information and also to prevent access by unauthorised personnel. Thus, both internal and external channels offer whistleblowers and third parties the same protection regarding their identity.

It is still questionable whether the protection of personal data referred to in the Directive is absolute or whether whistleblowers or third parties may in certain cases have their data disclosed under certain circumstances.

The intent of Article 16 of the Directive is that Member States need to ensure that without the whistleblower's explicit consent, none of his or her personal

⁴⁰ Dzida/ Granetzny, Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen, 2021, P. 5.

data, whether or not derived from his or her identity, is disclosed to a person other than the person responsible for processing the complaint. However, paragraph 2 of the same article provides that the identity of the whistleblower is to be disclosed if a necessary and proportionate obligation under Union or national law exists in the context of an investigation by national authorities or judicial officials, with a view to safeguarding the rights of defence of the person concerned. The whistleblower must be informed before the disclosure of identity or data takes place.

In this context the first decision of the LAG (Stuttgart Labour Court) of December 20, 2018, which ruled that employees must have the right to inspect files in complaints made by third parties which concern them,⁴¹ is relevant. The mere promise to keep the identity secret is not in itself a sufficient reason for a permissible withholding of information about the whistleblower.⁴²

The protection of the identity and other personal data of whistleblowers is not absolute. On the contrary, the whistleblower has to reckon with the fact that his or her identity may be revealed if he or she puts it in the report.

This position reflects current German legal practice. The safest way for a whistleblower to reveal his or her identity is to turn to a lawyer who acts as ombudsman in resolving the complaint. However, the Bochum Regional Court ruled in the appeals court that the documents that a lawyer receives, prepares and stores as ombudsman about the references or facts received from the whistleblower are not free from seizure under Section 97, (1) no. 3 StPO (German Code of Criminal Procedure), since the ombudsman's mandate relationship exists only towards the company and the whistleblower is not considered an accused, but simply a witness.⁴³

In the Jones Day decision, the *Bundesverfassungsgericht* (German Federal Constitutional Court. Hereinafter, Federal Supreme Court) also stated that the prohibition of seizure under Article 97 (1) no. 3 StPO (German Code of Criminal Procedure) presupposes a relationship of trust between the person subject to professional secrecy and the accused person.⁴⁴ Section 160 a (1) no. 1 of the same law prohibits investigative measures against lawyers who would presumably produce conclusions or evidence about which they would be authorised to refuse

⁴¹ LAG Stuttgart 20.12.2018 - 17 Sa 11/18.

⁴² Altenbach/ Dierkes, EU-Whistleblowing-Richtlinie und DSGVO, 2020, P. 129. The present article does not discuss specific rules of data protection law or labour law, which may be related to the EU Directive.

⁴³ Vitorino Clarindo dos Santos, Jorgete, 2020, Lecture „Internal Investigations“ at ICRio: <https://youtu.be/j8fAUKlzhU>; LG Bochum NSTZ 2016, P. 500; Criticised by Park, Beschlagnahme und Durchsuchung, 4. Aufl. 2018, Rn. 545 et seq.; Vogel/ Poth CB 2019, P. 45, especially p. 48; LG Hamburg NJW 2011, P. 942 (HSH Nordbank).

⁴⁴ BVerfG NJW 2018, P. 2385, especially P. 2388, Rn. 83 ff; Criticized by Xylander/ Kiefner/ Bahlinger BB2018, P. 2953, especially P. 2954.

to witness.⁴⁵ However, according to Section 160 a (5) of the StPO, this provision is considered an accessory rule in relation to Section 97 of the Code of Criminal Procedure, considered *lex specialis*, in the case of seizure.⁴⁶ Furthermore, the interest of the State in the Criminal Procedure prevails over the interest of the client with regard to secrecy.⁴⁷ Thus, a whistleblower (who is not also an accused) who seeks a lawyer as ombudsman (and not as a defence attorney) must fear, *de lege lata*, that his or her identity will be revealed, in case the law firm he or she has hired suffers the consequences of a search and seizure warrant (e.g., if the law firm is the object of a search and seizure on the matter reported by the whistleblower).⁴⁸ It should be noted, with regard to the confidentiality of the attorney-client relationship, that the Federal Supreme Court, in its constant jurisprudence, generally sets high standards for search and seizure in law firms, which is why it fortunately does not constitute a daily practice in the country.⁴⁹

The same cannot be said with respect to companies, which cannot invoke the provision of Section 160 a, of the Code of Criminal Procedure, which is likely to be applicable in any cases where the search is not also intended for a seizure.⁵⁰

Therefore, the claim that internet- or intranet-based whistleblowing systems protect the confidentiality of information and the anonymity of whistleblowers better than the use of attorneys as *ombudsmänner/ ombudsleute*⁵¹ is not correct. This is because companies receiving whistleblowers' allegations or reports cannot invoke the confidentiality of attorney-client communication, which is also in the public interest, and thus possibly attack the lack of proportionality of a search warrant.⁵²

Moreover, in the case of a search of a lawyer's office, there is less concern that the investigating authorities may use their discretion and, pursuant to Section 110, Subsection 1, Code of Criminal Procedure, "examine" the entire database and, in addition, also the documents and information of clients and whistleblowers

⁴⁵ Dilling, CCZ 2019, P. 6.

⁴⁶ BVerfG NJW 2018, P. 2385, especially 2387, Rn. 73 et seq.

