# Data protection enforcement in the era of the Directive on whistleblowers

Lachapelle, Amelie

*Published in:*
Research handbook on EU data protection law

*DOI:*
10.4337/9781800371682.00032

*Publication date:*
2022

*Document Version*
Publisher's PDF, also known as Version of record

# 23. Data protection enforcement in the era of the Directive on Whistleblowers: Towards a collective approach?

*Amélie Lachapelle*

## 1. INTRODUCTION

Whatever some people may say, the European Union (EU) General Data Protection Regulation (GDPR)[1] is not a revolution.[2] It only aims to adapt the European data protection rules to the major social and technological developments that have occurred since 1995. This is particularly apparent with regard to the 'governance system' put in place by the GDPR to ensure the effective enforcement of its rules.[3] Just like the Data Protection Directive,[4] the GDPR ignores the role played by whistleblowers as potential effective enforcers of EU law. This issue is indeed left to the discretion of the national lawmakers. While the European lawmaker sought to learn from the Snowden case with the GDPR, it seems it forgot one big lesson: the revelations were made by a whistleblower. Insiders may actively participate in data protection enforcement by providing feedback about the effective compliance of the data protection rules. Perhaps it considered it wise to leave each Member State, according to its own national legal tradition and particularities, to regulate the way public bodies become aware of the violations of European data protection rules, and more precisely the place given to whistleblowing.

It nonetheless remains that the EU Directive on Whistleblowers (DWB),[5] which also applies in the field of data protection, expressly recognizes the role played by whistleblowers as 'one upstream component of enforcement of Union law and policies'.[6] Enforcement 'denotes this process of turning paper into reality or, more eloquently, to translate a set of legal

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016,

[2] V. Verbruggen, 'RGPD: cœur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union européenne' in C. de Terwangne and K. Rosier (eds), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie* (1st edn, Larcier 2018), 31.

[3] Communication from the Commission to the European Parliament and the Council, 'Data protection rules as a trust-enabler in the EU and beyond – taking stock', COM(2019) 374 final, 24 July 2019, 4.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995.

[5] 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 303, 26 November 2019.

[6] Recital 2 DWB.





standards designed to influence human and institutional behaviour into social reality'.[7] With Whistleblowers, a fifth actor thus comes into the data protection governance system, next to national data protection authorities, data controllers, data protection officers and data subjects.

The purpose of this chapter is to examine how this new actor will work with the others. After having contextualized and defined whistleblowing, the main insights of the Directive on Whistleblowers are highlighted (2). The governance system established by the GDPR is then (re)read in the light of the DWB (3).

## 2. WHISTLEBLOWING AS AN EU LAW ENFORCEMENT TOOL

The difficulty in grasping the concept of whistleblowing is due to its history. The European concept of whistleblowing is the product of two distinct ideas: the Anglo-American concept of 'whistleblower' on the one hand and the French concept of 'lanceur d'alerte', on the other hand.[8] We introduce these two concepts before explaining the new rules laid down by the DWB.

### 2.1 Whistleblowing in Europe: Meaning and Functions

We first define the concept of whistleblowing and then highlight its main functions.

#### 2.1.1 The concept of whistleblowing

The concept of 'whistleblower' is multi-faceted. John Doe, Edward Snowden and Erin Brockovitch are all whistleblowers but they are distinct in some ways. Keeping in mind these examples, a distinction can be made between three conceptions of 'whistleblower': the 'civic' whistleblower (Brockovich), the whistleblower *sensu lato* (Snowden) and the whistleblower *sensu stricto* (Doe).[9] Previously, we had to distinguish the whistleblower from other categories of reporters: the informer (in the negative sense of snitch) and the informant.

The distinction between informer and informant is based on the criterion of motivation. The informer is driven by purely personal considerations. In reporting facts to the authorities, they do not seek to defend the public interest or to enforce the law. They seek to please, or at least satisfy, the authorities in order to serve their interests, whether it is to eliminate a competitor, to condemn an enemy, to receive a reward or to be protected. The distinction between 'informant' and 'whistleblower' is based on the public interest criterion. The informant has privileged access to information that may be of interest to a private authority, a State authority or the public and which could not otherwise be exposed. The whistleblower enjoys a surplus of legitimacy over the traditional informant in that he or she is seeking to defend the public interest.

[7] D. Wright and P. De Hert, 'Introduction to Enforcing Privacy' in D. Wright and P. De Hert, Paul (eds), *Enforcing Privacy Regulatory, Legal and Technological Approaches* (Springer 2016), 2.

[8] About the rapprochement between 'whistleblower' and 'lanceur d'alerte', see A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale: de la complaisance à la vigilance* (Larcier 2021), 252–269.

[9] A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale: de la complaisance à la vigilance* (Larcier 2021), 955-963.

The notion of whistleblower *sensu stricto* refers to a person who freely and consciously decides to report information of which he or she is aware *in the workplace*, despite the duty of loyalty, reserve and discretion to the employer, with a view to defending the public interest. An example here is 'John Doe', the whistleblower of the 'Panama Papers'. Using the common alias for the purpose of anonymity, John Doe obviously worked in *Mossack Fonseca*, the law firm where the documents about the offshore companies involved in illegal purposes, including fraud, tax evasion, and evading international sanctions came from.[10] This conception of whistleblower *sensu stricto* is reflected in the Recommendation CM/Rec(2014)7 of the Council of Europe which is inspired by the caselaw of the European Court of Human Rights.[11]

The notion of whistleblower *sensu lato* is extended to people *connected with an organization* and who, in this context, have privileged access to information likely to be of public interest and which could not be exposed otherwise. One example could be the whistleblower Edward Snowden who was a NSA subcontractor. He has worked for *Dell* and *Booz Allen Hamilton*, two NSA service providers. However, this was only a front, as the computer scientist was in fact working for the NSA. The conception of whistleblower *sensu lato* is reflected in the DWB.[12] The DWB aims to enhance the enforcement of Union law and policies in specific areas, privacy area included. That is why, in this chapter, we use the expression 'whistleblower' (or more exactly 'reporting person') as defined in the DWB.

Finally, the notion of 'civic' whistleblower is an extension of the republican conception of civic information.[13] It covers the situation in which a citizen does not only report an illegal fact (in this situation, the reporter is an informant),[14] but also takes a *risk* in order to defend the public interest due to the seriousness of the revelations or how he or she became aware of

[10] See https://en.wikipedia.org/wiki/Panama_Papers accessed 12 December 2021, for a general overview of the scandal.

