UiO : Faculty of Law
University of Oslo

# Reconciling the protection of whistleblowers with the right to data protection

An assessment of how European legislation allows for reconciliation between the protection of whistleblowers and the right to data protection in the context of internal whistleblowing systems.

Candidate number: 9002

Submission deadline: 8th September 2020

Number of words: 14 874

# Table of contents

## Abbreviations

| | |
|---|---|
| CJEU | Court of Justice of the European Union |
| DPA | Data Protection Authority |
| DPD | Directive 95/46/EC (Data Protection Directive) |
| EDPB | European Data Protection Board |
| EDPS | European Data Protection Supervisor |
| EDPS Guidelines | EDPS Guidelines on processing personal information within a whistleblowing procedure (2019) |
| EUDPR | Regulation 2018/1725 |
| EUIS | EU Institutions and Bodies |
| GDPR | Regulation 2016/679 |
| WBD | Directive 2019/1937 (Whistleblower Directive) |
| WP29 | Article 29 Working Party |
| WP29 Opinion | Opinion 1/2006 of the WP29 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. |

# 1. Introduction

The past years have witnessed important changes in various parts of society. In democratic societies, societal changes happen through the adoption of new laws and new awareness raising in the population. Such developments are often the result of civil movements[1] or major disruptive events. [2] Sometimes, changes are the consequence of light shed on serious wrongdoings affecting the public interest. Illegal or unethical behaviors are happening within both public and private entities. Recent cases show that a large range of fields are involved, including the pharmaceutical industry, [3] social media[4] or State surveillance. [5]

Persons who expose secretive information or activities within a private or public organization that is deemed illegal or unethical are whistleblowers.[6] At EU level, whistleblowers have been recognized as essential to safeguard the welfare of a society and to enhance the enforcement of law. [7] Illegal and unethical actions in work-related contexts are also a serious problem for companies.

---

[1] Ellen Messer-Davidow, "Disciplining feminism: from social activism to academic discourse." Duke University Press (Durham, North Carolina, 2002).

[2] Gautam Mukunda, "The social and political costs of the financial crisis, 10 years later." Harvard Business Review, (25th September 2018) < https://hbr.org/2018/09/the-social-and-political-costs-of-the-financial-crisis-10-years-later> Accessed 31st August 2020.

[3] Ana Popovich, "Exposing the Pharmaceuticals Industry: Insights From A Novartis Whistleblower" Front Line Whistleblower News (July 28, 2020) <https://www.whistleblowersblog.org/2020/07/articles/false-claims-qui-tam/exposing-the-pharmaceuticals-industry-insights-from-a-novartis-whistleblower/ >Accessed 31st July 2020.

[4] Clint Watts, "Inside the unscrupulous world of social-media manipulation with a penitent whistleblower" The Washington Post (October 11th 2019) <https://www.washingtonpost.com/outlook/inside-the-unscrupulous-world-of-social-media-manipulation-with-a-penitent-whistleblower/2019/10/11/eb357dd4-eb06-11e9-9306-47cb0324fd44_story.html> Accessed 31st July 2020.

[5] Ewen MacAskill and Gabriel Dance, "NSA files decoded: What the revelations mean for you" The Guardian (November 1st 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> Accessed 31st July 2020.

[6] Wim Vandekerckhove, "*Whistleblowing and organizational social responsibility: a global assessment.*" (Ashgate Publishing Co. 2007).

[7] The EU repeatedly stated it through Commissions proposals and Council declarations, before agreeing on an EU legislation on the topic: the new WBD (see recital 1 and 2).

Getting information about violations of legal or internal corporate rules and values is essential for them to be able to prevent and detect them.[8] However, potential whistleblowers are often discouraged from reporting their concerns or suspicions for fear of retaliation.[9] That is why it has become of growing importance to ensure an effective protection of whistleblowers. One way to protect whistleblowers and encourage them to contribute to society is providing them with safe channels to report alleged wrongdoings, so-called reporting schemes.

## 1.1. Whistleblowing explained

### 1.1.1. The wide definition of whistleblowing

The term "whistleblowing" has been defined and used in multiple ways. In the context of sensational journalism, it often refers to the act of exposing alleged misdeeds, regardless of their nature.[10] Similarly, the legal definition varies according to jurisdictions. Many do not provide a specific definition, but in most cases, the notion will cover individuals who disclose information that they believe is true, on defined matters and to an appropriate authority. [11] This also means that not all concerns raised among employees are meant to be reported through whistleblowing schemes. On this account, there should be an additional mechanism to be put in place for staff or other informants to report a specific category of unethical or unlawful activities. At EU level, both the WP29 advisory body[12] and EU legislator[13] have stated that whistleblowing should be viewed as subsidiary to, and not a replacement for, internal management.

[8] EQS Report on Whistleblowing (2019), p.6.

[9] Recital 1 WBD.

[10] Peter B. Jubb, "*Whistleblowing: A Restrictive Definition and Interpretation*." Journal of Business Ethics 21, no. 1 (1999).

[11] See, eg, Labour Code & Anti-Discrimination Act (Czech Republic), Legislative Decree 231/2001, amended by Law No 179/2017 (Italy), the Netherlands' House for Whistleblowers 2016 Act (Wet Huis voor klokkenluiders) and the Sarbanes–Oxley Act (US). Retrieved from <https://www.dlapiper.com/en/us/insights/publications/2015/06/whistleblowing-law-2015>. Accessed 6th September 2020.

[12] WP29 Opinion p.6.

[13] Recital 22 WBD.

The scope of what is reportable normally varies depending on the applicable legal obligations and limitations set by data protection rules. This aspect will be further developed under sub-chapter 3.1 when addressing the lawfulness of whistleblowing schemes.

### 1.1.2. Internal reporting, external reporting and public disclosures

There are three main types of reporting: internal reporting, external reporting and public disclosures. Internal reporting is the oral or written communication of information on specific violations within a legal entity in the private or public sector. Empirical studies show that most of the time, whistleblowers do tend to report internally, i.e. within the organization they work.[14] External reporting is the oral or written communication of information on alleged misconducts to the competent national authority. When the whistleblower decides to make the information on breaches directly available in the public domain, we talk about public disclosure.[15] The terminology used to describe channels that enable whistleblowing varies significantly: reporting channels,[16] whistleblowing procedures,[17] or reporting systems.[18] For the purpose of clarity, in this thesis, *channels* describe any means allowing information on breaches to be communicated. This includes postal letters, e-mails, hotlines, external ombudsmen or digital solutions. *Scheme* covers both the channels and the procedures enabling individuals to report information on breaches. This thesis will primarily discuss internal reporting schemes.

## 1.2. Scope and subject matter of the thesis

Internal reporting schemes have gained great interest in the recent years. On one hand, many companies have recognized that whistleblowing is beneficial to them as they help to identify misconduct at an early stage and avoid sanctions, fines and reputational damage.[19]

[14] Recital 33 WBD.
[15] Article 5 WBD.
[16] Article 7 WBD.
[17] EDPS Guidelines (2019), p.4.
[18] WP29 Opinion, p.8.
[19] EQS Whistleblowing Report (2019), p.4.

On the other hand and following the Cambridge Analytica and Panama Papers scandals - that were revealed by whistleblowers - the European Commission set out a proposal on an effective EU protection of persons who disclose information on wrongdoing in the workplace affecting the public interest.[20] This led to the adoption of a Directive on the protection of persons reporting breaches of EU Law (Whistleblower Directive or "**WBD**")[21] that entered into force in December 2019.

This new instrument aims to ensure a comprehensive and coherent whistleblower protection at EU level. Some EU laws regulating whistleblowing already exist, however only in high-risk sectors (such as the financial sector, protection of the environment, transport safety, and nuclear safety).[22] At national level, most of the Member State have not or only to some extent adopted specific whistleblower protection laws and obligations to establish reporting schemes.[23] *De facto*, this lack of strong policies contributed to an overall European legislation that is not particularly supportive of whistleblowing. In this setting, the EU legislator adopted the WBD, instrument aiming to add to and strengthen the enforcement of existing legal dispositions. For this purpose, the WBD introduces several novelties and minimum standards. These include mandatory reporting schemes for all private legal entities with 50 or more employees.[24] Member States can include smaller entities if operating in sensitive areas.[25]

[20] See the proposal for a Directive of the European Parliament and of the council on the protection of persons reporting on breaches of Union law (23rd April 2018).

[21] 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, OJ L 305.

[22] See Annex 5 of the WBD for the an overview of EU-legislation in the field, <https://ec.europa.eu/info/sites/info/files/1-11_annexes.pdf>.

[23] France's Loi Sapin 2, the Netherland's House for Whistleblowers Act and Italy's Law on Whistleblowing. See Annex 6 for an overview of the protection and the various obligations to set up reporting channels decided on Member State's level. <https://ec.europa.eu/info/sites/info/files/1-11_annexes.pdf>.

[24] Art. 8(3) WBD.

[25] Art. 8(7) WBD.

However, the general whistleblower protection introduced by the WBD is limited to whistleblowers reporting on breaches of EU law. Breaches are defined as acts or omissions that are unlawful and relate the Union acts and areas falling within the material scope of the WBD.

Notwithstanding, many EU companies will soon need to comply with the obligations deriving from the WBD and especially with the need to implement whistleblowing schemes. In addition, companies operating in the EU also need to comply with EU data protection rules.

Thus, companies need to ensure that the reporting channels they establish are in compliance with EU data protection law.

## 1.3. Research questions

More and more companies realize that internal reporting schemes are beneficial for them. In addition, an increasing number of companies will have a legal obligation to establish reporting schemes. However, considerations relating to data protection and privacy laws are likely to impose some limitations on the way these schemes are set up. This thesis seeks to address how internal reporting schemes should be set up to comply with EU data protection rules.

The central research question is: "How does EU law reconcile the protection of whistleblowers with the protection of personal data?"

To answer the main question, the following sub-questions have been formulated:

- How should companies design and establish reporting schemes in compliance with data protection law requirements?
- How should companies operate reporting schemes to ensure the protection of data subject's rights?

## 1.4. Methodology and sources

Most sources of this thesis are written in English language. Some national laws from EU Member States were also consulted. These were accessed in their original language: essentially Italian, French, German and Spanish. Where translations were needed, these were obtained either using Google Translate, through translations offered by the relevant governmental websites or through analyses in English of national laws published the websites of various law firms.

Legal sources are primary and secondary legislation of the EU, as well as guidelines and opinions of EU advisory bodies. Non-legal sources are legal scholarship and opinions of compliance experts. There is a significant amount of works addressing legal issues around whistleblowing, as well as many works addressing legal issues around the processing of personal data. Yet, there are not so many works covering the application of personal data protection rules to whistleblowing schemes. This is even less the case for works taking into consideration the newly established EU rules on data protection and whistleblowing. However, two EU documents provide some guidance: both the Article 29 Working Party ("**WP29**") and the European Data Protection Supervisor ("**EDPS**") have published documents in the form of practical checklists on the data protection challenges in the implementation of reporting schemes.