⁴⁷ BVerfG NJW 2018, P. 2385, especially 2389, Rn. 90.

⁴⁸ Dilling, CCZ 2019, P. 6, Rn. 218.

⁴⁹ BVerfG NJW 2018, P. 2385, especially 2386, Rn. 68; Park, *Beschlagnahme und Durchsuchung*, 4. Aufl. 2018, Rn. 828: „In this respect, the Federal Supreme Court requires a ‚special constitutional justification for the seizure of professional secrets.‘ The correlating prohibition on the excessive acquisition of evidence and data rarely plays a role in procedural reality. Investigators very often proceed here with the ‚vacuum cleaner method.‘ This has a particularly severe effect when fundamental rights of uninvolved third parties are affected.“

⁵⁰ Xylander/ Kiefner/ Bahlinger, BB 2018, P. 2953, especially 2954; Dilling, CCZ 2019, P. 6, Rn. 218.

⁵¹ Wiedmann/ Seyfert, CCZ 2019, P. 12, sobretudo 17; Dilling, CCZ 2019, P. 6.

⁵² Dilling, CCZ 2019, P. 6.

who are not directly affected by the complaint made by the whistleblower, which is not necessarily true of companies.⁵³ It therefore makes more sense to combine the technical possibilities offered by internet-based whistleblower systems and existing legal privileges for lawyers in order to provide the greatest possible protection for whistleblowers, so that the information they securely transmit can be received by their attorneys in the same way.⁵⁴ They may also make themselves available for face-to-face meetings as referred to in Article 9 (2) of the Directive.

In addition, according to its Article 3 (3) (b), the Directive does not affect the application of Union or national law with respect to the protection of the confidentiality obligations of attorneys and doctors.⁵⁵

At the same time, it can often happen in the course of internal investigations – if necessary, following internal notifications under Article 8 of the Directive – that law enforcement authorities “step in”⁵⁶ and seize company documents, which may lead to the identity of the whistleblower being revealed.⁵⁷

The confidentiality of the whistleblower’s identity is thus protected only to a very limited extent by Article 16 of the Directive. It is therefore particularly alarming that Article 5 (2) of the Directive leaves it to Member States to decide whether or not to accept anonymous reports and follow up on them. However, if the whistleblower cannot be sure that his or her identity will be protected, he or she may submit his or her report anonymously, if in doubt. If such an anonymous denunciation is not received and followed up as it should be, it will fail.⁵⁸

Nevertheless, and according to Article 25 (1) of the Directive, Member States may introduce or maintain provisions that are more favorable to the rights of whistleblowers than those laid down in the European rule. As safeguarding the identity of the whistleblower is a central concern of the Directive, this must be absolutely protected in practice so that the objectives sought by the whistleblower can be carried out.⁵⁹ Thus, the conflict between law enforcement interests on the one hand and the confidentiality of the whistleblower’s personal data on the other must be resolved in accordance with the objectives of the Directive, so that the

⁵³ Dilling, CCZ 2019, P. 6; Peters, NZWiST 2017, P. 465, sobretudo 467; Heinrich, wistra 2017, P. 219, sobretudo 223; Basar/ Hiéramente, NStZ 2018, P. 681.

⁵⁴ Dilling, CCZ 2019, P. 6.

⁵⁵ Dilling, CCZ 2019, P. 6.

⁵⁶ Dilling, CCZ 2019, P. 6; Xylander/ Kiefner/ Bahlinger BB 2018, P. 2953, especially P. 2956.

⁵⁷ Dilling, CCZ 2019, P. 6; Rieder/ Menne CCZ 2018, P. 203, especially P. 205.

⁵⁸ Dilling, CCZ 2019, P. 6; Bitmann/ Brockhaus/ v. Coelln/ Heuking, NZWiST 2019, P. 1, especially P. 5.

⁵⁹ Dilling, CCZ 2019, P. 6.

latter are free from discovery.⁶⁰ For while it is true that whistleblowing often fails due to the existing lack of trust on the part of whistleblowers, the elimination of this distrust can only be successful if the whistleblower's identity and personal data are protected and the whistleblower can be sure that they will remain so in any case.⁶¹

IV. WHISTLEBLOWER PROTECTION MEASURES

4.1. Protection from Reprisals and Liability and Punishment

The lack of adequate protection from the provisions of the Directive regarding the identity of the whistleblower has already been thoroughly addressed in section 6 of this article.

According to the provisions of Article 19 of the Directive, Member States shall prohibit any form of retaliation against whistleblowers.

The definition of retaliation is provided in Article 3, para. 12 of the Proposal for a Directive of the European Parliament and of the Council on the protection of persons who report breaches of Union law. According to this, "retaliation" is any threatened or actual act or omission prompted by the internal or external reporting which occurs in a work-related context and causes or may cause unjustified detriment to the reporting person.