[11] This also derives from the definition proposed by Prof. Marcia P. Miceli and Janet P. Near, unanimous accepted amongst the scholarship (in this sense, see namely T.M. Dworkin, 'Foreword' in D. Lewis, A.J. Brown et al. (eds), *International Handbook on Whistleblowing Research* (Edward Elgar Publishing 2014)), according to which 'whistleblowing' is 'the disclosure by organization members (formers or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action' (J.P. Near and M.P. Miceli, 'Organizational dissidence: The case of whistle-blowing' (1985) 4(1) *Journal of Business Ethics* 4).

[12] Indeed, effective enforcement of EU law requires that protection should be granted to the broadest possible range of categories of persons who, by virtue of their work-related activities, 'have privileged access to information on breaches that it would be in the public interest to report and who may suffer retaliation if they report them' (Recital 37 DWB 2019). Nonetheless, the European lawmaker did not have the legal competence to go further and to protect persons who report or disclose information outside a professional context ('civic' whistleblower).

[13] In the light of the republican ideas, the 'civic denunciation' is free (no reward), selfless (public interest purpose) and spontaneous (neither professional duty nor legal obligation). About the civic denunciation, see namely V. Martin, 'La révolution française ou l'"ère du soupçon"' (2009) Hypothèses No 1, 131–140.

[14] This situation refers to what we call 'dénonciation traditionnelle ou légale' (traditional or legal reporting) which covers the reporting of illegal acts, most often punishable under criminal law, to State authorities ('information' in the Anglo-American legal tradition). There are two variations: in countries with an adversarial tradition, such as the US and UK, the reporter (or the 'relator') is given the function of a citizen prosecutor. This conception refers to the 'Qui Tam' principle, which is closely linked in the US to the development of whistleblowing. In countries with an inquisitorial tradition, such as Belgium and France, the reporter is, on the other hand, confined to the role of a messenger. See A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale: de la complaisance à la vigilance* (Larcier 2021).



the revelations. In this situation, the reporting person does not therefore act in a work-related context. This is the case, for instance, of Erin Brockovich who became aware of pollution incidents – pollution of drinking water in Hinkley, California – through compensation files consulted in the workplace, a law firm, and decided to denounce them publicly. She was not in a professional relationship with the company denounced, *Pacific Gas & Electric Company (PG&E)*.[15] This conception is reflected in the '*Loi Sapin II*', which sets out a horizontal framework for whistleblowers in France.

In the three cases, the facts of a malpractice have been made public. This is the reason why we know these whistleblowers. But most whistleblowers first try to go up the chain of command and to alert the public bodies. For instance, Cynthia Cooper first reported the accounting malpractice she had discovered such an internal auditor at *WorldCom* to her superiors.[16] The DWB adheres to this model and recognizes whistleblowing as a process. It encompasses three channels of reporting: reporting within a public or private organization ('internal reporting'), to the competent authorities ('external reporting') and reporting to entities who defend the public interest, like a journalist, a parliamentary or a non profit organization (public disclosure).

What is a public interest information? In the first place it concerns information qualified as such by the lawmaker and by the judge where appropriate, but also information about an unlawful act or omission. Within the meaning of the DWB, information about an abusive practice[17] is also qualified for protection. When the reporting occurs within an organization, to a journalist or to an NGO, the information can concern more broadly immoral or illegitimate practices.

### 2.1.2 The functions of whistleblowing

In a 2016 Communication,[18] the European Commission outlined its vision for an effective enforcement of EU rules. Starting with a key finding, that '[e]ffective enforcement of EU rules … serves the general interest', the Commission notes that '[o]ften, when issues come to the fore — car emission testing, water pollution, illegal landfills, transport safety and security — it is not the lack of EU legislation that is the problem but rather the fact that the EU law is not applied effectively'. In this regard, the Commission brought to light that '[m]embers of the public, businesses and civil society contribute significantly to the Commission's monitoring by reporting shortcomings in the application of EU law by the Member States. The Commission acknowledges the crucial role of complaints in detecting infringements of EU law'.

The economic and financial crisis in 2008 has made clear that one cannot rely solely on the diligence of financial institutions to ensure the integrity of the financial system. We also need insiders to raise their concerns. The legislature took these lessons and implemented

[15] A starting point for exploring the work of Erin Brockovich is https://en.wikipedia.org/wiki/Erin_Brockovich.

[16] Cynthia Cooper was named Time Magazine's 'Person of the Year' in 2002 along with other whistleblowers.

[17] An abusive practice is an act or omission which does not appear to be unlawful in formal terms but defeats the object or the purpose of the law (Recital 42 and Art. 5(1)(ii) DWB 2019).

[18] Communication from the Commission 'EU law: Better results through better application' (2017/C 18/02), OJ C 18/10, 19 January 2017.

these into two directives. Pursuant to Directives 2013/36/EU[19] and 2009/138/EC,[20] known as the 'Banking' Directive and the 'Solvency II' Directive, credit institutions and insurance and reinsurance undertakings must have an effective system of governance, including an effective risk-management system, comprising appropriate procedures for their employees to report breaches internally through a specific, independent and autonomous channel.

Since then, the importance of whistleblower protection as a way to prevent and deter breaches of EU rules continued to be acknowledged in sectoral EU legislation. Nonetheless, it became obvious, from the EU legislature's point of view, that this fragmented approach negatively impacted the functioning of EU policies, especially when the breach of law has a cross-border dimension.[21] For several years, the European Parliament had been calling on the European Commission to bring forward a clear horizontal legal framework on the protection of whistleblowers who act in the public interest.

The purpose of the DWB is 'to enhance the enforcement of EU law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches of Union law'.[22]

Whistleblowers are not only the linchpin of corporate governance, but are also conceived as auxiliary agents of the State. Whistleblowing is commonly used as a way to strengthen prevention and countering misconducts, including illegal or wrongful practices, in relation to EU Law and policies (organized crime, corruption, money laundering, tax rulings ...).[23] As a vector of transparency, whistleblowing is expected to enhance detection of breaches to EU Law and policies and to stimulate compliance by the key actors with the latter (i.e., before the whistleblower publicly exposes a non-compliant conduct.[24] By expressly acknowledging public disclosure in the DWB, the European lawmaker finally accepted that a whistleblower may act in some exceptional cases as a citizen watchdog. This was obvious in the case law of the European Court of Justice, under the Article 10 of the Convention, but not so much in Secondary European Union Legislation. This is the symbolic significance defended on both

[19] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, OJ L 176, 27 June 2013, Art. 71.

[20] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), OJ L 335, 17 December 2009, Arts 41, 44 and 46.

[21] Recital 4 DWB 2019.

[22] Art. 1 DWB 2019.