The first document is Opinion 1/2006 of the Article 29 Working Party ("**WP29 Opinion**").[26] It was published in the aftermath of the U.S. Sarbanes-Oxley law of 2002 (so-called SOX-act), which required stock-listed companies in the U.S. to set up internal whistleblowing systems. This obligation extended to both their national and foreign subsidiaries, which led to many EU companies rapidly implementing such schemes.

[26] Opinion 1/2006 on the application of EU data protection rules to internal WB schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crimes.

The WP29 Opinion was intended to meet the need for harmonized guidelines on the applicability of data protection rules to these schemes. Data protection rules in the EU were at the time regulated by the old Data Protection Directive 95/46/EC ("**DPD**"), which has been replaced by the General Data Protection Regulation 2016/679 ("**GDPR**")[27]. Simultaneously, the WP29 has been replaced by the EDPB,[28] which has neither expressly endorsed the WP29 Opinion nor adopted a new one on the topic. Thus, to the exception of some guidance issued on the national level[29], most EU established private sector operators do not have any GDPR- updated guidance.

The second document is the Guidelines on processing personal information within a whistleblower procedure issued by the EDPS in December 2019 ("**EDPS Guidelines**"). The EDPS is the EU's independent data protection authority. As such, the guidelines, based on the Regulation 2018/1725 ("**EUDPR**")[30], are aimed towards EU institutions and bodies ("**EUIs**"). However, the Data Protection Framework applicable to EUIs and the one applicable to legal entities of the private sector is very similar.[31] Therefore, analogies will be drawn from the recommendations issued by the EDPS when analyzing how legal entities of the private sector can lawfully process personal data in reporting schemes.

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

[28] EU body in charge of contributing to the consistent application of data protection rules throughout the EU.

[29] See for instance "Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz" of the German DPA (14th November 2018), and the "Standard on processing personal data for the purpose of whistleblowing" of the French DPA CNIL (18th July 2019).

[30] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[31] The rules and principles contained in the EUDPR-Regulation 2018/1725 mirrors those of the GDPR.

It is worth mentioning that such documents do not feature among the sources of EU law and are therefore limited to the provision of non-binding opinions and guidelines. However, these are often more detailed and therefore crucial when it comes to interpreting EU law provisions. They also guide controllers on how to apply data protection norms in the specific field of reporting schemes. Thereby, they ultimately contribute to a safer legal environment within the EU to safeguard citizen's fundamental right to data protection.

The WP29 Opinion is old and does not cover GDPR-related novelties, but it considers questions rising in the private sector. The EDPS is aimed for EUIs, but it considers the GDPR. In this setting, these documents constitute the main source of inspiration for the structure of this thesis.

## 1.5. Structure of the thesis

Chapter 1 will set out the legal landscape in which reporting schemes are placed. This entails a review of the material scope of the instruments, in addition to what the interplay between the GDPR and the WBD means in the context of reporting schemes. This is imperative to understand the link between data protection rules and obligations relating to whistleblower protection.

Chapter 3 will elaborate on the data protection principles that govern the establishment of reporting schemes. This chapter will assess the practical implications for controllers.

Chapter 4 will explore the data subject's rights in the context of reporting schemes. The particularity of reporting schemes requires a balance to be struck between the rights of the whistleblower and the alleged wrongdoer. Some rights can also be tricky to satisfy when incompatible with the aim of reporting schemes. The relevance of exploring these is to provide with sufficient reflection and weighed arguments to constitute helpful guidance for entities establishing reporting schemes.

Chapter 5 will summarize the findings of this paper, reflecting on whether EU law on data protection and whistleblowing ensures a fair balance to be struck between data subject's rights within a reporting scheme.

# 2. Legal Background

While the newly adopted WBD establishes the EU rules on reporting schemes, it is the GDPR that regulates the processing of personal data. As stated by the EDPS, data protection principles can ultimately be used to strengthen the whistleblowing procedures.[32]

## 2.1. The EU legislation on whistleblowing

After more than two years of legislative process, the Whistleblowing Directive entered into force in December 2020. Member States have two years to implement it into their national laws.

Today, whistleblowers still rely on piecemeal rights found in employment, anti-corruption and criminal laws. Through the adoption of the WBD, the EU legislator hopes to achieve a less fragmented and more cooperative protection of whistleblower across the EU.[33] The objectives include ensuring confidential reporting[34] and protecting whistleblowers against retaliation.[35]

### 2.1.1. A general obligation to establish internal reporting schemes

The WBD aims to ensure that breaches of EU law may be reported, [36] but it also allows Member States to impose the establishment of reporting schemes for other breaches.[37] Accordingly, Member States must ensure that their national legislation mandates the establishment of internal confidential and safe reporting schemes in legal entities of both the private and public sector.[38]

In the private sector, the obligation applies to companies with 50 or more workers.[39] Member States are free to extend the obligation to smaller companies operating in high-risk fields, such as public health or the environment.[40]

[32] 2019 EDPS Guidelines, p. 4.
[33] Art. 1 WBD.
[34] Art. 16 WBD.
[35] Art. 19 WBD.
[36] Art. 8(2) WBD.
[37] Art. 2(2) WBD.
[38] Art. 8(1) WBD.
[39] Article 8(3) WBD.
[40] Article 8(7) WBD.

In the public sector, the obligation applies to all legal entities, with a possible exemption for municipalities with under 10 000 inhabitants.[41] Member States are also free to allow the outsourcing of the internal reporting schemes to third parties.[42]

### 2.1.2. A protection limited to whistleblowers reporting on breaches of EU law

The protection enshrined in the WBD is large as it aims to protect the whistleblowers' right to freedom of expression[43] while safeguarding whistleblowers against retaliation, dismissal and long-lasting proceedings.[44] However, it does not cover all matters that can be reported through reporting schemes but is limited to individuals reporting on breaches of EU law. As such, the material scope of protection applies to individuals making reports on, among others, breaches relating to the protection of the environment, public health, nuclear safety, or the protection of privacy and security of networks and IT systems.

These are typically fields where breaches could cause serious harm to the public interest and where enforcing EU law is facilitated by the help of whistleblowers.[45] However, this list is non-exhaustive because the WBD is without prejudice to the power of Member States to maintain or extend the protection of individuals reporting misconduct in other areas.[46] The text aims to set EU-wide *minimum* standards. Thereby, national laws still can be more favorable to whistleblowers.[47] When transposing the WBD, Member States are free to add categories of breaches triggering whistleblower protection that goes beyond EU-law breaches.

[41] Article 8(9) WBD.

[42] Article 8(5) WBD.

[43] See Recital 31 and 45 WBD.

[44] Art. 21 WBD.

[45] M. Krook, M.G. Madsen, T. Brautigam, K. Vesa, A. Lange, *An overview of the Whistleblowing Directive in the Nordics*, Bird&Bird (August 2020). < https://www.twobirds.com/en/news/articles/2020/global/an-overview-of-the-implementation-of-the-whistleblowing-directive-in-the-nordics> Accessed 1st September 2020.

[46] Article 2(2) WBD.

[47] Article 2 WBD.

The WBD also extends the scope of protection to anyone who has become aware of breaches in a work-related context. This includes employees, but also ex-employees, third-party or freelance workers, as well as trainees. The status of the whistleblower, from an employment-law perspective, becomes irrelevant.

However, the whistleblower must fulfill two complementary conditions to be granted protection when using internal reporting schemes: having had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that the breach falls within the scope of the Directive.[48] That is why using an internal reporting scheme to report misconduct of another nature (given that it is not covered by national law) prohibits whistleblowing protection as set out in the WBD.

## 2.2. The EU Data Protection Legal Framework and internal reporting schemes

The General Data Protection Regulation 2016/679, replacing Directive 95/46/EC and applicable since May 2018, is the main EU legislative instrument on personal data protection. While introducing new and clarified dispositions, there is no revolution contained in the GDPR when it comes to data protection principles. The main reason why data protection preoccupations have exponentially grown in businesses are the fines imposed for non-compliance.

The WBD expressly submits all processing of personal data carried out pursuant to it to the GDPR.[49] There is no specific legal disposition regarding the processing of personal data in the context of internal reporting schemes. Hence, legal entities are subject to the GDPR when processing whistleblowing reports to the same extent as they are for any other processing.

The rules enshrined in the GDPR aim to protect individuals from privacy and data breaches in an increasingly data-driven world, while creating a clearer and more consistent framework for businesses.[50] This is especially the case concerning data subject's rights and restrictions.

[48] Article 6 WBD.

[49] Art. 17 WBD.

[50] Udo Bux, "Personal Data Protection", Fact Sheets on the EU (January 2020). <https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection> Accessed 2nd August 2020

The GDPR enshrines the protection of natural (living)[51] persons in situations where their personal data is being processed. It therefore applies when there is a "processing" of "personal data" and when such processing is intended to be part of a filing system. The said system can be either electronic or manual and need only a simple structure to be considered as such.[52]

The text provides a wide definition of "personal data". The notion covers any information that relates to a living identified or identifiable person. Thus, if the information alone or in collection with other information can lead to the identification of the person, either directly as an individual or as belonging to a specific group, this information is also considered personal data.[53] Relevant straightforward examples of personal data in the context of reporting schemes are names, nicknames, position in the firm, working hours.[54] Some more arguable examples concern the reports being made by the whistleblower and the communication operated internally in relation to the whistleblowing reports being investigated. Considering the CJEU's wide interpretation of personal data, the balance seems to be in favor for a large encompassing of the notion.

In *Nowak*, the judges stated that "the use of the expression *any information* in the definition of the concept of personal data reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it *relates* to the data subject.[55]" Legal persons are not entitled to the data protection rules enshrined in the GDPR,[56] as reiterated in a recent case of the Austrian Data Protection Authority[57] ("**DPA**"). Reporting a *specific person* in a company will therefore trigger data protection rules in relation to that natural person. Reporting *a company* will not.

---

[51] Recital 27 GDPR.

[52] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st Edition, Springer 2017), p. 11.

[53] WP29 Opinion 1/2007 on the concept of personal data, (2013), p. 13.

[54] C-342/12 *Worten*.

[55] C-434/16 Nowak, para. 34.

[56] Art. 4(1) GDPR.

[57] Decision GZ: 2020-0.191.240, Austrian Data Protection Authority, (25 May 2020).

However, the CJEU has also recognized exceptions in which legal persons can invoke their right to personal data protection, "in so far as the official title of the legal person identifies one or more natural persons".[58]

The concept of "processing" is equally extensive. The notion essentially covers any act carried out on personal data.[59] In the context of reporting schemes, relevant examples of processing are collecting, organizing, storing, using, consulting or destroying personal data.[60]

A controller is someone who determines the purposes and means for processing.[61] Per the WBD, companies are responsible for establishing reporting schemes that allow individuals to report on breaches of EU law[62] and for designating the person competent to receive and follow-up on reports.[63] As such, companies determine the purposes (i.e. exposing breaches of EU law) and the means (i.e. through reporting schemes). Therefore, they fall under the definition of *controller*, deeming them responsible for complying with data protection rules.