The damages are also listed by the legislator in Article 19 of the Directive, including suspension, layoff, dismissal, demotion or withholding of promotion, transfer of duties, change of location of place of work, reduction in wages and change in working hours, withholding of training, negative performance assessment or negative reference for employment purposes, imposition or administering of any disciplinary measure, reprimand or other penalty, (including financial) coercion, intimidation, harassment or ostracism, discrimination,

⁶⁰ Vogel/ Poth, CB 2019, P. 45, especially 47. Free translation of the authors' comment, „The seizure of whistleblower reports disrupts the architecture of an effective and functional whistleblower system.“

⁶¹ Vogel/ Poth, CB 2019, P. 45, especially P. 47. Free translation of the authors' comment: "Whistleblowers who cannot rely on preserving their anonymity will rarely report violations of law for fear of reprisals, regardless of the level of legal protection, in order not to expose themselves to whistleblowing charges (wall of silence)." Dilling, CCZ 2019, P. 6. Bittmann/ Brockhaus/ v. Coelln/ Heuking, NZWiSt, 2019, P. 1, especially P. 5. Free translation of the authors' comment: "However, in the context of whistleblowing, there is an urgent need to recognize the ombudsmänner/ ombudsleute's right to silence and freedom to seize their documents, as the effectiveness of a whistleblowing system depends on the anonymity of whistleblowers."

disadvantage or unfair treatment, failure to convert a temporary employment contract into a permanent one, where the employee has legitimate expectations that he or she would be offered permanent employment, non-renewal or early termination of a temporary employment contract, harm, including to reputation, particularly in social media, or financial loss, including loss of business and loss of income, blacklisting, based on formal or informal industry-wide agreement, which may result in the complainant's being unable to find future employment in the industry or sector, early termination or cancellation of a contract for the supply of goods or provision of services, revocation of a license or permit, as well as referrals for psychiatric medical treatment.

A causal link between the listed measures and the whistleblower's complaint is indispensable: A close connection must be found between the complaint and the unfavorable treatment suffered, directly or indirectly, by the whistleblower, so that this unfavorable treatment is considered an act of retaliation. Consequently, the whistleblower may benefit from legal protection in this context.⁶²

Protection against retaliation as a means of safeguarding freedom of expression and freedom and pluralism of the media is granted both to persons who report information about acts or omissions within an organisation (through internal whistleblowing) or to an external authority (through external whistleblowing) and to persons who make such information available in the public sphere, for example, directly to the public through online platforms or social media, or to the media, elected representatives, civil society organisations, trade unions or business and professional organisations.⁶³

With regard to imputation of liability, this is regulated in Article 21, no. 2 of the Directive, according to which whistleblowers shall not incur any type of liability, provided that they have reasonable grounds to believe that the reporting or public disclosure of such information was necessary to reveal a violation under the Directive, especially in matters provided for in Article 21, para. 7, namely in legal proceedings for defamation, copyright infringement, breach of secrecy, breach of data protection rules, disclosure of trade secrets, or for claims for damages based on private, public law or collective bargaining agreements.

The high legal costs arising from litigation through the courts are a topic that can scare off whistleblowers, as foreseen in Explanatory Memorandum no. 99 of the Directive. Thus, companies committed to keeping them quiet will try to prove their bad faith, intending to remove them from the cloak of legal protection, thus

⁶² Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 25 (44).

⁶³ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 25 (45).

imputing liability to them.⁶⁴ It is then up to the whistleblower to claim that his complaint is based on the provisions of Article 99 of the Directive's Explanatory Memorandum, and it is up to the current or former employer to prove otherwise.⁶⁵

The criticism made in this context by *Dilling*, however, is that there is little support in the Guideline for the solution to the problem arising from Article 21 (7), since it is the whistleblower himself or herself who has to prove the reasonable grounds on which the whistleblower's disclosure or public disclosure of the violation is based, and not the employer or former employer.⁶⁶ This is not an easy matter to prove as a defendant, highlighting here the lack of regulation of the reversal of the burden of proof.⁶⁷ Depending on the whistleblower's financial and emotional condition and health, the consequences of a liability lawsuit may dissuade him or her from offering denunciations.

Finally, with regard to protection against reprisals other than those mentioned above, the European Directive provides in its Article 21 (8) that Member States shall take the necessary measures to ensure that remedies and full compensation are available for the damage suffered by the persons protected under Article 4 who meet the requirements of Article 5 (1), that is, having reported in good faith. These guarantee measures include financial assistance and support measures, including psychological support for whistleblowers in legal proceedings.⁶⁸

4.2. Reversal of Burden of Proof

Under the Directive, it is likely that in order to justify acts of reprisal, it will be difficult for the whistleblower to prove the existence of the causality relationship between the complaint and the retaliation, the offenders of the latter possibly having more power and resources to document the measures taken as well as their substantiation. Therefore, once the whistleblower demonstrates *prima facie* that they have reported violations or made a public disclosure under the Directive and have suffered harm, there should be a reversal of the burden of proof to the person taking the harmful measures, who will thus be compelled to demonstrate that those measures were in no way connected to the complaint or to the public disclosure.⁶⁹

⁶⁴ Dilling, CCZ 2019, P. 9.

⁶⁵ Dilling, CCZ 2019, P. 9.

⁶⁶ Dilling, CCZ 2019, P. 9.

⁶⁷ Regarding the reversal of the burden of proof, see item 4.2.

⁶⁸ The recognition of the provision of such guarantees is provided in Article 20, para. 2 of the Directive.

⁶⁹ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 31 (93).