[23] See namely European Parliament resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report) (2013/2107(INI)), P7_TA(2013)0444, §§ 14–15; European Parliament resolution of 25 November2015 on tax rulings and other measures similar in nature or effect (2015/2066(INI), TAXE 1, P8_TA(2015)0408, §§ 144–145; European Parliament resolution of 6July2016 on tax rulings and other measures similar in nature or effect (2016/2038(INI)), TAXE 2, P8_TA(2016)0310, §§ 44–46; European Parliament resolution of 14February 2017 on the role of whistleblowers in the protection of EU's financial interests (2016/2055(INI)), P8_TA(2017)0022.

[24] For an illustration of the regulatory function of transparency in tax matters, see L. Johnson, 'Whistleblowing and investigative journalism: reputational damage and the private governance of aggressive tax planning' in R. Eccleston and A. Elbra (eds), *Business, Civil Society and the 'New' Politics of Corporate Tax Justice. Paying a Fair Share* (Edward Elgar Publishing 2018), 272-276.



sides of the Atlantic. The whistleblower can sometimes act as an auxiliary agent of the State, sometimes as a compliance officer and sometimes as a citizen watchdog.

Even though the GDPR does not really express this point of view, the collective dimension of privacy enforcement has been brought to light for a few years in the literature. Privacy enforcement is an activity that goes beyond regulatory enforcement. In some sense, according to David Wright, 'enforcing privacy is a task that befalls to all of us. [...] Privacy advocates and members of the public play or can play an important role in enforcing privacy'.[25] Finally, influenced by the 'Snowden case' and the 'Cambridge Analytica Files', the European law-maker recognized the valuable role played by whistleblowers in the specific field of data protection with the DWB.

The DWB applies to specific policy areas 'where: (i) there is a need to strengthen enforcement; (ii) underreporting by whistleblowers is a key factor affecting enforcement; and (iii) breaches may result in serious harm to the public interest'.[26] Breaches of EU Law in the area of privacy and personal data protection may undoubtely cause serious harm to the public interest, in that they create significant risks for the welfare of society.[27] Moreover, weaknesses of enforcement have been identified in those areas on the basis of currently available evidence while whistleblowers are usually in a privileged position to disclose breaches.[28] Whistleblowers are particularly valuable in the detection of some types of breaches of European data protection rules despite the robust oversight system put in place by the EU legislation.[29] In addition, the reporting by whistleblowers is also particularly valuable for the prevention of security incidents in accordance to the 'NIS' Directive.[30] Accordingly, the DWB lays down common minimum standards for the protection of persons reporting, amongst others, the breaches falling within the scope of the 'ePrivacy' Directive,[31] the 'GDPR'[32] and

[25] D. Wright and P. De Hert, 'Introduction to Enforcing Privacy' in D. Wright and P. De Hert (eds), *Enforcing Privacy Regulatory, Legal and Technological Approaches* (Springer 2016), 4.

[26] D. Wright and P. De Hert, 'Introduction to Enforcing Privacy' in D. Wright and P. De Hert (eds), *Enforcing Privacy Regulatory, Legal and Technological Approaches* (Springer 2016), 4. With those criteria, the DWB remains proportionate to the objective of strengthening the enforcement of Union law and does not go beyond what is necessary to achieve it in accordance with the principle of proportionality (Recital 108 DWB 2019).

[27] See Recitals 3 and 14 DWB 2019.

[28] Recital 106 DWB 2019.

[29] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law, Commission Staff Working Document, Brussels, 23 April 2018, 26–27.

[30] The DWB underlines that 'whistleblowers can also help disclose breaches of Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of network and information systems, which introduces a requirement to provide notification of incidents, including those that do not compromise personal data, and security requirements for entities providing essential services' (Recital 14 DWB 2019).

[31] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016.

the 'NIS' Directive[33] that concern the area of the protection of privacy and personal data and the security of network and information systems.[34]

## 2.2 The Directive on Whistleblowers

As we noted above, the purpose of the DWB is 'to enhance the enforcement of EU law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches of Union law'. Accordingly, the DWB consists of two main rules: the establishing of channels of reporting and the laying down of common minimum standards providing for a high level of protection of persons reporting breaches of EU Law under the conditions established by the DWB.

### 2.2.1 Channels of reporting

The DWB requires private and public entities to establish, within their own governance structure,[35] internal reporting channels.[36] The notion of 'private entity' is broadly understood in order to encompass all enterprise, for speculative purposes or not. Those channels are, as a rule, a complementary mechanism alongside the other usual control and reporting mechanisms (employee representatives, reporting line, audit, inspection service etc.).[37]

The DWB establishes both internal reporting and external reporting channels. The obligations to establish such channels should build as far as possible on the existing channels provided by specific EU Acts.[38] In addition, the DWB explicitly addresses the issue of public disclosure, in particular to the media.

[33] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19 July 2016.

[34] Art. 2(1) DWB 2019.

[35] About the 'structural' approach of whistleblowing, see T.M. Dworkin and A.J. Brown, 'The Money or the Media? Lessons from Contrasting Developments in US and Australian Whistleblowing Laws' (2013) 11(2) *Seattle Journal for Social Justice* Art. 8, 679. See also A. Lachapelle, 'Le lancement d'alerte ou la délation organisée?' in Y. Poullet (ed), *Vie privée, liberté d'expression et démocratie dans la société numérique* (Larcier 2020), 213–215.

[36] For a comment of the Directive on Whistleblowers, see namely E. Andreis, 'Towards Common Minimum Standards for Whistleblower Protection Across the EU' (2019) European Papers Vol. 4 No 2, 575–588; D. Pollet-Panoussis, 'La protection renforcée des lanceurs d'alerte dans le cadre de l'Union européenne' (2020) Les Petites Affiches No 40, 9–15; A. Lachapelle, 'And thus Tax Whistleblowing was born! Comment on the Directive on whistleblowers in Tax Matters' (2020) T.F.R. No 588, 798–818; A. Lachapelle, 'L'encadrement juridique du lancement d'alerte au sein de l'Union européenne: commentaire de la Directive sur les lanceurs d'alerte' (2020) R.D.T.I. No 78-79, 15–52.

[37] See N. Smaili, 'Le *whistleblowing* : la solution en gouvernance ?' in S. Rousseau (ed), *Gouvernance, risques et crise financière* (Thémis 2013), 240; B. Fasterling, 'Whistleblower protection: A comparative law perspective' in D. Lewis, A.J. Brown et al. (eds), *International Handbook on Whistleblowing Research* (Edward Elgar Publishing 2014), 345; M. Lauvaux, V. Simon and D. Stas de Richelle, *Criminalité du travail: détecter et contrôler les comportements frauduleux – sanctions et responsabilité du travailleur* (Kluwer 2007), 129.