This entails both an obligation to process in accordance with data protection principles as well as safeguarding the rights of both the whistleblower and the alleged wrongdoer.

## 3. Data protection in design and establishment of reporting schemes

As a preliminary statement, even though addressed under the title consecrated to data protection in the design and establishment of reporting schemes, the principles analyzed thereunder must be applied all along the functioning of the whistleblowing scheme, and not only when initially established. This paper aims to emphasize the specific requirements linked to ensuring data subject's rights. For this purpose, these principles will be further addressed under Chapter 4 when analyzing how companies can restrict or should pay special attention to them.

[58] See Joined Cases C- 92/ 09 and 93/ 09, *Schecke*, para. 53.
[59] Art. 2(1) GDPR.
[60] Art. 4(2) GDPR.
[61] Art. 4(7) GDPR.
[62] Art. 8(1) WBD.
[63] Art. 9(1)c WBD.

When it comes to processing personal data in internal reporting schemes, there was no specific data protection legislation in the DPD nor is there in the GDPR. Therefore, companies are on their own when it comes to correctly materializing GDPR data protection rules into reporting schemes they wish to establish. The benefits of the application of data protection rules to reporting channels is double. First, it ensures that the individual rights of privacy and data protection are protected and henceforward incentivizes the report of fraudulent behaviors). Simultaneously, it enhances the effectiveness of the reporting channels by reducing the processing to what is strictly necessary to reach the objectives, especially through the purpose limitation, data quality and proportionality principles.

The first step for companies is to assess whether they have a valid legal basis for establishing reporting schemes.

## 3.1. Ensuring the lawfulness of reporting schemes

Just like for all personal data processing-systems, processing as conducted in the context of reporting schemes is only lawful if it finds its legal basis within the exhaustive list of legal bases in Article 6 GDPR.

The particularity of the type of the data circulating in reporting schemes is that they are accusations of misconduct raised against individuals. Consequently, reporting schemes essentially process personal data that has not been obtained from the alleged wrongdoers.

On account of this, the legal bases available for processing are limited. To lawfully set up reporting schemes, companies will predominantly rely either on (1) the fulfillment of a legal obligation to which they are is subject, or (2) the pursuit of a legitimate interest. In the context of reporting schemes established in the working environment, it is also worth mentioning the specific protection of personal data in the context of employment (3). Henceforth, viability of consent from the main data subjects, i.e. the whistleblower and the alleged wrongdoer, will also be analyzed (4), as well as the restrictions on processing special categories of personal data (5).

### 3.1.1. Compliance with a legal obligation

Per Article 6(1)c GDPR, is valid the processing of personal data that is necessary for ensuring compliance with a legal obligation to which the controller is subject. Such a legal obligation can originate both from a mere national law (ex: Chapter 2A of the Arbeidsmiljøloven in Norway), but also from EU law (ex: Art. 8 WBD) or international law (ex: OECD convention on combating bribery) such as implemented in national law. However, the establishment of a reporting scheme should have the purpose of meeting a legal obligation *especially* designed to establish internal control procedures in well-defined areas.[64]

The WBD provides a legal basis for the establishment of reporting channels that is limited to reports on infringements of EU law. Companies can therefore justify the establishment of reporting schemes with their need to comply with a legal obligation, but only to the extent that they are exclusively meant to host reports concerning breaches of EU law. This means that if a company wants to extend the scope of what can be reported and so include matters that are not covered by the WBD dispositions, it will have to rely on another legal basis. In this situation, there are two options. The first is to check whether the national laws they are subject to set out an obligation to establish reporting schemes in the operating sector of the company. In most EU countries, there is a legal obligation to establish internal control procedures in the banking sector, or in the context of combating bribery. This is the first step to extend the scope of what can be reported, and it is ensured by a stable and reliable legal basis.

It is worth mentioning that a foreign national law cannot constitute a legal obligation as defined under the GDPR.[65] The WP29 pointed out that would this be the case, it would make it too easy to circumvent EU data protection rules. This said, even if foreign provisions cannot directly constitute a legal basis, their content can in some situations inspire ground for a legitimate interest pursued by the controller. This constitutes the second legal basis-option.

[64] WP29 Opinion, p.7.
[65] WP29 Opinion, p.8.

### 3.1.2. Legitimate interest of the controller

Processing is also lawful if necessary for the purposes of the legitimate interests pursued by the controller.[66] As an example, several international organizations such as the EU or the OECD have recognized the importance of ensuring good corporate governance principles within companies. In the absence of EU legal obligations on the topic, the WP29 considered that the rules laid down in the Sox-Act effectively contributed to ensuring those good corporate governance principles.[67] This materializes in recital 47 GDPR, explicitly stating that the processing of personal data strictly necessary for the purposes of preventing fraud does constitutes a legitimate interest of the controller concerned.

Nevertheless, legitimate interests only constitute a valid basis if they are not overridden by the interests for fundamental rights and freedoms of the data subject. This means that the controller must strike a balance between the two interests at stake, i.e. the interest of the controller versus the interest of the data subject whose data the controller intends to process. In the context of reporting scheme, companies will have to consider both the whistleblower and the alleged wrongdoer before engaging in any processing operation on their personal data. Such a balancing test involves taking into account the main data protection principles, such as proportionality and subsidiarity.

For the alleged wrongdoer, such test should for instance include the seriousness of the alleged offences that can be notified; for the whistleblower, the test should include the risks for potential retaliation. This work of balancing interests must be performed preliminarily to the establishment of the scheme and be documented.[68] Shortly put, the sole existence of a legitimate interest is not enough to justify the processing of personal data: the key to ensure a reliable legal basis for the establishment of reporting channels is to have struck a solid balance demonstrating that the risks to which individuals are exposed are worth it.

[66] Art. 6(1)f GDPR.
[67] WP29 Opinion, p.9.
[68] Article 12(1) GDPR.

Relying on a legitimate interest also opens the door for the data subjects' right to object.[69] The right to object of the alleged wrongdoer – which seems to be the most likely in the context of reporting schemes - will be further developed in sub-section 4.3.4).

### 3.1.3. The specific protection of personal data in the context of employment

The EU legislator recognized the particularity of processing personal data in the context of an employment relationship between the controller and the data subject. However, the topic remains unharmonized, as the GDPR defers to the Member States the option to operate potentially needed adjustments.[70] This means that Member States may lay down more specific rules when personal data is processed with the purposes of the performance of the contract of employment, including compliance with obligations set by law or by collective agreements, equality and diversity in the workplace or health and safety at work. These rules must however include appropriate measures to preserve among others, human dignity, as well as the legitimate interests and rights of the data subject.[71] Initially, the second proposal for the GDPR authorized Member States to fix the conditions under which personal data relating to employment can be processed on the preliminary consent of the employee. This provision has been deleted, knowing that the WP29 denies that the consent of an employee can be considered as explicitly and freely expressed within the framework of an employment contract characterized by the link of subordination.[72]

On the other hand, some EU countries labor laws implicitly prohibit the establishment of whistleblowing schemes. This is the case in Finland for example, where the only way employers can collect personal data concerning their employees, is directly from them. Other sources are only lawful to the extent that they are collected with the concerned employee's consent.[73] In this type of legal framework, unless they rely on a legal obligation providing for exceptions to this Finnish law, companies will most likely not be able to lawfully set up reporting schemes.

[69] Article 21(1) GDPR.
[70] Article 88 GDPR.
[71] Ibid.
[72] Opinion 15/2011 of 13 July 2011 on the definition of consent, p. 15.
[73] Finnish Act on the Protection of Privacy in Working Life (759/2004).

Notwithstanding, establishing reporting schemes in a work-related environment raises the question of the particularity of consent of the data subjects as a legal basis for processing.

### 3.1.4. Consent as a limited valid ground for processing

Although there may be a strong presumption that consent is weak in the employment context, this does not completely exclude its use, provided there are sufficient guarantees that consent is really free.[74] Consent will first be thoroughly analyzed in regard to the whistleblower, and then shortly in regard to the alleged wrongdoer.

For entities beyond authorized staff member, the WBD submits disclosure of information concerning the whistleblower to his explicit consent.[75] Thereby, the WBD acknowledges consent of the whistleblower as a valid legal basis to reveal his identity or other information from which identity can be deducted.[76] This might create a tension with the established WP29 recommendations to generally not recognize consent when given in a work-related environment because employees are *almost* never in a position to freely give, refuse or revoke consent.[77]

Interestingly, the WBD's reasoning behind the need of specific whistleblower protection also seems to weigh in favor for excluding consent obtained in the work-context. Indeed, according to the WBD, the underlying reason for providing whistleblowers with protection is their position of economic vulnerability vis-à-vis the person on whom *de facto* they depend for work.[78] This very imbalance is the reason why the WP29 generally excluded the possibility of a free consent. Notwithstanding, there are some elements that might reduce the imbalance of powers between the employer and the employee. This could for instance be the case where the report does not incriminate the high hierarchy, i.e. does not involve a misconduct of the employer.

[74] WP29 Opinion 15/2011 on the definition of consent, p.14.
[75] Art. 16 WBD.
[76] Ibid.
[77] WP29 Opinion 2/2017 on data processing at work, p.23.
[78] Recital 36 WBD.

As such, if the imbalance is not materialized in the context of reporting schemes, consent might be considered as lawful, even if given in a work-related context.[79]

Admitting consent of the whistleblower as legal basis for processing the whistleblowing report creates other difficulties. If companies accept that the initial processing of the data submitted by the whistleblower is based on the whistleblower's consent, they also risk consent to be withdrawn at any time.[80] In that situation, the company will have no other choice to stop processing the relevant whistleblowing case. Notwithstanding, there are situations where companies could try to invoke their legitimate interest to continue the processing of personal data. It is worth reminding that normally, legal bases cannot be switched along the processing operation.[81] However, if the information received would give ground to legal claims, the company could proceed its processing at the condition to demonstrate new purposes and justify a new processing operation.[82] A trickier solution would be to try and differentiate between the data relating to the whistleblower and the content of the report the whistleblower submitted, and as such, consider that the report is not information relating to the whistleblower anymore.

If the issue on consent of the whistleblower is not clearly settled yet, consent of the alleged wrongdoer is clearly excluded. Given the imbalance of power and relationship of dependency between an employer and the employees, consent is only admitted in exceptional circumstances: when it will have no adverse consequences at all whether or not they give consent. [83] In the context of reporting schemes, the processing that requires consent from the data subject concerns information on alleged wrongdoing attributed to him.

[79] WP29 Opinion 2/2017 on data processing at work, p.23.
[80] Article 7(3) GDPR.
[81] WP29 Opinion 15/2011 on the definition of consent. See also PWC v the Hellenic DPA: Entities that misled individuals in this way are found to act in contravention to EU law and fined by DPAs.
[82] "If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis, which better reflects the situation." See EDPB Guidelines on Consent (2020), para. 58, p.14.
[83] WP29 Guidelines on consent under Regulation 2016/679 (28th November 2017), p.7.

Consenting or not to this type of processing undoubtedly involves adverse consequences for the said employee[84]. As such, companies will very hardly be able to demonstrate that they fulfill the criteria for a valid consent.