With regard to the reversal of the burden of proof, there is a doctrinal understanding that this position of the Guideline carries a risk of abuse, since employees may claim that by offering an “alleged complaint” they will not be fired.⁷⁰ This is especially true in European countries, where the whistleblower protection system is deeply rooted; Great Britain may be cited as an example. Thus it is not uncommon for the number of whistleblowers to rise in England when a company is about to make staff cuts.⁷¹ In order to combat this practice, the employer must produce extensive documentation to be able to prove, if necessary in a subsequent dismissal action, that the measures were not related to the complaint made by the employee.⁷²

Another aspect to be reported is that, according to Article 21 no. 1 of the Directive, Member States must take the necessary measures to ensure protection from acts of retaliation for persons who enjoy the protection of the Directive. Accordingly, Article 21 para. 6 provides that persons referred to in Article 4 must have access to remedies against acts of victimisation, where appropriate, including precautionary measures pending the outcome of judicial proceedings, in accordance with national law.

Article 21 (5) rules that in proceedings before a court or other authority, concerning damage suffered by a whistleblower, and subject to the whistleblower’s demonstration that he or she has made a report or public disclosure and suffered damage, it shall be presumed that the damage corresponds to retaliation for having made the report or public disclosure. In such cases, it is incumbent on the person who has taken the adverse measure to demonstrate that such measure was based on duly justified grounds. In the Explanatory Memorandum to Directive no. 95, it is recognised that while the types of legal action may vary according to legal systems, they should ensure that compensation or reparation is real and effective, proportionate to the harm suffered, and dissuasive.

It must be clear, however, that the protection afforded to the whistleblower is limited in practice. It will not be too difficult for the employer to prove the absence of a causal connection between the whistleblower and, for example, the dismissal, in cases where a written warning was given some time after the whistleblower’s allegation was made.⁷³ Therefore, the reversal of the burden of proof only helps the whistleblower in part.⁷⁴ It is known that the lack of financial

⁷⁰ Dzida/ Granetzny, *Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen*, 2021, P. 5.

⁷¹ Dzida/ Granetzny, *Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen*, 2021, P. 5.

⁷² Dzida/ Granetzny, *Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen*, 2021, P. 5.

⁷³ Dilling, CCZ 2019, P. 8.

⁷⁴ Dilling, CCZ 2019, P. 8.

equality in the search for the right in court can lead companies to drag out lawsuits for years, which will make the whistleblower's situation very difficult. In countries where there is no Public Defender's Office, it is necessary that the whistleblower find not only one, but several lawyers who are willing to act in his or her defence, receiving only predetermined amounts in minimum fee tables, which is not necessarily easy to find.⁷⁵ It should be emphasised that the complexity of the matter is such that the whistleblower will in fact need more than one suitably qualified professional to defend him.⁷⁶ It is of little use, therefore, "to have or to be with the Law" if he lacks resources in the execution of his claim.⁷⁷

It is recommended in this context that companies in particular thoroughly document their employees' evaluations, bonus systems, career developments, and warnings of performance issues, as well as problems and conflicts that have already been raised in isolation, in order to create a favorable evidence base for the company in the event of a legal dispute.⁷⁸

4.3. Penalties

Article 23, par. 2 of the Directive requires Member States to provide for effective, proportionate and dissuasive penalties applicable to natural or legal persons who prevent or attempt to prevent whistleblowing, engage in acts of retaliation against whistleblowers, bring vexatious proceedings or breach the duty to keep their identity or data confidential.

European law further provides – in addition to the express prohibition of retaliation imposed by law – that it is essential that whistleblowers who are subject to acts of retaliation have access to remedies and compensation. The appropriate remedy in each case should be determined according to the type of retaliation suffered, and compensation for the loss suffered should be in full accordance with national law. The appropriate remedy could take the form of action for reinstatement, for example, in the case of dismissal, transfer or

⁷⁵ Moreover, the court's agreement to offer gratuitous justice refers only to a single retained attorney.

⁷⁶ Dilling, CCZ 2019, P. 8.

⁷⁷ This difficulty is recognized in Explanatory Memorandum no. 99 of the European Directive, which states that legal costs may be a significant expense for whistleblowers who challenge their retaliatory measures through the courts. Although they may be able to recover these costs at the end of the procedure, they may not be able to afford them at the beginning of the procedure, especially if they are unemployed and blacklisted. In certain cases, legal aid in criminal proceedings, in particular when complainants meet the conditions set out in Directive (EU) 2017/1919 of the European Parliament and of the Council, and, more generally, support for persons in severe economic need, may be essential for the effective exercise of their rights to protection.

⁷⁸ Dzida/ Granetzny, Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen, 2021, P. 5.

demotion, as well as for refusal of training or promotion, or for restoration of a cancelled permit, license or a contract; for compensation for current and future financial loss, for example, for lost past wages, but also for future loss of income, additional costs to a change of occupation; and compensation for other economic damage, such as litigation expenses and health care costs, as well as for intangible damage such as pain and suffering.⁷⁹

According to explanatory memorandum no. 102 of the Guideline, criminal, civil or administrative sanctions are necessary to ensure the effectiveness of the rules on whistleblower protection. It is believed that imposing sanctions on persons who commit retaliatory or other harmful acts against whistleblowers may discourage them from committing them.

The sanction regarding the disclosure of false information made by the whistleblower when offering the denunciation (art. 23, no. 2), will be dealt with in section 4.4 below.

4.4. Truthfulness as a Ground for Whistleblower Complaints

Whistleblowers benefit from the protection guaranteed by the European legislator if the information about the violations they reported was true at the time it was presented in the complaint and whose matters were covered by the scope of application of the Directive, according to its Article 6 (1) (a).