[38] Recital 68 DWB 2019.



#### 2.2.1.1 *Internal reporting channels*

According to Article 8 of the DWB, Member States shall ensure that, unless a derogation is made, private and public entities establish channels and procedures for internal reporting and for follow-up, following consultation and in agreement with social partners where provided for by national law. As a general principle and without prejudice to external reporting and public disclosure, information on breaches may be reported through the internal reporting channels and procedures.[39]

Each individual legal entity in the private and public sector must define the kind of reporting channels to establish. As long as the confidentiality of the identity of the whistleblower is ensured, flexibility is required in the way of reporting.[40]

According to Article 9(1) DWB 2019, the procedures for internal reporting and for follow-up should include the following safeguards and requirements:

i. secure and confidential reporting channels;[41]
ii. acknowledgment of receipt of the report to the reporting person within seven days of that receipt and sending 'feedback' within a reasonable timeframe about the 'follow-up';[42]
iii. the designation of an impartial person or department competent to receive and follow-up on reports;[43]
iv. diligent follow-up by the designated person or department and, where allowed by national law, regarding anonymous reporting;[44]
v. appropriate information relating to the use of internal reporting channels[45] and external reporting channels.[46]

It follows that the designation of a 'Whistleblower Officer' (WBO) to receive and follow-up on reports is mandatory. However, the choice of the most appropriate persons or departments to assume this function depends on the structure of the entity. The DWB also foresees that third parties may be authorized to receive reports of breaches on behalf of public or private entities, provided they offer appropriate safeguards.[47] The DWB draws particular attention to the fact that they must offer appropriate guarantees to respect independence, confidentiality, data protection and secrecy.[48] Such third parties could be external reporting platform providers, external counsels, auditors, trade union representatives or employees' representatives.

At first glance, it can be said that the most appropriate person to receive information on breaches falling within the area of the protection of privacy and personal data, should be the DPO when the designation of such a person is mandatory. This union of functions is, however, not obvious.

[39] Art. 7(1) DWB 2019.

[40] Art. 9(2) and Recital 53 DWB 2019.

[41] Art. 9(1)(a) DWB 2019.

[42] Art. 9(1)(b) and (f) DWB 2019.

[43] Art. 9(1)(c) DWB 2019.

[44] Art. 9(1)(d) and (e) DWB 2019.

[45] Art. 7(3) DWB 2019.

[46] Art. 9(1)(g) DWB 2019.

[47] Art. 8(5) DWB 2019.

[48] Recital 54 DWB 2019.

One particular issue is whether the functions of Data Protection Officer (DPO) and of WBO may be exercised by the same person/department. According to Recital 56 of the DWB, the function of WBO:

> could be a dual function held by a company officer well placed to report directly to the organisational head, such as a chief compliance or human resources officer, an integrity officer, a legal or privacy officer, a chief financial officer, a chief audit executive or a member of the board.

It follows therefore that the WPO could be, at the same time, a DPO. But the reverse is not so obvious because such a situation can give rise to a potential conflict of interest. The GDPR contains rules to prevent DPOs from holding conflicting positions within the organization which:

> may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing.[49]

In a recent decision, the *Chambre contentieuse* of the Belgian DPA recalled that the same natural person cannot be at the same time the DPO and the chief of Audit, Risk & Compliance. The company concerned (the incumbent electronic communications service provider) argued that the functions performed by its DPO were purely consultative. Nevertheless, the *Chambre contentieuse* concluded that there was a potential conflict of interest on the part of the DPO. Indeed, it results from the investigation report that the DPO unquestionably determines the purposes and means of the processing of personal data carried out within the Audit, Risk & Compliance departments, thus acting as a data controller.[50] However, a single (natural) person cannot control and be controlled at the same time.[51]

In so far as the WBO determines the purposes and means of the processing of personal data performed in the course of the whistleblowing mechanism, it is easy to understand that the WBO cannot be at the same time the DPO when both functions are performed by a single natural person. A potential conflict of interest could certainly arise in some circumstances. However, they will need to work hand in hand in many cases.

#### *2.2.1.2 External reporting channels*

According to Article 11 of the DWB, Member States must designate the competent authorities to receive, give feedback and follow up on reports, and must provide them with adequate resources. The notion of 'competent authority' is broad: it could be judicial authorities, regulatory or supervisory bodies competent in the specific areas concerned, or authorities of a more

[49] WP29, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, WP 243, 16. These independence requirements explain why many companies in practice use external consultants to perform the function of DPO.

[50] Chambre contentieuse (APD), Decision on the merits 18/2020 of 28 April 2020 on the inspection report on liability for data leak and the position of the Data Protection Officer, 19, available (in French) on https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf accessed 24 March 2021.

[51] WP29, Guidelines on Data Protection Officers ('DPOs'), cited above, 16.



general competence at a central level within a Member State, law enforcement agencies, anticorruption bodies or ombudsmen.[52]

In the area of the protection of privacy and personal data there is no doubt that the competent authority is the national Data Protection Authority as established under Article 51 GDPR.

Competent authorities in the field of whistleblowing already exist in the UK and Ireland which already have horizontal whistleblowing laws. Indeed, the British Public Interest Disclosure Act (PIDA) has, since 1998, protected workers who make certain disclosures of information ('protected disclosures' in accordance with the law) in the public interest.[53] The worker who is concerned that his or her employer (or ex-employer) may be contravening legislation relating to data protection or freedom of information may contact the British Information Commissioner's Office (ICO), the national DPA.[54] As a 'Prescribed Person', the ICO is required to report annually on whistleblowing disclosures made to it.[55] It adopted a special procedure and published advice for individuals considering making a whistleblowing disclosure.[56] The same practice is observed in Ireland. The Irish Data Protection Commission received, in 2020, pursuant to the Protected Disclosures Act 2014,[57] nine protected disclosures from individuals in relation to issues pertaining to data protection within other entities.[58] As a 'prescribed person', it is required, like the British DPA, to report annually on whistleblowing disclosures made to it.[59]

Whistleblowers are also entitled to report to the European Data Protection Supervisor (EDPS), where appropriate, pursuant to Article 6(4) of the DWB 'persons reporting to relevant institutions, bodies, offices or agencies of the Union breaches falling within the scope of this Directive shall qualify for protection as laid down in this Directive under the same conditions as persons who report externally'.

#### *2.2.1.3 Public disclosure*

The DWB contains an express provision on public disclosure (Art. 15). Reporting persons shall qualify for protection against retaliation whatever the channels of reporting, including public disclosure.[60]

[52] Recital 64 DWB 2019.