The author is of the opinion that systematically excluding consent as a lawful legal basis in any processing operation taking place within reporting schemes would be the best safeguard to avoid situations in which (1) the alleged wrongdoer could be coerced to agree and as such, free the controller from his obligation to demonstrate of a legitimate interest that is not overridden by the rights and freedoms of the alleged wrongdoer and (2) whistleblowers will feel pressured into taking decisions they do not wish or do not wish anymore.

### 3.1.5. Restricting the processing of special categories of data

Under the GDPR, legal obligations and legitimate interests are only valid for processing of a limited scope of personal data[85]. Indeed, the text differentiates between generic personal data and special categories of personal data.

Special categories of personal data are information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs or trade union membership, such as data concerning health or data concerning an individual's sex life or orientation.[86]

Processing such data is as a rule prohibited.[87] However, situations could emerge in which reports will need to include information that is categorized as special categories of personal data.

This can for example be the case in reports on suspicion of corruption, where a political belief will potentially need to be mentioned, or on suspicion of fraud in the field of public health, where a health condition will potentially need be disclosed. These special scenarios must be apprehended by companies, especially when it comes to demonstrating the legal basis they use for processing said personal data.

[84] Ibid.
[85] Art. 6 GDPR.
[86] Art. 9(1) GDPR.
[87] Ibid.

Processing special categories of data is only lawful in specific situations exhaustively listed in the GDPR.[88] These include, the explicit consent of the data subject,[89] the protection of the vital interests of the data subject,[90] legitimate activities of non-profit bodies,[91] or when necessary for the establishment, exercise or defense of legal claims.[92]

In the context of reporting schemes, companies might receive and investigate (i.e. process) reports mentioning special categories of personal data relating to the whistleblower or the alleged wrongdoer, or both. Companies will need to have and justify the legal basis used for each distinct processing. Thus, the legal basis for processing of special data relating to the whistleblower might differ than the one used for the alleged wrongdoer.

Concerning the whistleblower, explicit consent can be admitted if given for specific purposes – notwithstanding the reserves on the possibility of a valid consent in an employment relationship as analyzed in subchapter 3.1.4.

Concerning the alleged wrongdoer, the available legal bases are reduced. Controllers will need to justify of reasons of substantial public interest or public interest in the field of public health if provided for by national or Union law[93]or justify that the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorized by national or Union law.[94] Companies wishing to archive received special categories of data might only do so they demonstrate that it is in the public's interest on the basis of national or Union law and if they implement appropriate safeguards.[95] Thus, companies can only process special data related to the alleged wrongdoer in so far as it is authorized in Union or national legislation.

[88] Article 9(2) GDPR.
[89] Article 9(2)a GDPR.
[90] Article 9(2)c GDPR
[91] Article 9(2)d GDPR.
[92] Article 9(2)f GDPR.
[93] Article 9(2)g and i GDPR.
[94] Article 9(2)b GDPR.
[95] Article 9(2)j GDPR.

However as stated earlier, most Member States today do not have specific obligations to set up reporting schemes in the private sector. This leaves companies without any clear available legal basis to lawfully establish reporting schemes that might host special categories of personal data.

On EU-level, the WBD sets out that personal data which is manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.[96] This also means that personal data that *is* relevant for the whistleblowing case *can* be processed. However, the wording is not clear on whether it covers both generic and special data. As such, depending on how Member States will implement the new WBD, companies might be able to derive an employment law or public interest obligation from it – and as such, provide companies with a lawful basis for processing of sensitive data.

When it comes to advisory bodies, the WP29 Opinion does not mention or consider the legal basis for processing special data. The EDPS Guidelines equally provide limited guidance: they merely recommend to avoid the processing of excessive personal data and to set up policies reminding employees that they can only report sensitive information if relevant to the case.[97] That being so, the EDPS acknowledges that there might be special categories of data circulating on reporting schemes, without addressing how to solve it from a lawful legal basis point of view.

[96] Article 17 WBD.

[97] EDPS 2019 Guidelines p. 6 para. 13 and 15.

## 3.2. Ensuring transparency, fairness and accountability of reporting schemes

Transparency became[98] an overarching obligation under the GDPR. [99] Per se, transparency supplements fairness of processing and accountability of the controller.[100] Requirements deriving from transparency apply irrespective of the legal basis for processing and throughout the life cycle of a processing operation.[101] In the context of the establishment of reporting schemes, transparency mainly means providing clear and complete information on the scheme to all potential data subjects. This subchapter aims to clarify what transparency entails *in practice.*

### 3.2.1. Documenting the internal policies on reporting schemes

Transparency means that companies must inform all potential data subjects about the existence, the purpose and functioning of the reporting scheme.[102] Transparency must also be demonstrated, which means that controllers not only must comply with data protection rules but be able to *demonstrate* that they actually do so. As such, transparency always come in pair with accountability.[103]

The first step is therefore to adopt an internal whistleblowing policy. This includes setting out an extensive description of the procedure, e.g, how reporting can be done, who will be receiving the reports and who will investigate. It is not clear what level of detail is required, but in light of the GDPR's purposes and the risks involved in processing this type of sensitive data, the information obligations are likely to be stringent in this context.[104]

[98] The old DPD did not expressly refer to the notion of transparency.

[99] WP29 Guidelines on transparency under Regulation 2016/679 (2018), p.4.

[100] Art.5(1)a and Art.5(2) GDPR.

[101] WP29 Guidelines on transparency under Regulation 2016/679 (2018), p.6.

[102] Art. 12(1) GDPR.

[103] Art. 5(2) and Art.24 GDPR.

[104] Luca Tosoni, "Whistleblowing e GDPR: punti critici e scenari futuri" Network Digital 360, (13th January 2020) <https://www.agendadigitale.eu/sicurezza/privacy/whistleblowing-e-gdpr-punti-critici-e-scenari-futuri/> Accessed 20th July 2020.

In this regard, the WBD sets out the obligation to designate an impartial person or unit within the company for receiving and following-up on reports.[105] However, the WBD does not specify the model according to which reporting schemes should be established: it allows reporting in writing, orally or both.[106] Nonetheless, reporting by means of a physical meeting should be an available option for the prospective whistleblower.[107]

The second step is to document all policies, internal rules or decisions that have been made on the topic.[108]

The third step is to make those easily accessible and make their employees aware of them. Companies cannot assume that their employees or other related individuals can know about the existence nor the functioning of the scheme.[109] The EDPS recommends that information on reporting schemes should be established following a two-step procedure.[110] While making the whistleblowing policy available on an easily accessible platform (e.g. the company's webpage) is encouraged, it is not sufficient to comply with the information obligation of the controller because the said information might be overlooked.[111] As such and in addition, controllers need to create and directly communicate individual notices to all relevant data subjects (i.e. the individuals concerned by a whistleblowing procedure).[112]

[105] Art. 9(1)c WBD.

[106] Art.9(2) WBD.

[107] Art.9(2) WBD.

[108] See recommendations issued in light of the principles of transparency and accountability by Caroline Joly in the webinar: *Loi Sapin 2: Avez-vous mis en place un dispositif d'alertes professionnelles efficace et conforme ?,* organized by EQS Group (21st June 2018), <https://www.eqs.com/fr/ressources-compliance/loi-sapin-2/> Accessed 10th June 2020.

[109] Art. 12(1) GDPR.

[110] EDPS Guidelines (2019), p.7.

[111] Ibid, p.8.

[112] Ibid.

In parallel, companies must keep in mind that the quality, accessibility and comprehensibility of the information is also important (i.e.fairness).[113] Therefore, communication between the controller and the data subject should be concise, intelligible and easily accessible. This can be achieved by using clear and plain language.[114]

It is worth mentioning that even where reporting schemes are clearly established, internal whistleblowing reports can still emerge from various sources (e.g. in the panic of a discovery of misconduct, an employee decides to send a mail to his direct supervisor). Companies should take it into consideration and foresee the consequences of such situations in their whistleblowing policies.

### 3.2.2. Documenting the internal investigation

Transparency also means that companies must document every step of the internal investigation. The document complied for this purpose is subject to the confidentiality requirement[115] and must therefore remain internal (i.e., not freely accessible). Companies must ensure that such document is neutral and objective, providing with a clear description of the facts and measures adopted by the controller, as well as the timeframe.[116]

In this regard, the WBD establishes the obligation to issue an acknowledgment of receipt of the report to the whistleblower within seven days.[117] The company has then maximum three months to provide feedback on the report.[118] As such, the WBD extends the timeframe imposed by the GDPR. Indeed, the GDPR would normally requires controllers to immediately, i.e. "at the time when personal data are obtained"[119] provide the whistleblower with all information relating to the processing of his personal data, i.e. the whistleblowing report submitted by him.

---

[113] WP29 Guidelines on transparency under Regulation 2016/679 (11 April 2018).

[114] Ibid.

[115] Art. 5(1)f, that will be further developed in subchapter 4.1. of this thesis.

[116] See recommendations issued in light of the principles of transparency and accountability by Caroline Joly in the webinar: « Loi Sapin 2: Avez-vous mis en place un dispositif d'alertes professionnelles efficace et conforme ? » EQS Group (21st June 2018)<https://www.eqs.com/fr/ressources-compliance/loi-sapin-2/> Accessed 10th Junes 2020.

[117] Art. 9(1)b WBD.

[118] Art. 9(1)f WBD.

[119] Art. 13(1) GDPR.

Taking into account the complexity of reporting schemes, especially in relation to the information obligation concerning the legal basis for processing and the purposes for processing,[120] this provision of the WBD will most likely not cause a big compatibility issue with the GDPR.

## 3.3. Ensuring purpose limitation and data minimization in reporting schemes

Purpose limitation and data minimization are two very practical data protection principles.[121] Indeed, they require controllers to only process data that is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". As such, companies must first clearly specify the purpose -or the several purposes- of their reporting schemes and second, limit the processing of personal data to these set-out purposes.

### 3.3.1. Setting-out clear circumstances in which reporting schemes must be used

The purposes of the reporting scheme must be specified, explicit and legitimate.[122] Thus, the purposes must be included in whistleblowing policies. It is also worth reminding that potential purposes are limited to what can lawfully be processed with respect to the available legal bases. Accordingly, controllers will also have to specify the legal basis they rely on.[123]

Companies should also break down and demystify the scope of matters that can be reported. A good practice would be for instance to create a typology of reports that can be made. In the context of the WBD, whistleblowing is, a priori, [124] limited to matters of EU law.[125] However, it is highly probable that most employees will not grasp the extent of this scope. On this account, it might be appropriate for companies to make an understandable summary of the matters that are actually covered by EU law, i.e. matters that can be reported. In addition, if a prospective whistleblower is hesitant because he is unclear on whether his report will be covered by the whistleblower protection, it could be a deterring factor.

[120] Art. 13(1)c GDPR.
[121] Art. 5(1)b and c.
[122] WP29 Opinion, p.12.
[123] See subchapter 3.1. on the lawfulness of processing.
[124] Member States can extend reportable matters to matters going beyond EU law, Art.2(2) WBD.
[125] Art.2(1) WBD.