Legal protection requires that the information presented by the whistleblower be truthful, and whistleblowers who, being aware, report facts or situations containing errors are not legally protected. Veracity as a criterion for motivating whistleblower reporting predates the directive itself and was already included in the work authored by the European Parliamentary Assembly no. 2300 of 2019.⁸⁰

Irrelevant to the offering of a whistleblower complaint remains the motive that moved the whistleblower to report.⁸¹

According to the Directive's explanatory memorandum, truthfulness, as a whistleblower's motive requirement, is an essential safeguard against malicious, frivolous or abusive whistleblowing, as it ensures that persons who knowingly and deliberately report erroneous or misleading information at the time of whistleblowing do not enjoy protection. At the same time, the requirement ensures that protection does not cease if the whistleblower has reported inaccurate

⁷⁹ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 32 (94).

⁸⁰ Resolution 2300, 2019, Improving the protection of whistleblowers all over Europe.

⁸¹ Dzida/ Granetzny, Die neue EU-Whistleblowing-Richtlinie und Ihre Auswirkungen auf Unternehmen, 2021, P. 6.

information about violations in good faith.⁸² Similarly, whistleblowers should be entitled to protection under the Directive if they have reasonable grounds to believe that the information reported falls within its scope.⁸³

One of the difficulties presented by the doctrine is in ensuring that the whistleblower is not acting in bad faith when he or she reports.⁸⁴ There will always be the risk that the opposing party will try to prove the inexistence of good faith, in order to deprive the whistleblower of the protection guaranteed by law.⁸⁵

The European whistleblower protection order, when it comes to the veracity of information as a criterion for motivating whistleblowing, resembles § 93 Abs. 1, S. 2 of the German Stock Corporation Act (AktG), which codifies the so-called Business Judgement Rule. Under the AktG, the board of directors does not violate its duty to make a business decision based on adequate information, even if such decision later proves to be wrong, if it has acted in good faith.⁸⁶ In both whistleblower protection laws, as well as the Business Judgment Rule reference in the Corporations Act, a decision made in good faith based on valid facts is favored.⁸⁷

It is not an easy matter to assess in corporate practice whether good faith based on existing information exists on the part of the board of directors, which can, in this respect, rely on highly qualified and experienced lawyers in its defence.⁸⁸ Whether whistleblowers can afford the same technical armor in their favor, years of enforcement practice will demonstrate. *Dilling* adds that whistleblowers with a lack of knowledge in the legal field may find it difficult even to know whether the information they wish to disclose falls within the scope of the Directive.⁸⁹

Business practice shows a great diversity of reasons why someone becomes a whistleblower, and the European legislator has been criticised for seeming to

⁸² Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 23 (32).

⁸³ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 23 (32).

⁸⁴ Garden/ Hiéramente, BB 2019, P. 963, especially P. 964: "It is unclear what standard of care the whistleblower must apply when examining the requirements for a report"; Vogel/ Poth, CB 2019, P. 45, especially 46.

⁸⁵ Dilling, CCZ 2019, P. 4.

⁸⁶ Vitorino Clarindo dos Santos, Jorgete, Rechtsfragen der Compliance in der internationalen Unternehmensgruppe, 2013, P. 5.

⁸⁷ Exposition of reasons to the European Directive on the protection of whistleblowers, 2019, P. 23 (32).

⁸⁸ Dilling, CCZ 2019, P. 4.

⁸⁹ Dilling, CCZ 2019, P. 4.

know of only two types: those who act in good faith and those who blow the whistle in bad faith. There is no doubt that the whistleblower who acts in good faith needs protection, regardless of whether the facts listed in the report are true – bad-faith allegations already lack legal protection. The fact is that investigation in corporate groups is frequently more complex than the case to which the law offers protection, as the Compliance Officer not rarely deals with whistleblowers who, in the overwhelming majority of cases, participated in some way in what they report, either as co-authors, or through acts of action or omission that compromise or even incriminate them. Co-authors and accessories do not, as a rule, report false information.⁹⁰ However, it is questionable whether the prohibition of reprisal will allow companies to punish whistleblowers disciplinarily in the labour field if their sphere of responsibility is proven. According to *Hommel*, this is necessary in order to achieve appropriate results, both with regard to personal liability and to ensure the general functioning and acceptance of a compliance management system in the company.⁹¹

The Directive provides in Article 23 (2) that Member States should provide for effective, proportionate and dissuasive sanctions applicable to whistleblowers where the latter have knowingly communicated or publicly disclosed false information. States must also provide for measures to compensate for the damage resulting from such false reporting or public dissemination, in accordance with national law. It is unacceptable for the whistleblower to mobilise the internal apparatus of a company, as well as the state machine, if he knows beforehand that he is disclosing information that is not true. It is worth remembering that there is a feasible difficulty of proof in this case.

V. PROCEDURE

Regarding the procedure for receiving and handling internal whistleblower complaints, the European Directive provides in its Article 9 (1) (b) that an acknowledgement of receipt of the complaint must be sent to the whistleblower within seven days from the date of receipt.

In addition, it requires that an impartial person or service be designated, who will maintain communication with the whistleblower and, if necessary, request additional information and provide feedback to the reporting person.

⁹⁰ Hommel, CCZ 2021, Die Zusammenarbeit mit Whistleblowern - Anmerkungen zu der EU-Whistleblower-Richtlinie, P. 2 e 3.