[53] The full title is: 'An Act to protect individuals who make certain disclosures of information in the public interest; to allow such individuals to bring action in respect of victimisation; and for connected purposes'. Available on www.legislation.gov.uk/ukpga/1998/23/contents accessed 25 November 2020.

[54] 'Protection for whistle-blowers disclosing information to the ICO', available on https://ico.org.uk/media/report-a-concern/documents/1042550/protection_for_whistle_blowers.pdf accessed 2 March 2021.

[55] Prescribed Persons (Reports on Disclosures of Information) Regulations 2017, No 507, available on www.legislation.gov.uk/uksi/2017/507/contents/made accessed 25 November 2020.

[56] See https://ico.org.uk/about-the-ico/our-information/whistleblowing-disclosures/accessed 25 November 2020.

[57] Protected Disclosures Act 2014, available on http://www.irishstatutebook.ie/eli/2014/act/14/enacted/en/html accessed 23 March 2021.

[58] Report on Protected Disclosures received by the Data Protection Commission in 2020. See also DPC, Annual Report 2020, 81.

[59] Section 22 of the Protected Disclosures Act 2014. 'Reports on Protection Disclosures' are available on https://www.dataprotection.ie/en/who-we-are/corporate-governance/making-protected-disclosure-dpc accessed 23 March 2021.

[60] Recital 45 DWB 2019.

Scandals like the Snowden revelations showed the need to be able to count on insiders in order to monitor effective enforcement of the GDPR. As noted by the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, 'the files leaked by journalists with the help of Mr Snowden have unquestionably contributed to the public interest by disclosing the nature and extent of mass surveillance taking place around the world and the threats to Internet security resulting from certain practices'.[61] The Snowden case showed that cryptographic tools, often considered as the cornerstone of many secure systems, may be cracked by the secret services. Those revelations do not only put into perspective the use of technologies as privacy enforcement but also prove the need to count on insiders to blow the whistle.[62] The public bodies cannot combat unlawful data processing without knowledge of it. It is all the more difficult for the lawmaker to anticipate by law – *in abstracto* – what will be the unlawful data processing of tomorrow because the latter are born in secret thanks to the help of experienced computer scientists. It follows that only insiders are in a position to blow the whistle about what happens really on the ground.

The need to protect whistleblowers in the field of data protection was confirmed a few years later when the 'Cambridge Analytica Files' came to light through revelations made to *The Guardian* and to *The Observer* by a whistleblower who was a former employee of the company at issue. Everyone has since become aware that Facebook data was collected without the knowledge of its users by another company, Cambridge Analytica, and used for different purpose than the one for which it had been collected, in this case, to influence the opinion of Facebook users, but also of their contacts, in the context of election campaigns.[63] Furthermore, recent revelations have taken place in Belgium which shows that whistleblowing may also be useful to expose shortcomings within the National DPA, in this case on questions relating to the independence of the DPA.[64]

#### 2.2.2 Protection of 'reporting persons'

According to Article 6(1) of the DWB, 'reporting persons' qualify for protection under the DWB provided that:

i. they had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of the DWB; and
ii. they reported either internally or externally or made a public disclosure in accordance with the requirements laid down by the DWB.

[61] Parliamentary Assembly of the Council of Europe, Improving the protection of whistle-blowers, Doc. 13791, 19 May 2015, p. 14, § 60.

[62] See namely D. Métayer, 'Whom to Trust? Using Technology to Enforce Privacy' in D. Wright and P. De Hert (eds), *Enforcing Privacy Regulatory, Legal and Technological Approaches* (Springer 2016), 395–437.

[63] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law, Commission Staff Working Document, Brussels, 23 April 2018, 26–27.

[64] See for instance in the press 'Belgium's Data Protection Authority's independence no longer guaranteed, director warns', *The Brussels Times*. Available on www.brusselstimes.com/belgium/156137/belgiums-data-protection-authoritys-independence-no-longer-guaranteed-director-warns/ accessed 22 February 2021.



It should be underlined that only a natural person may benefit from the protection.[65] It follows that the DPO or the processor who whould act as a whistleblower would be qualified for protection only if it acts as a natural person, which is seldom the case. Conversely, the data subjects shall be qualified for protection to the extent that they comply with the conditions prescribed by the DWB.

Additional conditions must be met when the reporting person makes a public disclosure.[66]

## 3. THE WAY THE DIRECTIVE ON WHISTLEBLOWERS OVERTURNS THE ENFORCEMENT OF GDPR

In line with the former 'Data Protection Directive', the GDPR created a 'governance structure' supported by three pillars:[67] national data protection authorities, the controller and the processor, who may rely on a new actor of the compliance, the DPO, and the data subjects. Surprisingly enough, giving that the GDPR was adopted in the middle of the '*Panama Papers*' scandal,[68] the GDPR totally ignores whistleblowing. It further advances an 'individualistic' outlook to enforcement in the sense that the GDPR puts the focus on the data subjects. With specific rights, the data subject is meant to check compliance with the GDPR only as far as he or she is concerned and to bring an action where appropriate. The approach is also centralized in so far as the compliance with the GDPR firstly relies on state bodies.

By acknowledging the role played by the whistleblowers in EU law enforcement, the DWB blows a fresh wind on data protection law. Privacy enforcement becomes a matter of general concern (1). In particular, whistleblowers may be seen as the new pillar of the EU data protection governance structure next to the traditional actors (2).

### 3.1 From an Individual towards a Collective Privacy Enforcement

The GDPR aims at strengthening citizen's empowerment by providing data subjects with effective control over their personal data.[69] For instance, the data subjects should be able to verify the lawfulness of the processing of their personal data.[70] Despite the ambiguous nature

[65] According to Art. 5(7) of the DWB 2019, a 'reporting person' 'means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities'.

[66] Art. 15(1) DWB 2019.

[67] Communication from the Commission to the European Parliament and the Council, 'Data protection rules as a trust-enabler in the EU and beyond – taking stock', COM(2019) 374 final, 24 July 2019, 4. These three kind of actors has competence to decide on data protection issues at an operative level. See L.A. Bygrave and D. Wiese Schartum, 'Consent, Proportionality and Collective Power' in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds), *Reinventing Data Protection?* (Springer 2009), 158.

[68] This scandal came to light thanks to the revelations to the German journal *Süddeutsche Zeitung* made by an anonymous whistleblower. See B. Obermayer and F. Obermaier, *Panama Papers: Die Geschichte einer weltweiten Enthüllung* (Kiepenheuer & Witsch 2016).

[69] Recital 7 GDPR.