On the other hand, concerns that can be reported through whistleblowing schemes must be limited. To that end, companies must clearly exclude the reporting of a grievance or making a complaint on matters that solely affect the individual making the report.[126]

### 3.3.2. Confine processing to what is strictly necessary

The principle of necessity is widely recognized in EU law. It has also been consecrated in EU data protection law through the CJEU case-law[127] and the GDPR principle of data minimization.[128] Henceforth, necessity is fundamental when assessing the lawfulness of processing operations within a reporting scheme.

In practice, necessity brings restrictions upon the allowed processing operations and categories of data.[129] This means that companies must limit the processing to facts and information related to the set-out purposes. However, applying data minimization to information retrieved from whistleblowing reports will ultimately help controllers reach their goal of having efficient reporting schemes. [130] For instance, immediately destroying and avoiding further processing of data that is irrelevant for the set-out purposes will prohibit the triggering of all the encompassed information rights that would have otherwise needed to be complied with.[131]

## 4. Ensuring data subject's rights in management of reporting schemes

As already stated, the aim of whistleblowing is to expose wrongdoings by providing safe channels for staff or other informants to report unethical or illegal behavior in the workplace. Such procedure requires the processing of sensitive personal information relating to a potentially large scope of individuals, including suspected wrongdoers, whistleblowers, and other parties, such as witnesses.

[126] EDPS Guidelines (2019), p. 4.

[127] See C-524/06 *Huber*.

[128] The GDPR does not provide with a definition of data minimization but explains it in Art. 5(b).

[129] Necessity also influences the storage period, which will be further developed in subchapter 4.3.3.

[130] Or the goal of the applicable legislation, in cases where the reporting scheme is based on a legal obligation.

[131] EDPS Guidelines (2019), p.9.

Due to the specificity of this procedure and risks imposed on the persons involved, the protection of their personal data is of the utmost importance.[132] Chapter 4 will therefore focus on the main difficulties linked to ensuring data subject's rights in the management of reporting schemes. Notwithstanding the importance to ensure the rights of *all* data subjects within a reporting scheme, the analysis in Chapter 4 will be limited to the specificities relating to the whistleblower and the alleged wrongdoer.

As a preliminary statement, it is worth mentioning that ensuring data subject's rights must be followed through the entire processing operation. In the context of reporting schemes, the operation starts with the establishment of reporting schemes and ends with personal data storage or deletion.

## 4.1. The overarching principle of confidentiality of reporting schemes

Confidentiality is a fundamental principle in EU data protection law. The principle already existed under the old DPD,[133] before being further specified under the GDPR,[134] which defines it as the prevention of unauthorized or illegal access to- and use of personal data.[135] Non-respect of the confidentiality requirements in  have also been sanctioned by national DPAs.[136]

In parallel, the most effective way to encourage staff to report concerns is to ensure that their identity will be protected.[137] To that end, confidentiality has also been consecrated in the WBD: controllers establishing reporting schemes have a so-called *duty to confidentiality*.[138] This duty is wide, as it protects from unauthorized disclosure any information from which the identity of the reporting person may be directly or indirectly deduced. Thereby, the WBD adopts the wide EU definition of personal data relating to the whistleblower. Even though the explicit prohibition is

[132] EDPS Guidelines (2016), p.10.
[133] Art. 1 DPD.
[134] Art.5(1)f GDPR.
[135] Recital 39 GDPR.
[136] "Corrective and sanctioning measure against *La Sapienza* University of Rome" of the Italian DPA (23rd January 2020): the University got sentenced to an administrative pecuniary fine for their failure to comply with the security and confidentiality requirements of data management when establishing their internal whistleblowing scheme.
[137] EDPS Guidelines (2019).
[138] Art. 16 WBD.

only directed against disclosure of the identity of the reporting person,[139] the WBD also enshrines the obligation to establish channels that are designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the reporting person *and any third party* mentioned is protected and prevents unauthorized access thereto.[140]

But in in the absence of more precisions on the field, data protection rules are the strongest gatekeeper to data subject's right to confidentiality.[141]

## 4.2. Whistleblowing schemes must be safe to use for the whistleblower

This subchapter aims to analyze what guarantees internal reporting schemes offer to those who use them. One of the main questions that controllers are likely to ask themselves when managing reporting schemes, is to what extent the reporting person (i.e. the whistleblower) is entitled to confidentiality, and whether reporting schemes must grant them the possibility to choose anonymity. It is worth mentioning that the issue has not been dealt with by the CJEU. However, some national legislations have already decided on the topic. The WBD provides also with some guidance on how the EU stands.

### 4.2.1. Reporting schemes must be confidential

It is widely recognized in various national laws that reporting schemes must always be confidential for the whistleblower.[142] Confidentiality is especially important because it may be determinant for a prospective whistleblower: the whole procedure cannot be set in motion (i.e. by a report) if there is no trust in the scheme. Point 5 of the Proposal on the WBD also stressed the importance for reporting schemes to guarantee the confidentiality of the identity of the reporting person as a cornerstone of whistleblower protection.[143]

[139] Ibid.

[140] Art. 9(1)a WBD.

[141] Art. 17 WBD.

[142] See Loi Sapin 2 (France), Regulation on Labor Security Supervision and Criminal Procedure Law of the PRC (China), SOX-Act (USA).

[143] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of persons reporting on breaches of Union law, (2018).

As a rule, the controller must ensure the confidentiality of the sensitive information circulating in reporting scheme. [144] It is worth mentioning that the obligation of confidentiality also extends to any potential third-party given authority to process, third-party which will have to be bound by a specific contractual obligation of confidentiality.

Confidentiality should also be achieved through adapted technical and organizational measures.[145] The initial proposal of the GDPR provided for a list of the said measures, but it has not been included in the final version. However existing national laws provide example of such measures. France for instance adopted a special law[146] allowing employees to report crimes, serious violations of legal obligations or a serious threat or harm to the general interest. As such, this law supplements to the existing EU obligations in matters of suspected corruption, but it also has a big focus on reinforcing confidentiality of reporting schemes. For this purpose, companies now have the obligation to adopt a specific organizational measure: the establishment of ethical referent. A mirroring obligation can also be found in the WBD,[147] enshrining the mandatory designation of impartial person or department.

Both the ethical referent and the impartial person are meant to provide with an individual in the reporting scheme who will be responsible for receiving and handling whistleblowing reports. In France, the employment contract of this ethical referent must contain an obligation of reinforced confidentiality. In the case where the role of ethical referent is attributed to an employee who will now have this mission as additional role, this employee must go through a specific training including special data protection considerations. The strategy behind the establishment of a mandatory ethical referent seems to limit to one the number of persons responsible for the confidentiality of the system.

[144] Art. 24(1) GDPR.
[145] Ibid.
[146] Loi Sapin 2 (LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique).
[147] Art. 9(1)c WBD.

By being familiar with the case from the date of the reception of the whistleblowing report, through the evaluation of its validity, its transmission to the competent investigating team and by being the contact person of the whistleblower, the ethical referent has a central position. The responsibilities are numerous (arguably, too numerous for one person), but the overview the referent will gain on the case, is seemingly hoped to be key when it comes to correctly balancing the various rights of the data subjects.

While it is generally important to maintain the confidentiality of the whistleblower's identity, in certain situations the ethical referent/impartial person may reasonably believe that disclosure of the whistleblower's identity is essential to the investigation. This point will be further developed below, when addressing the non-absolute character of confidentiality.

### 4.2.2. However, confidentiality is not absolute

The principle of confidentiality in the GDPR seems to not be absolute.[148] Indeed, the obligations of Art.5(1)f, i.e. ensuring protection against unauthorized or unlawful processing, do not prohibit the GDPR to simultaneously allow controllers to disclose to data subjects the source from which their personal data has been collected.[149]

This provision applies in situations where the personal data processed by the controller had not been provided by the data subject- which is the very essence of the type of processing taking place in reporting schemes. In practice, disclosing the source will imply disclosing the identity of the individual who provided said personal data. Thus, in this context, disclosing an identity (i.e. processing said identity) could fall within the scope of a lawful processing of personal data. This demonstration explains why confidentiality, as enshrined in the GDPR, is not an *absolute* confidentiality i.e. that would prevail in all situations. In the contrary, the right to confidentiality could potentially be balanced with other interests – i.e. the rights of other data subjects.

[148] See Irene Hagen, "Konfidensialitetsprinsippet ved varsling av kritikkverdige forhold", Juridika (18th May 2020) <https://juridika.no/innsikt/gdpr-og-varsling> Accessed 10th June 2020.
[149] Art. 15(1)g GDPR.

Thus, in light of the GDPR, confidentiality in reporting schemes might be materialized as a duty to keep the identifying information about the whistleblower secret (i.e. limited to the authorized staff members), as long as this does not conflict with other rights.[150] This could for instance be the case in situations where the whistleblower has knowingly and intentionally made false accusations.[151]

It is also worth reminding that the person responsible for processing (i.e. the controller) must rely on a valid legal basis for each processing of personal data operated by him. Simultaneously, each processing operation must have its own set out purpose.[152] As analyzed in Subchapter 3.1., the reception of a whistleblowing report constitutes a processing of personal data requiring a legal basis. Similarly, the handling, transmitting or internal discussing of such report falls under the definition of processing personal data and from there, also subject to a valid ground for processing. The same applies to any disclosure of the whistleblower's identity. Indeed, the GDPR provides data subjects with the right to know the source from which their personal data has been collected.[153]

In addition, according to the principle of necessity and data minimization discussed in subchapter 3.3., processing of personal data should be limited- but is allowed to the extent that is it necessary for the purposes. And in the context of reporting schemes, revealing information concerning the whistleblower might be admitted as necessary for an effective internal investigation.

On EU level, the WBD also considers the validity of a potential "necessary and proportionate obligation" to disclose the identity or information related to the identity of the reporting person. The WBD therefore acknowledges disclosure in two situations. The first has a larger scope, stating the context of investigations by national authorities or judicial proceedings. The second is more specific, expressly mentioning judicial proceedings with a view to safeguarding the rights of defense of the alleged wrongdoer.[154]

---

[150] Irene Hagen, "Konfidensialitetsprinsippet ved varsling av kritikkverdige forhold", Juridika (18th May 2020) <https://juridika.no/innsikt/gdpr-og-varsling> Accessed 10th June 2020.

[151] WP29 p.11

[152] Art. 5(1) a and b GDPR

[153] Art. 15(1)g and Art. 14(2)f GDPR.

[154] Art. 16(2) WBD.

The WBD seems here to highlight a possible reconciliation between the rights of the two main data subjects in the context of reporting schemes, and as such, appropriately reflect the exceptions derived from the data protection obligations enshrined in the GDPR.

### 4.2.3. Anonymity must be possible

Anonymity is often presented as the ultimate guarantee of confidentiality. Sometimes, anonymity might even be the only possible way for an individual to communicate on misconduct without taking risks on his safety. This is especially relevant where the whistleblower does not trust his organization or/and the applicable national legislation on the field.