⁹¹ Hommel, CCZ 2021, Die Zusammenarbeit mit Whistleblowern - Anmerkungen zu der EU-Whistleblower-Richtlinie, P. 3.

Additionally, the Directive requires that a reasonable time limit be established for providing feedback to the whistleblower, not to exceed three months from the acknowledgement of receipt. In cases where the acknowledgement of receipt has not been sent to the whistleblower, the time limit of three months from the seven days after the submission of the offer of complaint applies.

Even for companies that already have a whistleblower system in place, the Directive brings with it the need to adapt their system, either through the new rule of a specific deadline for acknowledgement of receipt of the complaint, or in relation to the period of time regarding the return to be given to the whistleblower, within 3 months. It is important to note that these 3 months do not necessarily include the specific time to end the investigation, since, depending on the subject and concrete case, as well as the actors involved in it during the examination of the facts and new information that may arise during the process, the investigation time can be extended.⁹² Efforts must always be made to guarantee a quick response, in respect to the trust of the whistleblower in the Compliance system and to other deadlines provided in other legislation for the conclusion of the investigation, especially with regard to Labour Law.

As for the deadline for processing complaints through external whistleblowing channels, the Directive refers the law enforcer to Articles 11 and 12, which establish the rules regarding the application of internal whistleblowing channel deadlines, recommending first the use of the latter before filing a complaint through the external channel.⁹³

With regard to public whistleblowing, understood as reporting to the press, a whistleblower who discloses information is entitled to protection under the Directive if any of the following conditions are met: He or she has initially reported internally and externally or directly externally in accordance with Chapters II and III, but no appropriate action has been taken on his report within the timeframe set out in Article 9(1)(f) or Article 11(2)(d); or the whistleblower has reasonable grounds to believe that

- the breach may pose an immediate or obvious threat to the public interest, for example in an emergency situation or where there is a risk of irreversible damage;
- in the case of an external report, there is a risk of reprisals or, because of the particular circumstances of the case, there is little prospect of effective action

⁹² Art. 11, para. 5 EU Directive 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: Member States may provide that, in the event of a high inflows of reports, competent authorities may deal with reports of serious breaches or breaches of essential provisions falling within the scope of this Directive as a matter of priority, without prejudice to the timeframe as set out in point (d) of paragraph 2.

⁹³ See for this information in this article under heading 5 - Internal and External Equality of Information Channels.

being taken against the breach: for example, because evidence may be suppressed or destroyed or where there may be collusion between a public authority and the perpetrator of the breach or the public authority may be involved in the breach.

It is worth highlighting that Article 15 does not apply in cases where a person discloses information directly to the press on the basis of specific national provisions which constitute a system of protection for freedom of expression and information.

The Guideline is silent as to the validity of the time limits for filing a public accusation.⁹⁴

VI. THE POSITION OF THE U.S. DEPARTMENT OF JUSTICE (DOJ) IN EVALUATING THE EFFECTIVENESS OF COMPLIANCE PROGRAMMES

On June 1, 2020 the U.S. Department of Justice (DOJ) updated its guidance to its prosecutors on how to conduct investigations.⁹⁵ The guidance also helps corporations to better design programmes to mitigate potential misconduct, and if an issue arises, to negotiate a more favorable resolution. How the government resolves an investigation is partly dependent upon quality of a corporate compliance programme, not only when misconduct occurred but during the investigation and after.

Prosecutors should look at three basic questions:

1. Whether a corporate compliance programme is well designed:
 - The focus should be geared towards constant review, testing, and improvement, and not merely a risk assessment at the outset.
 - This constant scrutiny applies to *both* the corporation itself as well as third parties, particularly common ways to hide misconduct or bribes, and should be done at all times.
 - It is also helpful if the programme and risk assessment utilise other resources in the corporation or in the industry as part of its continual improvement. One example is making training, as well as availability of policies and procedures (e.g., code of conduct), more accessible/

⁹⁴ See for this information in this article under heading 5 - Internal and External Equality of Information Channels.

⁹⁵ U.S. DEP'T JUSTICE, CRIMINAL DIV., EVALUATION OF CORPORATE COMPLIANCE PROGRAMS (June 2020), <https://www.justice.gov/criminal-fraud/page/file/937501/download>.

- searchable to employees in order to maintain compliance, report issues confidentially, and so on.
- While this guidance focuses on the corporation's ability to improve its internal compliance programme, the DOJ offers a hotline for employees of any company to report misconduct to the Office of the Inspector General.
2. Whether the programme is implemented in good faith with the appropriate level of resources and empowerment to function effectively:
- The focus should be reasonable based on corporate size, industry, landscape, and so on, and the compliance programme should continually adapt to fit corporate needs and risk profile.
 - Creation of an internal channel for whistleblowers to report misconduct contributes to the effectiveness of the compliance programme.
 - Compliance personnel should be given the appropriate training and resources (including manpower and mandate) to monitor and test policies and controls as well as access to appropriate authorities.
 - A culture of encouraging compliance (and discouraging noncompliance) should be incentivised at every level.
 - The DOJ will look at the Human Resource Process and who participates in making disciplinary decisions.
3. And, whether the programme actually works in practice:
- An adequate and effective corporate compliance programme should be implemented, or an existing one should be improved. Prosecutors will want to know why a corporation has chosen to set up a compliance programme a certain way and how it has evolved over time.
 - Whistleblowers should be able to report suspected misconduct via internal confidential and/or anonymous channels.
 - Existence of misconduct does not automatically mean the compliance programme was ineffective at the time of misconduct.