[70] Recital 63 GDPR.

of the expression 'data *subject*', one may doubt that the legislator intended to grant a passive role to the data subject.[71]

Nonetheless, in the spirit of the GDPR, an individual can legitimately act only when it has a personal interest.[72] Thus, only concerns about one's individual rights may be raised with the DPO or the DPA. In addition, an individual would not be able to take legal action on the grounds that the rights granted to other individuals by the GDPR have been violated.[73] Such a possibility is obviously reserved only for organizations covered by Article 80 of the GDPR i.e., any body, organization or association referred to in Article 80(1) of the GDPR, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the DPA and to exercise the right to an effective judicial remedy, provided that it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing. In this case, the judgement may be an impact for all the users of the controller and/or the processor concerned. However, the organization is required to consider, before taking an action, that *the rights of a data subject under the GDPR have been infringed as a result of the processing.*

Even if the GDPR puts the focus on the data subjects' rights, the measures of awareness raising and training of the staff members which are now prescribed by the GDPR can be seen as complementary to the reporting channels established by the DWB. Compliance with the accountability principle entails offering adequate data protection training and education to staff members.[74] Some people, like Martin Brodin, think that the GDPR also:

> requires a new way of thinking and working. This makes education important. Organisations need to ascertain that everyone has the right competence to comply with GDPR and to play their individual part.[...] Finally, the people in charge for the strategy and corresponding documents need to pay attention to signals from the business that point to deficiencies in policies and instructions.[75]

In practice, all members of an entity have a role to play to protect personal data, from the lower worker to the senior management. Nevertheless, the higher the position held, the higher the expectations in terms of compliance. It can be said that this collective power of decision making on protection of personal data is a condition of success of the data protection governance system.[76]

[71] For a interesting reflection (already under the 'Data Protection' Directive) about the necessity to grant a positive role to the individual in data protection, see R. Leenes and I. Oomen, 'The Role of Citizens: What Can Dutch, Flemish and English Students Teach Us About Privacy?' in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds), *Reinventing Data Protection?* (Springer 2009), 139–153.

[72] But this is not obvious that only the person concerned has an interest in bringing proceedings. This issue has already been discussed under the 'Data Protection' Directive. See namely J. Herveg, 'La procédure "comme en référé" appliquée aux traitements de données' in J.-F. Van Drooghenbroeck (ed), *Les actions en cessation* (Larcier 2006), 238 and references cited.

[73] While some cases may well have a colletive impact, such cases can not be seen as a common exercise of individual rights. For instance, the proceeding in the *Schrems* case has lasted for seven years and is not finished yet. The financial burden are also very significant.

[74] WP29, Opinion 3/2010 on the principle of accountability, WP 173, 13 July 2010, 11–12.

[75] M. Brodin, 'A Framework for GDPR Compliance for Small and Medium-Sized Enterprises' (2019) 4 *European Journal for Security Research* 255.

[76] On this assumption, see L.A. Bygrave and D. Wiese Schartum, 'Consent, Proportionality and Collective Power' in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds), *Reinventing Data Protection?* (Springer 2009), 157–173.



Despite the scholars' expectations, the GDPR, in its provisions, continues to defend an individual approach of law enforcement. But it was not counting on the DWB which clearly incorporates a collective approach by expressly recognizing the need to protect the persons who work for a public or private organization or are in contact with such an organization in the context of their work-related activities and who speak about threats or harm to the public interest which arise in that context, such as violations in the area of protection of privacy and personal data. Enforcement becomes collective as more space is given to private actors.

### 3.2 Whistleblower as a New Pillar of the EU Data Protection Governance Structure

In light of the DWB, the whistleblower clearly becomes a privileged partner of the DPA firstly and of the controller secondly.

#### 3.2.1 A (new) enforcement tool for the national data protection authorities

At the top of the governance system lies the supervisory authorities.[77] They monitor the application of the provisions pursuant to the GDPR and contribute to its consistent application throughout the EU.

As such, each supervisory authority is competent to handle complaints lodged by a data subjects.[78] No mention is made of reporting by whistleblowers. The GDPR indeed reproduces the centralized approach of enforcement in which a private person may only act in order to ensure the respect for his or her own interests.

In practice, the term 'complaint' is generally understood as limited to the report by a 'victim' or by his or her representative. For instance, a complaint may be submit through the website of the Irish Data Protection Commission if it:

> fall under one of the following headings:
> - A complaint from an individual relating to the processing of their own personal data;
> - A legally authorised person or entity complaining on behalf of an individual (e.g. a solicitor on behalf of a client or a parent/ guardian on behalf of their child); or
> - Advocacy groups which meet the requirements to act on behalf of one or more individuals under the GDPR, LED and the Data Protection Act 2018.[79]

Along the same lines, the UK Information Commissioner's Office (ICO) draws the attention on the difference between a reporting by a whistleblower and a complaint by a data subject.[80]

Nonetheless, in some countries like Spain, the term 'complaint' encompasses the reporting by whistleblowers. Since 25 May 2018, the '*denuncias*' and the '*reclamaciones de tutela*' have been renamed '*reclamaciones*' (complaints) according to the nomenclature in force in the

[77] Recital 117 GDPR.

[78] Art. 57(1)(f) GDPR.

[79] DPC, Annual Report 2020, 14, available on https://www.dataprotection.ie/sites/default/files/uploads/2021-02/DPC%202020%20Annual%20Report%20%28English%29.pdf accessed 22 March 2021.

[80] 'Advice for individuals considering making a whistleblowing disclosure' available on https://ico.org.uk/media/report-a-concern/documents/1042550/protection_for_whistle_blowers.pdf accessed 22 March 2021.

GDPR, thereby eliminating the distinction between the two notions.[81] The concept is broadly understood so that a whistleblower can be recognized as having an indirect interest. In this way, the *Agencia Española de Protección de Datos* (AEPD) accepts that reports to the police and reports of harassment in the workplace may, if the facts include a data protection breach, give rise to a 'reclamacion' before it.[82] The articulation between these different reporting systems is regulated by protocols between the relevant public bodies. Within the framework of the priority channel created for reporting the dissemination of sensitive content on the Internet and requesting its removal, the AEPD also expressly recognizes that reporting can be carried out by 'victims', but also by third parties who have knowledge of these situations.[83]

Next to the complaint, the national DPA may also conduct an inquiry without a complaint, but only on its own volition.[84]

In this case, the DPA can clearly act on the basis of a report from a whistleblower. Nothing in the GDPR prevents an individual from reporting a violation of the data protection rules to the DPA.

But the rules to follow will be different depending on whether there is a whistleblowing law in force in the area of data protection or not.

We have seen that in the UK and Ireland, the whistleblower may already contact the ICO and the DPC to report breaches in the area of data protection. Where possible, the ICO gives restricted feedback about any action taken as a result of a public interest disclosure.[85] On its website, the DPC mentions that all disclosures are taken seriously and all efforts are made to address them appropriately.[86] It acknowledges disclosures within 14 days of receipt and will assess the information provided.