However, there are suggestions leaning towards the fact that anonymity might sometimes have the exact opposite effect. Most of the arguments against anonymity as an appropriate mean to contribute to either an efficient reporting scheme or confidentiality are firmly grasped by the WP29. The document goes pretty deep in the analysis and thoroughly explores the tension between the need to protect whistleblowers from retaliation in the workplace and the need to protect companies from the distraction and expense of defending against frivolous or misguided claims.[155] Some of the most convincing arguments are depicted below.

When it comes to protecting the identity of the whistleblower, anonymity might not be efficient because it does not guarantee that others will not guess it, including the alleged wrongdoer. When it comes to protecting the whistleblower against retaliation, it is easier when the competent entities clearly know who must be protected.

When it comes to the company, including anonymity isn't considered as contributing to a good whistleblowing policy because it might shift the focus on the unknown variable (i.e., focusing on finding out who is the anonymous whistleblower), instead of focusing on the wrongdoing that is being reported.

[155] International Bar Association, "Whistleblower Protections: A Guide" (April 2018).

When it comes to the social climate in the company, the idea of anonymous reporting on them potentially striking at any time might lead to a suspicious atmosphere among employees.

In this context, the WP29 still admits that there are some cases where the possibility of anonymity is essential and acknowledges that Member States should allow it. However, reporting schemes should be built in a way where anonymity is not encouraged.[156] On the other hand, the EDPS does not address the benefits of anonymity and adopts the view that in principle, whistleblowing should not be anonymous.[157] Currently, many whistleblowing laws provide a process of anonymous reporting for whistleblowers. [158] Some allow anonymous reporting while not encouraging them – or even discourage them.[159] In some national laws, anonymity is not allowed at all.[160]

The WBD leaves the choice to the Member States. They can themselves determine whether the legal entities of the private and public sector must allow the anonymous report on breaches of EU law, or whether the whistleblower must disclose his identity for the report to be accepted and followed-up.[161]

It is also worth mentioning that anonymous data is per definition non-personal data and should as a rule, not be subject to data protection rules.[162] However, anonymity of the whistleblower does not mean that the data linked to his report is not personal data anymore. The report might refer to specific events, situations and contexts that are only linkable to one potential whistleblower;[163] and personal data is defined as any information that relates to an identifiable person.

[156] WP29 Opinion, p.10-11.
[157] EDPS Guidelines (2019), p.6.
[158] Sox-Act (USA), in the UK or also in Japan.
[159] This is the case in France, in Germany and in the Netherlands.
[160] In Australia and in South-Africa.
[161] Recital 34 and Art. 6(2) WBD.
[162] Recital 26 GDPR.
[163] EDPS Guidelines (2019), p.10.

There is no requirement that all the information enabling the identification of the data subject must be in the hands of one person.[164] In light of this, companies should continue to process the received information with as much diligence as they would a non-anonymous report.

## 4.3. Reporting schemes must equally protect the alleged wrongdoer

After having analyzed how data protection rules contribute to ensuring confidentiality of reporting schemes in respect to the whistleblower, the following chapter will focus on how data protection apply to alleged wrongdoers incriminated in reporting schemes.

### 4.3.1. Proper application of the information rights

One of the GDPR's main concern is to grant EU citizens a stronger control over their personal data. [165] For a data subject to have control, the preliminary step is for him to be aware of the processing operations taking place on his personal data. For this purpose, the GDPR introduces a (longer)[166] list of information that must be communicated to the data subject where personal has not been collected directly by him, but by a third party.

Mandatory information includes the identity of the controller, the legal basis for and purpose of processing and the categories of data concerned.[167] Novelty after the DPD, the obligation laying on the controller to inform about the processing operation now also includes specifying the period of data storage, or at least the criteria for determining the storage period;[168] the legitimate interest of the controller if the processing is based on Art. 6(1)f GDPR as well as informing the data subject on his right to lodge a complaint with the supervisory authority.[169]

Provision of these information is systematic, i.e. provision is not conditioned to express solicitation from the data subject. This *systematic* aspect makes sense because data subjects have no other way

[164] C-582/14 *Breyer*.
[165] See the European Commission's "Questions and Answers-GDPR", Fact Sheet IP/17/386 (Brussels, January 2018).
[166] In relation to the equivalent provision in the old DPD, i.e. Art. 11 DPD.
[167] Art. 14(1) GDPR.
[168] Art. 14(2)a GDPR.
[169] Art. 14(2)f GDPR.

to know that there is personal data about them that is being processed, and as such, have no incentive to ask the controller up front for the processing details. This information obligation rests on the controller, who is also responsible for providing and making the information available in a clear and understandable way.[170]

The particularity of reporting schemes is that their aim is to host transmissions of potentially incriminating information on an individual (i.e. the alleged wrongdoer) being denunciated by another (i.e. the whistleblower). As such, and even if the scope of what can be reported is limited,[171] reporting schemes essentially require processing of personal data that has not been obtained from the data subject. The difficulty here lays in complying with the alleged wrongdoer's information rights when they collide with the purposes of the reporting scheme.

There are two main information obligations that present difficulties when applied in the context of reporting schemes. The first is warning the alleged wrongdoer that his personal data is being processed in relation to a whistleblowing procedure.[172]

In 'standard' situations, companies have per art. 14(3)a GDPR a "reasonable period" after reception of the whistleblowing report to provide all processing information on the data subject's personal data. This reasonable period is limited to one month.[173] However, having regards to the specific circumstances in which the personal data is processed, the GDPR acknowledges some exceptions. Indeed, per Art. 14(5)b GDPR, paragraphs 1-4 of Art. 14 GDPR (i.e. the information that must be provided and the information period limitation) do not apply insofar as the provision of such information is *likely to render impossible* or *seriously impair* the achievements of the objectives of that processing. [174] Thus, the purposes of the processing operation can be ground for limitations to the information rights of the data subject.

[170] See subchapter 3.2. on the overarching principles of transparency, fairness and accountability.
[171] See subchapter 3.1. on lawfulness of processing and 3.3 on the principle of purpose limitation.
[172] Art. 14(1) GDPR.
[173] Art. 14(3)a GDPR.
[174] Art. 14(5)b GDPR.

In the context of reporting schemes, the purpose will mostly be to expose misconduct affecting either the company or the public interest. In both cases, informing the alleged wrongdoer on an early stage might be detrimental for the internal investigation needs.[175]

In other words, in the exceptional circumstances where there is a substantial risk that such notification would jeopardize the company to effectively investigate the allegation or gather the necessary evident, companies could lawfully defer information rights as long as such risk exists.[176] In such case, the controller must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests.[177] This means that companies must not only adopt internal rules covering the exceptional cases where providing this information could be deferred,[178] but also systematically exercise a preliminary necessity and proportionality test, specific to each case, where restriction of the alleged wrongdoer's information right is considered.[179] In light of the overarching principle of transparency, the decision to restrict a data subject's right – which, again, must be decided on a case-by-case basis- must also be documented.[180]

It is worth reminding that when informing the alleged wrongdoer, controllers must ensure to preliminarily remove from the files the personal data on the other individuals concerned by the whistleblowing procedure.[181]

The second information obligation presenting difficulties in the context of reporting schemes is providing the alleged wrongdoer with information on the source of said data. [182] This issue will be analyzed under the alleged wrongdoer's right to access his personal data.

[175] EDPS Guidelines (2019), p.8; WP29 Opinion (2006), p.13.
[176] Art. 14(5)b GDPR.
[177] Ibid.
[178] EDPS Guidelines (2018), p.9.
[179] Ibid.
[180] WP29 Opinion, p.7.
[181] See subchapter 3.2. on purpose limitation and data minimization.
[182] Art. 14(2)f GDPR.

### 4.3.2. Lawful restrictions of the right to access personal data

Right of access of the data subject on his personal data is regulated in Art. 15 GDPR. Access confers the data subject with the right to obtain confirmation from the controller as to whether or not personal data concerning him is being processed. As such, it is tightly linked to the information right of Art. 14 GDPR discussed earlier. The difference is that the right to information is systematic, while the right to access is conditioned to a solicitation from the data subject.

Reading these provisions subsequently, we could deduct that if companies lift the right to information through the exception of Art. 14(5)b, the right to access of Art.15 would simultaneously be restricted too. However, there is no existing opinion or guideline that is either confirming or denying such interpretation of these GDPR provisions. Guidance on the topic is hoped to arrive soon as the EDPB set as one of its 2020 priority to develop guidance on the rights of data subjects as outlined in the GDPR.[183]

As stated earlier, the second problematic concerns the data subject's right to know from which source his personal data originated. The first unclarity concerns the meaning of "source". The obligation to divulgate the source of personal data that has not been directly obtained from the data subject is formulated slightly differently in the two GDPR provisions. Per Art.14(2)4, the alleged wrongdoer should be systematically be informed "from which source the personal data originates".

Per Art. 15(1)g, the alleged wrongdoer should have the right to obtain from the controller "any available information as to the source". In the context of reporting schemes, it is not clear as whether this requirement would oblige controllers to disclose *the identity of* the whistleblower, or if it would be sufficient that it emanates from *a* whistleblower. However, in light of the GDPR's aim to transparency and reinforcing data subject's right, limiting the information on the source to "a" whistleblower might be both dishonest and unlawful.

[183] Greet Gysen, "Getting Data Subject's Rights right" Information and Communication of the EDPB (Linkedin, 8th January 2020) < https://www.linkedin.com/pulse/getting-data-subject-rights-right-greet-gysen/ > Accessed 30th August 2020.

Notwithstanding, there are other exceptions restricting the alleged wrongdoer's right to access to the source.

The first exception lies in Art.14(5)b GDPR. Equivalently to the right of access, the right to know the source of the personal data is consecrated in both Art. 14 and Art. 15 GDPR. However, in light of whistleblower protection that is raising on both national and EU level, controllers could also choose to rely on the exception listed in Art. 14(5)c GDPR. Indeed, this provision provides with an exception to the information rights of the data subject "in the case where obtention and communication of the said personal data is subject to specific provisions in national or EU law". To lawfully rely on this exception, companies have to ensure that they are *expressly* subject to the legal obligation. The WP29 already made clear that for a legislation to lawfully back up processing operations, the said legislation must be directly addressed to the controller relying on it.[184]

One of the main interrogations in today's applicable EU data protection law revolves around the meaning of Art. 15(4) GDPR, which seems to provide for a second potential exception to the alleged wrongdoer's right to access. The provision states that "the right to obtain a copy of the personal data undergoing processing shall not adversely affect the rights and freedoms of other". As such, this provision constitutes the only *express* exception to the data subject's right to access. The first question here is whether the right of access could negatively affect the rights and freedoms of others. In the context of reporting schemes, there is a clear friction between the right to confidentiality of the whistleblower and the right to access of the alleged wrongdoer.

Providing information on the whistleblower to the alleged wrongdoer could undoubtedly involve potential risks of work-related retaliation.