This guidance was first issued in 2017 and its focus is to reinforce the notion that companies should be continuously improving to make sure that they are not criminally prosecuted.

VII. OUTLOOK AND FINAL CONSIDERATIONS

The Directive puts additional burdens and responsibilities on small and medium-sized companies with at least 50 employees, which do not yet have a properly installed whistleblowing reporting channel. Companies that currently already have a whistleblower system in place need to review it, adapting it to the

new rules that have come into effect with the Directive. This adaptation concerns both the technical parts of the Directive and the procedure to be observed for the proper treatment of the whistleblower, as well as the necessary qualifications for personnel to deal both with the processing of a whistleblower complaint and with the whistleblowers, whether or not the latter wish to make their identity public.

As an essential element of the compliance system, the good functioning of the whistleblowing reporting channel depends on the guarantee of confidentiality of the whistleblower, related to his or her identity and to the data contained in his or her reports, as well as those of third parties reported by the whistleblower.

Confidentiality is not absolute in all European Union countries today. There is greater protection in the judicial seizure of data in law firms than in companies, whether or not the latter have a legal department or compliance system properly in place. The role of the lawyer as ombudsman is of paramount importance in this matter.

The protection of the confidentiality of the whistleblower is essential in the success of the whistleblower system. Otherwise, a potential whistleblower will remain silent, behavior that can permit the continuation of internal or legal infractions.

The continued development of the compliance system also depends on the whistleblower. Therefore, it is the task of each member state, before incorporating the rules contained in the Directive into its national legal system, to analyse related national laws (e.g., criminal law, labour law) and adapt them to ensure that companies and law firms are prohibited from seizing information submitted by the whistleblower.

As the Directive allows the whistleblower to approach the public body before reporting possible violations in companies he or she works or has worked for, it is necessary that companies create or adapt whistleblowing reporting channels in such a way that they motivate the whistleblower to report. Here too, ensuring the absolute confidentiality of his or her identity and data and that of third parties plays an extremely important role. Otherwise, companies run the risk of seeing flaws in their internal processes taken to public agencies, without first being aware of it, at possible risk to their reputation.

In some European countries, the establishment of internal reporting channels requires the approval of the employee body (e.g., works council or unions), which must be obtained as soon as possible. Approval is not only a legal requirement, it also increases the credibility of the whistleblower's reporting system.

Another pivotal factor in increasing trust by whistleblowers in whistleblowing systems, is the prohibition of reprisals. It is essential that the legal treatment to be offered by Member States strengthens the whistleblower on this point. In addition, financial support must be guaranteed, as well as comprehensive personal support (including costs for medical assistance expenses as well as for moral damages

such as pain and suffering), in order to support the whistleblower in dealing with the consequences of the facts he or she reports, even during the investigation phase.

As far as the costs of implementing and operating whistleblowing channels in companies are concerned, they will be much higher than those estimated by the Guideline, both for the whistleblower and for the companies that need to have an apparatus to process the reported information and process it properly. And these costs only make sense if companies do not have to fear having their internal information taken public, even before they can be informed about it. Small and medium-sized European companies need to be guaranteed the ability to process whistleblowing, so that they can effectively enforce the legality principle. Whistleblowers here run the risk of being financially unable to afford competent technical defence, should they become victims of reprisals.

As for the employees and officials assigned to receive and handle the complaint, it is necessary that they are qualified for this purpose, receive adequate training, and that they know and have the technical conditions to properly process the complaint. Lawyers, investigators and compliance officers are the most suitable people to perform this function. Training must also be offered to all employees and officers of the company, at all levels of the hierarchy, regarding the use of the process and its safeguards related to internal whistleblowing. This includes confirmation that a complaint has been made within one week and a response to the whistleblower within no more than three months.

With regard to the reversal of the burden of proof by European companies, caution will be required more than ever in future documentation with employees and officials, since there is a danger here that the whistleblower will take advantage of the national norm introduced in incorporation of the Directive in order to “dig” for protection in cases where he or she is about to have his or her employment relationship terminated by his or her employer.

In general the creation of the Directive will have a positive impact on companies in Member States, having to emphasise the existence of its chances and above all many challenges to whistleblowers, companies, especially small and medium-sized ones, as well as to the Member States of the European Union.

References

Altenbach, T and Dierkes, K, EU-Whistleblowing-Richtlinie und DSGVO, CCZ, 2020, P. 126-132.

Anstageslicht.de, Dr. Margrit Herbst Ehemals, Tierärztin im Schlachthof Bad Braustet, <<https://www.anstageslicht.de/menschen-dahinter/dr-margrit-herbst/>>.

Arte, Der Gefährlichste Mann in Amerika, Daniel Ellsberg und die Pentagon-Papiere, <<https://www.youtube.com/watch?v=eGYLxyLh8d8>>.

Bachmann, G and Kremer, T, Deutscher Corporate Governance Kodex (DCGK), Compliance Management System, Whistleblowing, 2021, 8. ed., Rn. 16 – 31.

Basar, E and Hiéramente, M, Datenbeschlagnahme in Wirtschaftsstrafverfahren und die Frage der Datenlöschung, NStZ, 2018, P. 681 – 687.