In France, the *Commission nationale de l'informatique et des libertés* (CNIL) does not expressly contain a reference in its Annual Report to the Loi Sapin II, which protects broadly 'civic' whistleblowers who report or disclose, in an unselfish way and in good faith, information on threats or harm to the public interest. However, it puts on the same level the 'plainte' (complaint) and the 'signalement' (reporting). According to the report, the complaint and the reporting are the main source of information of the CNIL.[87] Almost 43 per cent of the checks carried out take place in the frame of investigations on the basis of a complaint or a reporting. Moreover, it should be noted that the CNIL has formerly put in place a platform for reporting on its website in the context of the previous electoral campaigns.[88]

In Belgium, it is more complicated to get a sense of what is happening in relation to whistleblowing. In the absence of any specific text, there is no obligation for the Belgian DPA to

[81] AEPD, Memoria 2019, 79 and 106, available on https://www.aepd.es/sites/default/files/2020-05/memoria-AEPD-2019.pdf accessed 20 March 2021.

[82] AEPD, Memoria 2019, 23.

[83] AEPD, Memoria 2019, 22.

[84] See for instance Art. 110 of the Irish Data Protection Act.

[85] 'Advice for individuals considering making a whistleblowing disclosure', 3, available on https://ico.org.uk/media/report-a-concern/documents/1042550/protection_for_whistle_blowers.pdf accessed 23 March 2021.

[86] 'Making a Protected Disclosure to the DPC', https://www.dataprotection.ie/en/who-we-are/corporate-governance/making-protected-disclosure-dpc accessed 23 March 2021.

[87] CNIL, Rapport d'activité 2019. Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles, 89, available on https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf accessed 20 March 2021.

[88] See https://www.cnil.fr/fr/webform/signalement-campagne-electorale accessed 22 March 2021.



report annually on whistleblower disclosures. However, pursuant to the Article 58 of the 'Loi du 3 décembre 2017 portant création de l'Autorité de protection des données', any person may submit a complaint ('plainte') or request ('requête') to the Autorité de protection des données.

Once the DWB is implemented and in force in all the Member States, each DPA will be required to 'diligently follow up on the reports and provide feedback to the reporting person within a reasonable timeframe not exceeding three months, or six months in duly justified cases'.[89] Competent authorities will need to publish on their websites in a separate, easily identifiable and accessible section useful information for submitting a report.[90] Moreover, persons reporting violations to DPA will be expressly protected against retaliation.[91]

It should be noted that whistleblowers do not only play a role in the detection of violations of data protection rules they also complement the coercive action of the DPA.

Penalties including administrative fines may be now imposed for some infringements of the GDPR in order to strengthen the enforcement of the rules.[92] These penalties will apply in addition to, or instead of appropriate measures imposed by the supervisory authority (e.g., reprimand).[93] But as others have noted, 'carrots' and 'soft law' need to be backed up by 'sticks' and 'hard law'.[94] By reporting violations to the DPA, whistleblowers allow the latter to be the 'stick' by applying where appropriate the penalties laid down by the GDPR. But they act also ahead as a 'carrot' because the threat to be reported may be sufficient to encourage data controllers to comply with the data protection rules.[95] According to the same rationale of 'naming and shaming', whistleblowing has the effect of increasing transparency on misconducts in order to trigger a reaction, by the state or by the market.[96]

### 3.2.2 A (new) compliance tool for data controllers

By enshrining the accountability principle, the GDPR raises expectations from the data controllers and the data processors. They have the primary responsibility to enforce the rules in the area of data protection.[97] This broader responsibility goes hand in hand with a renewed vigilance from data protection actors.[98] While each staff member is likely to help them in the implementation of the accountability principle, the European lawmaker preferred to institu-

[89] Art. 11(1) (c) and (d) DWB 2019.

[90] Art. 13 DWB 2019.

[91] Art. 21 DWB 2019.

[92] See Art. 83 GDPR.

[93] Recital 148 GDPR.

[94] D. Wright and P. De Hert, 'Introduction to Enforcing Privacy' in D. Wright and P. De Hert (eds), *Enforcing Privacy Regulatory, Legal and Technological Approaches* (Springer 2016), 4. For an illustration of the benefits of a mix between hard law tools, as monetary penalties, and soft law tools as 'naming and shaming', see namely H. Grant and H. Crowther, 'How Effective Are Fines in Enforcing Privacy?' in D. Wright and P. De Hert (eds), *Enforcing Privacy Regulatory, Legal and Technological Approaches* (Springer 2016), 287–305.

[95] This is true if the threat is credible and so if the whistleblower may speak out without fear of reprisals. The whistleblower has to be able to report breaches of data protection rules.

[96] See A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale: de la complaisance à la vigilance* (Larcier 2021), 362.

[97] C. de Terwnangne, K. Rosier and B. Losdyck, 'Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel' (2016) R.D.T.I. No 62, 27.

[98] For an illustration, see for instance Art. 28(3)(h) subpara. 2 GDPR.

tionalize vigilance around one staff member in particular, the Data Protection Officer.[99] This reporting professional is made mandatory in some cases.

#### *3.2.2.1 Accountability principle*

The DWB shed new light on three measures of the GDPR in particular: the data protection impact assessment, the drawing-up of codes of conduct and the personal data breach notification.

Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller must, prior to the processing, according to Article 35(1) of the GDPR, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data ('Data Protection Impact Assessment' (DPIA)). A single assessment may address a set of similar processing operations that present similar high risks.

In the light of the '*Cambridge Analytica*' scandal, it could be recommended to easily make available to staff members the impact assessment carried out by the controller in order to prevent public scandals.[100] The breaches exposed in the '*Cambridge Analytica*' scandal concerned cases where an impact assessment was mandated.[101] Just like the controller and the processor need to support the DPO in performing his or her tasks in accordance to Article 38(2), it could be expected to facilite the duty of vigilance implicitly recognized to the staff members. A worker could blow the whistle on the basis of the information contained in a DPIA.

In order to offer some legal certainty while recognizing a degree of scalability, the GDPR provides for a number of tools demonstrating data protection compliance, such as codes of conduct.[102] In order to have a positive impact from a data protection perspective, the code of conduct must be approved in accordance with the procedure established by Article 40(5) of the GDPR. According to Article 40(2) of the GDPR, codes of conduct may specify, among other things, the accountability measures and procedures and the measures to ensure security of processing operations. Beyond the measures explicitly listed by the GDPR, it should be noticed that according to the Article 29 Data Protection Working Party (WP29), which is now replaced by the European Data Protection Board (EDPB), 'accountability measures' may include among others the establishment of an internal complaints handling mechanism and the setting up internal procedures for the effective management and reporting of security breaches.[103]

Pursuant to Article 40(4) of the GDPR, codes of conduct must also contain 'suitable mechanisms to ensure that those rules are appropriately monitored and that efficient and

[99] It should be noticed that pursuant to Art. 37(6) of the GDPR, the functions of the DPO may be externalized too.