This then leads to the second question: whether this provisions means that controllers should apply a balancing test between the different rights of freedoms at stake, i.e. between the rights of the data subject invoking his right to access, and any other potential individual who would adversely be affected. Indeed, the broad wording chosen by the EU legislator seems to imply that any conflict between, on one hand, the right to obtain a copy and, on the other hand, the rights of freedoms of

[184] WP29 Opinion, p.7.

others, will always be settled to the prejudice of the first one.[185] Even though the provision does not preclude this interpretation, i.e. in systematic favor for the "other's right", the GDPR's aim and thorough developments on data subject's rights seems to largely scream against it and would probably not hold if argued in Court.

As such, companies wishing to restrict the alleged wrongdoer's access on his personal data should ensure to establish a balance of rights and adopt the appropriate measures to protect his rights, freedoms and legitimate interests per Art. 14(5)b GDPR.

The third exception to the data subject's right to access lies in Art. 23 GDPR. Indeed, the provision allows for national or Union legislation to restrict the scope of obligations of the controllers and rights of the data subject. On EU level, the relevant legislation applicable to internal reporting schemes is the WBD. Art. 16(2) provides that the controller's duty of confidentiality i.e. to protect the identity of the whistleblower can only be lifted in two specific situations. Indeed, it is permissible to disclose personal data to others than "authorized staff members" exclusively (1) where there is a necessary and proportionate statutory obligation in connection with investigations carried out by national authorities, or (2) in legal proceedings, including with a view to safeguarding the rights of defense of the alleged wrongdoer. Thus, as a rule and with the exception of legal proceedings engaged by the alleged wrongdoers, the protection of the whistleblower's identity should not be divulged to the alleged wrongdoer.

However, it is worth reminding that the WBD only covers the protection of whistleblowers reporting breaches of EU law. As such, companies establishing and managing reporting schemes with the purpose of a legitimate interest or fulfilling other purposes falling outside the scope of the WBD, will have to rely on another provision that the WBD in order to lawfully restrict the right of access of the alleged wrongdoer.

[185] IT IP Law Group Europe "Right of Access of the Data Subject: Review of EU Regulation" (UK, 2016) <https://www.gdpr-expert.com/article.html?mid=5&id=15#eu-regulation> Accessed 1st September 2020.

The WP29 further recognized that there are cases where a report could be found unsubstantiated and where a user of the reporting scheme could have maliciously made a false declaration. In these situations, the alleged wrongdoer may want to pursue a case for libel or defamation.

Then, and only where national law allows, could the identity of the reporting person be disclosed to the falsely accused person.[186]

Another exception to the right to access could also be adopted on the basis of Art. 88 GDPR, allowing Member States to lay down specific rules in the field of employment by law or collective agreements, provided that the Commission is notified without delay.[187]

### 4.3.3. Fair limitations to the storage of personal data

Art. 5(1)e GDPR provides that personal data shall not be kept in a form which permits identification of the alleged wrongdoer for longer that is "necessary for the purposes for which the personal data are processed". In the context of reporting schemes, the storage question emerges once the whistleblowing case is closed. Companies have then the option between either deleting or storing the relevant personal data. The answer lies in the notion of "purposes": controllers should determine the data retention period with regard to the purposes of processing, i.e. in regard to the specific context of internal investigations. Consequently, this means that data retention must have an expiration date. There is no need to have a precise time-frame, but the controller must set out the criteria according to which the period will be determined.[188] This includes the obligation for the controller to have a tool able to manage the destruction of data when the said period expires.

In practice, conservation periods should depend on the outcome of the case.[189] As such, companies should not implement standard conservation periods, but instead, apply different ones on a case by case basis. This includes taking into consideration the type of personal data that has been processed, making a selection of the information that might be important to keep demonstrating potential recidivism or to provide for in future legal proceedings. The WP29 also stated that

[186] WP29 Opinion, p.15.

[187] See subchapter 3.1.3. on the specific protection of personal data in the context of employment.

[188] Art. 14(2) a GDPR.

[189] EDPS Guidelines (2019), p.10.

personal data relating to whistleblowing reports found to be unsubstantiated should be deleted and not be further processed.[190] The EDPS added that any information that is not relevant to the case should not either.[191]

In parallel, Art. 18 WBD provides that Member States shall ensure that the legal entities in the private sector keep records of every report received, at the condition that it is done in accordance with the confidentiality requirements. As such, the only limitation derives from the obligation to keep the information safe from unauthorized and unlawful access.[192] In light of the GDPR's obligation to restrict processing through storage limitation, Member State will most probably not choose to introduce the infinite storage period recommended by the WBD. However, companies will probably be able to rely on the WBD's provision to justify long storage periods.

In addition, Art. 5(1)b GDPR introduces a new exception to the prohibition to process personal data for purposes that are incompatible with the initial purposes, i.e. ensuring a functional reporting scheme. Indeed, archiving for the "higher" public interest, i.e. historical, statistical and scientific purposes, can lawfully replace the initial legal obligation or legitimate interest of the controller. However, controllers will have to ensure that they fulfill the Art. 89(1) GDPR requirements of "appropriate safeguards for the rights and freedoms of the data subject."

In practice, this means that companies will have to strictly apply the principles of data minimization, [193] i.e. controllers should not process information that is not strictly necessary for the case and reduce the risks to the data subjects through pseudonymization of the personal data, if compatible with the purposes.[194]

[190] WP29 Opinion, p. 12.
[191] EDPS Guidelines (2019), p.9.
[192] See subchapter 4.1. on the overarching principle of confidentiality.
[193] Art. 5(1)c GDPR.
[194] Art. 89(1) GDPR.

### 4.3.4. Lawful overriding of the right to object, rectify and erase personal data

The alleged wrongdoer can exercise his right to object pursuant to the conditions laid down in Art. 21 GDPR. Where the reporting scheme is based on the legitimate interest of the company, the data subject has a right to object at any time to the processing of personal data concerning him.[195] The alleged wrongdoer should specify on what elements relating to his particular situation he grounds his request.

In this situation, the only possibility for the controller to proceed the processing operation is by demonstrating "compelling legitimate grounds" which "overrides the interests, rights and freedoms" of the alleged wrongdoer; or for the "establishment, exercise or defense of legal claims". However, in the context of reporting schemes, the right to object might be difficult to apply in practice. If it is undeniably trickier for a company to demonstrate compelling legitimate grounds justifying further processing at the early stage of a whistleblowing procedure, it might pass a long time during which the alleged wrongdoer will not be warned that his data is being processed. [196] As such, it is very possible that most of the time, the alleged wrongdoer will only be made aware once the allegations are already confirmed or unfounded. Thus, even where the reporting scheme is based on the legitimate interest of the company, the alleged wrongdoer will most likely not be successful in his request to cease the processing operations concerning him.

Notwithstanding, the alleged wrongdoer has a right to rectification, regulated in Art. 16 GDPR and specifically recognized by Art. 8 of the European Charter conferring him the "right to obtain from the controller without undue delay the rectification of inaccurate data concerning him."

However, rectification only applies to objective, factual data: the alleged wrongdoer cannot invoke his right to rectification to modify subjective statements which cannot, by definition, be factually wrong.[197] In this regard, the French DPA provides guidance: the alleged wrongdoer's right to rectification should only affect data whose accuracy can be verified by the data controller.

---

[195] Art. 21(1) GDPR.

[196] Subchapter 4.3.1. on the proper application of information rights.

[197] EDPS Guidelines on the rights of individuals with regard to the processing of personal data (25th February 2014), p.18.

The right to rectification should also not be ground for the deletion or replacement of the initially collected data, and this even where demonstrated that said data is erroneous. In addition, controllers should ensure that granting this right does not lead to the modification of the elements of the whistleblowing report, nor impede the chronological reconstruction of the elements which are essential to the internal investigation.[198]

In light of these elements, it once again seems that in the context of reporting schemes and similarly to the right to object, the right of rectification of the alleged wrongdoer is subject to a very restrictive interpretation. The practical implications of the alleged wrongdoer's right of rectification will therefore be limited to the right to complement the data that is being processed on him with his own version of the facts, i.e. provide a supplementary statement, or have the possibility to rectify inaccuracies through counter arguments. Thus, the right to rectification contained in the GDPR provides with a real opportunity for the alleged wrongdoer to express himself and make his case.

The right to erasure, also called the right to be forgotten, is regulated in Art. 17 GDPR. This right becomes particularly relevant once the whistleblowing case is closed and potentially stored. As discussed earlier, controllers are restricted in their storage processing operations by the data protection principle of purpose limitation. The alleged wrongdoer – who will, in this situation, not be an alleged, but confirmed wrongdoer- must be forgotten if he either (1) demonstrates that the storage, i.e. processing of his personal data is no longer necessary in relation to the processing purposes,[199] or (2) if he objects on the basis of Art. 21(1) GDPR as discussed above,[200] or (3) demonstrates that his personal has been unlawfully processed, e,g. on a unlawful legal basis or treated with a lack of confidentiality,[201] or (4) demonstrates of a national or Union legal obligation to which the controller is subject and requiring that his personal data be erased.[202]

---

[198] See "Standard on processing personal data for the purpose of whistleblowing" of the French DPA CNIL (18th July 2019) <https://www.dataguidance.com/opinion/france-cnil-standard-processing-personal-data-purpose-whistleblowing> Accessed 4th September 2020.

[199] Art. 17(1) a.

[200] Art. 17(1) c.

[201] Art. 17(1) d.

[202] Art. 17(1) e.

Notwithstanding, his right to be forgotten will only succeed if the controller does not have (1) a legal national or EU obligation which requires further processing[203] nor (2) archiving purposes that would be rendered impossible or seriously impaired were the wrongdoer's personal data erased,[204] or (3) legal claims to establish, exercise or defend.[205] As such, the right to be forgotten is not absolute and really limited in its scope in case the alleged wrongdoer is proved guilty through an internal investigation.

However, it becomes very handy in the case of unfounded and malicious claims, allowing the wrongfully suspected individual to not have a record and leave unstained from the whistleblowing procedure.

# 5. Conclusion

Throughout this thesis, we saw that in the context of reporting schemes, enforcing the data protection rules enshrined in the GDPR mainly contributes to the protection of the accused person, while the WBD focuses on the protection of the whistleblower.

Whistleblowing benefits from a growingly wide recognition both at national and Union level, where there has been a prioritization in ensuring a thorough protection of whistleblowers. But on the other hand, reporting schemes also entail a very serious risk of stigmatization and victimization of the person being accused.[206] Such risks exist within the organization to which he or she belongs already before the investigation of the alleged facts and the conclusion on whether or not they are substantiated. There are, as of today, no Union or national laws specifically aiming to protect the investigated individual in the context of internal reporting schemes. Indeed, since the procedure remains internal to the company, the rules existing in governmental investigations or legal proceedings do not apply. As such, the key to reduce the aforementioned risks, is to ensure a proper application of data protection rules. There is no element against the fact that even if incriminated by a reporting scheme, the alleged wrongdoer is still entitled to their data protection rights[207]. This

[203] Art. 17(3) b.
[204] Art. 17(3) d.
[205] Art. 17(3) e.
[206] WP29 Opinion, p.7.
[207] Ibid, p. 6.

is also a direct consequence of the EU principle of presumption of innocence[208]. In these circumstances, protecting the alleged wrongdoer will primarily go through protecting their personal data.