Bittmann, F, Brockhaus, M, von Coelln, S and Heuking, C, Regelungsbedürftige Materien in einem zukünftigen „Gesetz über interne Ermittlungen“, NZWiSt, 2019, P. 1 e seg.

Deiseroth, D and Derleder, P, Whistleblower und Denunziatoren, ZRP, 2008, P. 248 – 251.

Dilling, J, Der Schutz von Hinweisgebern und betroffenen Personen nach der EU-Whistleblower-Richtlinie, CCZ, 2019, P. 214 – 224.

Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho de 23 de outubro de 2019 relativa à proteção das pessoas e terceiros, que denunciam violações do direito da União, <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L1937&from=en>>.

Dzida, B, Neue datenschutzrechtliche Herausforderungen für das Personalmanagement, BB, 2019, P. 3060.

Dzida, B, NZA Editorial 23/2012 (cit.: Dzida/ Granetzny).

Dzida, B and Granetzny, T, Die neue EU-Whistleblowing-Richtlinie und ihre Auswirkungen auf Unternehmen, 2020, P. 1201 – 1207.

faz.net, Chelsea Manning aus Haft entlassen, <<https://www.faz.net/aktuell/politik/ausland/whistleblowerin-chelsea-manning-aus-haft-entlassen-15020248.html>>.

Garden, F and Hiéramente, M, Die neue Whistleblowing-Richtlinie der EU - Handlungsbedarf für Unternehmen und Gesetzgeber, BB, 2019, P. 963 – 965.

Granetzny, T and Krause, M, Was kostet ein gutes Gewissen? – Förderung von Whistleblowing durch Prämien nach US-Vorbild?, CCZ, 2020, P. 29 – 36.

Heinrich, Wistra, 2017, P. 219 - 223 (cit.: Dilling).

Hommel, U, Die Zusammenarbeit mit Whistleblowern – Anmerkungen zu der EU-Whistleblower-Richtlinie, CCZ, 2021, Rn. 95-97.

Kremer, T, Compliance-Programm in Industriekonzernen, ZGR, 2010, 113 e seg.

Mahnhold, T, “Global Whistle” oder “deutsche Pfeife” – Whistleblower-Systeme im Jurisdiktionskonflikt, NZA, 2008.

Milieu Ltd/ Fernandes, Meena/ McGuinn, Jennifer/ Rossi, Ludovica

Estimating the economic benefits of whistleblower protection in public procurement, 2017,

<https://op.europa.eu/pt/search-results?p_p_id=eu_europa_publications_portlet_search_executor_SearchExecutorPortlet_INSTANCE_q8EzsBteHybf&p_p_lifecycle=1&p_p_state=normal&queryText=Estimating+the+economic+benefits+of+whistleblower+protection+in+public+procurement+:+final+report.&facet.collection=EULex,EUPub,EUDir,EUWebPage,EUSummariesOfLegislation&startRow=1&resultsPerPage=10&SEARCH_TYPE=SIMPLE>.

Peters, A-K, Anwesenheitsrechte bei der Durchsicht gem. § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme, NZWiSt, 2017, P. 465.

Resolution 2300, 2019, Improving the protection of whistleblowers all over Europe, <<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=28150>>.

Schmolke, U, Die neue Whistleblower-Richtlinie ist da! Und nun? Zur Umsetzung der EU-Richtlinie zum Schutz von Hinweisgeber in das deutsche Recht, NZG, 2020, P. 5 – 12.

spiegel.de, US-Bundesgericht: Von Snowden enthülltes Überwachungsprogramm war illegal, <<https://www.spiegel.de/netzwelt/netzpolitik/edward-snowden-enthueelltes-ueberwachungsprogramm-war-illegal-a-1e08c392-aec9-4149-94f1-cd8a6ad535fb>>.

Süddeutsche-Zeitung, “Nicht-Zuständig”: Zeuge kritisiert Behörden, <<https://www.sueddeutsche.de/bayern/ekelfleisch-prozess-nicht-zustaendig-zeuge-kritisiert-behoerden-1.1099136>>.

tagesschau.de, Ausbreitung des Corona-Virus: Kritik an chinesischen Behörden, <<https://www.tagesschau.de/thema/coronavirus/>, acessado pela última vez em 20 de maio de 2021>.

U.S. Dep’t Justice, Criminal Div., Evaluation of Corporate Compliance Programs, 2020, <<https://www.justice.gov/criminal-fraud/page/file/937501/download>>.

Vitorino Clarindo dos Santos, J, Rechtsfragen der Compliance in der Internationalen Unternehmensgruppe, Lohmar, 2013, p. 58.

Vitorino Clarindo dos Santos, J, Internal investigations, ICRio, 2020: <<https://youtu.be/j8fAUKlzhU>>.

Vogel, J-P and Poth, C, CB, 2019, P. 45 e seguintes (cit.: Dilling).

Wiedmann, M and Seyfert, S, Richtlinienentwurf der EU-Kommission zum Whistleblowing, CCZ, 2019, P. 12 – 21.

Whistleblowing Report 2019, <<https://whistleblowingreport.eqs.com>>.

Xylander, K-J, Kiefner, A and Bahlinger, S, Durchsuchung und Beschlagnahme in der Sphäre des Unternehmensanwalts im Zuge von internen Ermittlungen, BB, 2018, P. 2953.