An interesting aspect highlighted in this thesis is that there is no case law in the field of whistleblowing on the CJEU level. Consequently, guidance on both EU and national level derives principally from advisory bodies.

This thesis has shown that in practice, the particularity of reporting schemes allows for important restrictions of the data protection rights of both the alleged wrongdoer and, to a smaller extent, the whistleblower. At EU level, these restrictions are derived from both the GDPR and the WBD. However, the GDPR also provides with safeguards aiming to limit the possible restrictions on these rights: while the overarching principle of confidentiality generally restricts the divulgation of the identity of the whistleblower, the limitations on the alleged wrongdoer's right to information, access, object, rectify and delete are confined to what is strictly necessary for either the purposes of reporting schemes or for the protection of the whistleblower. At national level and following the GDPR, the focus has principally been on ensuring proper data protection rules in the controller-data subject relationship. Reporting schemes however introduce the difficulty to balance the rights of various data subjects. In light of this, it will be interesting to see how Member States implement the WBD into their national legislation.

Until then, it seems like reconciling the protection of whistleblowers and the various obligations deriving from data protection rules is possible, provided to constantly operate a fair balancing work between the two rights.

[208] Article 48 EU Charter of Fundamental Rights.

# References

## Legal instruments

EU legislation


- Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02. Retrieved from: <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> Accessed 6th September 2020.
- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31. Retrieved from: <https://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX%3A31995L0046 > Accessed 6th September 2020.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1. Retrieved from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj > Accessed 6th September 2020.
- 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, OJ L 305. Retrieved from :< https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L1937> Accessed 6th September 2020.
    - Annex 6 of Directive (EU) 2019/1937. Retrieved from : <https://ec.europa.eu/info/sites/info/files/1-11_annexes.pdf> Accessed 6th September 2020.


National legislation


- « Sarbanes–Oxley Act of 2002 ». Retrieved from: <https://www.soxlaw.com/> Accessed 6th September 2020.

- « Loi Sapin 2 (LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique) ». Retrieved from : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033558528&categorieLien=id> Accessed 6th September 2020.
- "Finnish Act on the Protection of Privacy in Working Life (759/2004)". Retrieved from: < https://tem.fi/en/protection-of-privacy-at-work#:~:text=The%20most%20important%20Finnish%20legislation,Life%20(759%2F2004).&text=many%20special%20acts.-,The%20Act%20on%20the%20Protection%20of%20Privacy%20in%20Working%20Life,relationship%20between%20employers%20and%20employees. > Accessed 6th September 2020.


**Guidelines and Opinions**

On EU level


- Proposal for a Directive of the European Parliament and of the council on the protection of persons reporting on breaches of Union law (23rd April 2018). Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0218> Accessed 6th September 2020.
- EDPB Guidelines on consent under Regulation 2016/679, version 1.1 (4th May 2020), retrieved from: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> Accessed 6th September 2020.
- EDPS Guidelines on processing personal information within a whistleblowing procedure (18th July 2016), retrieved from : < https://edps.europa.eu/sites/edp/files/publication/16-07-18_whistleblowing_guidelines_en.pdf > Accessed 7th September 2020.
- EDPS Guidelines on processing personal information within a whistleblowing procedure (17th December 2019), retrieved from <https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-processing-personal-information-within_en> Accessed 7th September 2020.

- EDPS Guidelines on the rights of individuals with regard to the processing of personal data (25th February 2014), retrieved from: < https://edps.europa.eu/press-publications/press-news/press-releases/2014/edps-guidelines-rights-individuals-data-protection_en> Accessed 7th September 2020.
- WP29 Guidelines on consent under Regulation 2016/679 (28th November 2017). Retrieved from: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> Accessed 6th September 2020.
- WP29 Guidelines on transparency under Regulation 2016/679 (22nd August 2018), retrieved from: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 > Accessed 6th September 2020.
- WP29 Opinion 1/2006 on the application of EU data protection rules to internal WB schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crimes. (1st February 2006). Retrieved from : <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf> Accessed 6th September 2020.
- WP29 Opinion 15/2011 on the definition of consent (13th July 2011). Retrieved from: <https://www.pdpjournals.com/docs/88081.pdf> Accessed 6th September 2020.
- WP29 Opinion 2/2017 on data processing at work (23rd June 2017). Retrieved from: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 > Accessed 6th September 2020.

On national level

- "Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz" of the German DPA (14th November 2018), retrieved from: <https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf> Accessed 6th September 2020.

- "Standard on processing personal data for the purpose of whistleblowing" of the French DPA (18th July 2019), retrieved from <https://www.dataguidance.com/opinion/france-cnil-standard-processing-personal-data-purpose-whistleblowing> Accessed 4th September 2020.
- "Decision GZ: 2020-0.191.240" of the Austrian DPA (25th May 2020), retrieved from : <https://gdprhub.eu/index.php?title=DSB_-_2020-0.191.240 > Accessed 6th September 2020.
- "Decision 26/2019" of the Hellenic DPA (2019), retrieved from: <https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_fr#:~:text=Company%20fined%20%E2%82%AC150%2C000%20by%20the%20Hellenic%20DPA&text=The%20DPA%20considered%20that%20PWC,used%20an%20inappropriate%20legal%20basis> Accessed 6th September 2020.
- "Sanction Nº: PS/00376/2019" of the Spanish DPA, (18th February 2020), retrieved from: <https://cdn.www.gob.pe/uploads/document/file/352614/Resoluci%C3%B3n_del_Consejo_de_Apelaci%C3%B3n_de_Sanciones_N__00376-2019-PRODUCECONAS-2CT20190816-22407-1tpgsw6.pdf> Accessed 6th September 2020.
- "Corrective and sanctioning measure against "La Sapienza" University of Rome" of the Italian DPA (23rd January 2020), retrieved from : <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9269618> Accessed 6th September 2020.


**Books, articles, online publications webinar**


- Udo Bux, *Personal Data Protection*, Fact Sheets on the EU (January 2020). Retrieved from: <https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection> Accessed 2nd August 2020
- DLA Piper, *Whistleblowing laws: Employer's guide to global compliance,* (23rd June 2015). A study by DLA's Piper Employment Group. Retrieved from: <https://www.dlapiper.com/en/us/insights/publications/2015/06/whistleblowing-law-2015> Accessed 6th September 2020.

- European Commission, *Questions and Answers-GDPR*, Fact Sheet IP/17/386 (24th January 2018). Retrieved from: <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387> Accessed 6th September 2020.
- EQS Groups and HTW Chur, *Whistleblowing Report 2019*, (2019) retrieved from: <https://whistleblowingreport.eqs.com/en/home > Accessed 6th September 2020.
- Greet Gysen, *Getting Data Subject's Rights right*, Information and Communication of the EDPB via Linkedin (8th January 2020) < https://www.linkedin.com/pulse/getting-data-subject-rights-right-greet-gysen/ > Accessed 30th August 2020.
- Irene Hagen, *Konfidensialitetsprinsippet ved varsling av kritikkverdige forhold*, Juridika (18th May 2020), retrieved from: <https://juridika.no/innsikt/gdpr-og-varsling> Accessed 10th June 2020.
- C. Hauser, N. Hergovits, H. Blumer (2019), *Whistleblowing Report 2019*, EQS and University of Applied Sciences HTW Chur, Chur Verlag, ISBN 978-3-907247-00-6, retrieved from: <https://whistleblowingreport.eqs.com/en/results/results> Accessed 6th September 2020.
- International Bar Association, *Whistleblower Protections: A Guide*, (April 2018). Retrieved from : <https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=abdcd17c-00e9-444b-9315-f71bdc127a7e > Accessed 6th September 2020.
- IT IP Law Group Europe, *Right of Access of the Data Subject: Review of EU Regulation*, (2016). Retrieved from: <https://www.gdpr-expert.com/article.html?mid=5&id=15#eu-regulation> Accessed 1st September 2020.
- Caroline Joly, i.e. her contribution in the webinar *Loi Sapin 2 : Avez-vous mis en place un dispositif d'alertes professionnelles efficace et conforme ?*, EQS Group (21st June 2018)<https://www.eqs.com/fr/ressources-compliance/loi-sapin-2/> Accessed 10th June 2020.
- Peter B. Jubb, *Whistleblowing: A Restrictive Definition and Interpretation*, Journal of Business Ethics 21, no. 1 (1999).
- M. Krook, M.G. Madsen, T. Brautigam, K. Vesa, A. Lange, *An overview of the Whistleblowing Directive in the Nordics*, Bird&Bird (August 2020), retrieved from : <https://www.twobirds.com/en/news/articles/2020/global/an-overview-of-the-

implementation-of-the-whistleblowing-directive-in-the-nordics> Accessed 1st September 2020.

- E. MacAskill and G. Dance, *NSA files decoded: What the revelations mean for you*", The Guardian (November 1st 2013), retrieved from: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 >Accessed 31st July 2020.
- E. Messer-Davidow, (2002). *Disciplining feminism: From social activism to academic discourse*. Durham, N.C: Duke University Press.
- Gautam Mukunda, *The social and political costs of the financial crisis, 10 years later*, Harvard Business Review, (25th September 2018), retrieved from: < https://hbr.org/2018/09/the-social-and-political-costs-of-the-financial-crisis-10-years-later> Accessed 31st August 2020.
- Luca Tosoni, *Whistleblowing e GDPR: punti critici e scenari future*, Network Digital 360, (13th January 2020) <https://www.agendadigitale.eu/sicurezza/privacy/whistleblowing-e-gdpr-punti-critici-e-scenari-futuri/> Accessed 20th July 2020.
- W. Vandekerckhove, *Whistleblowing and organizational social responsibility; a global assessment*, (2007). *22*(1), Reference & Research Book News, 2007-02-01, Vol.22 (1).
- P. Voigt and A.v.d. Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st Edition, Springer 2017),
- Clint Watts, *Inside the unscrupulous world of social-media manipulation with a penitent whistleblower*, The Washington Post (October 11th 2019), retrieved from: <https://www.washingtonpost.com/outlook/inside-the-unscrupulous-world-of-social-media-manipulation-with-a-penitent-whistleblower/2019/10/11/eb357dd4-eb06-11e9-9306-47cb0324fd44_story.html > Accessed 31st July 2020.

**Case-law of the CJEU**

- Judgment of the Court (Grand Chamber) of 16th December 2008, case C-524/06, Heinz Huber v Bundesrepublik Deutschland.

- Judgment of the Court (Grand Chamber) of 9th November 2010, joined cases C- 92/09 and 93/09, Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen.
- Judgment of the Court (Second Chamber) of 19th October 2016, case C-582/14, Patrick Breyer v Bundesrepublik Deutschland.
- Judgment of the Court (Second Chamber) of 20th November 2017, case C-434/16, Peter Nowak v. Data Prot. Commissione.