[100] Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law, Commission Staff Working Document, Brussels, 23 April 2018, 26–27.

[101] Art. 35(3) GDPR sets out three hypothesis in which the carrying out of an impact assessment is mandatory.

[102] To have a positive impact from a data protection perspective, the code of conduct must be approved in accordance with the procedure established by Art. 40(5) of the GDPR.

[103] WP29, Opinion 3/2010 on the principle of accountability, WP 173, 13 July 2010, 11–12.



meaningful enforcement measures are put in place to ensure full compliance'.[104] According to the EDPB, mechanisms may include 'policies for reporting breaches of its provisions' such as whistleblowing mechanisms.[105] For a company, the amending of codes of conduct in order to add a whistleblowing mechanism is a way to show the willingness (real or not) to strengthen enforcement with rules whose non-observance has been exposed in the frame of a scandal. In the aftermath of the '*LuxLeaks*' scandal, many audit firms thus approved codes of conduct encouraging reporting of misconducts in tax matters.[106]

Finally, the controller should notify the personal data breach to the supervisory authority as soon as he or she becomes aware that a personal data breach has occurred according to Article 33(1) of the GDPR.[107] Controllers may become aware of the occurrence of a data breach thanks to the vigilance of not only the DPO, but also of a potential whistleblower. The rule also applies in case of a security incident to whose notification is, for some entities, required in accordance with the 'NIS' Directive.

Staff members are aware of what is happening at work and then are well placed to escalate the matter up the chain of command acting in this way in the public interest. Of course, this issue is irrespective of the responsibility issue, only the DPO is required pursuant to the GDPR to monitor compliance. In reaction to the '*Cambridge Analytica*' scandal, *Facebook* strengthened, its 'Bug bounty programme processes' which allows users with an expertise in security to report a security vulnerability on *Facebook* or on another company of the *Facebook* group (such as *Instagram* and *WhatsApp*). But the purpose of such a program is more to improve the company's image than to improve compliance with law.

#### *3.2.2.2 Compliance monitoring by the Data Protection Officer*

Article 39 of the GDPR mainly entrusts DPOs with the duty to monitor compliance with the GDPR. In the performance of this task, the DPO needs to be able to count on the vigilance of the employees and the data subjects and where appropriate of potential clients. In this regard, Article 38(4) of the GDPR sets out that '[d]ata subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR'. But, the question is how whistleblowers fit into this reporting process.

Like the Compliance Officer and the Anti-Money Laundering (AML) Compliance Officer, who receive concerns of whistleblowers in financial matters, the DPO is a new function of '(privacy) compliance'.[108] It should logically receive the concerns from whistleblowers in data protection matters. The DPO is indeed the most 'appropriate person' to receive information on breaches concerning data protection, acting therefore as the WBO. When the DPO and the WBO are a single natural person, we have nonetheless seen that this situation might give rise

[104] EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Version 2.0, 4 June 2019, 16.

[105] EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Version 2.0, 4 June 2019, 16.

[106] CFE Tax Advisers Europe, Opinion Statement PAC 2/2017 on the European Commission public consultation on protection of whistleblowers, issued by the CFE Professional Affairs Committee, submitted to the European Commission on 17 May 2017, 4, available on http://taxadviserseurope.org accessed 20 October 2020.

[107] See also Recital 85 GDPR.

[108] J. Terstegge, 'EU Watch: Data protection and the new face of privacy compliance' (2013) 6 *Business Compliance* 34–43.

to a conflict of interests. A case-by-case evaluation should be conducted in such situations to determine whether combining roles indeed is undesirable.

In any case, the DPO remains the right hand of the supervisory authorities in that the DPO 'facilitates' compliance with the provisions of the GDPR within the organization of the controller[109] and acts as a contact point for the supervisory authority.[110] In the words of the Belgian *Autorité de protection des données* and its Investigation Department, the DPO is indeed, according to the Strategic Plan, 'an ally, an ambassador, in order to help accomplish the mission of the DPA in the field'.[111]

Furthermore, he or she may also act '*as a whistleblower*' since the DPO must 'directly report to the highest management level of the controller or the processor'[112] and must 'cooperate with the supervisory authority'.[113] But if the DPO acts 'as a whistleblower',[114] they are not exactly whisteblowers because it is part of their job to talk. They are professionally responsible if they do not speak when they should. However, the fact remains that the DPO is a 'professional' or 'institutionalized' reporting person as well as the journalist and the policeman in so far as blowing the whistle falls within their functions.[115] The safeguards in terms of independence and confidentiality around the function of the DPO are there precisely to allow the DPO to speak out freely and to blow the whistle, where appropriate, in the place of a worker which would be afraid to take the floor.[116]

Even if the law evolves a lot, a culture of secrecy and omerta still prevails in many companies. The European lawmaker saw moreover fit to provide that the DPO shall not be 'dismissed or penalised by the controller or the processor for performing his tasks'.[117] The immunity enjoyed by the DPO looks like the one that will be enjoyed by the whistleblower in the future.

[109] On this role of 'facilitator', see namely K. Rosier, 'Délégué à la protection des données: une fonction multifacette' in K. Rosier and C. de Terwangne (eds), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie* (1st edn, Larcier 2018), 559–592. See also WP29, Guidelines on Data Protection Officers ('DPOs'), 16/EN WP 243 rev.01, Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, 5.

[110] Art. 39(1)(e) GDPR.

[111] APD, Rapport annuel 2019, 26, available on https://www.autoriteprotectiondonnees.be/publications/rapport-annuel-2019.pdf accessed 23 March 2021.

[112] Art. 38(3) GDPR.

[113] Art. 39(1)(d) GDPR.

[114] For a rapprochement between the function of whistleblower and the function of DPO, see 'L'APD rappelle l'importance de l'indépendance du DPO en prenant la décision de sanctionner Proximus', Digilex, 2 juin 2020, available on https://digi-lex.be/index.php/2020/06/02/lapd-rappelle-limportance-de-lindependance-du-dpo-en-prenant-la-decision-de-sanctionner-proximus/ accessed 17 March 2021.

[115] Jean-François Gayraud showed that the police and the journalists are forms of institutionalised reporting. See J.-F. Gayraud, *La dénonciation* (P.U.F. 1995), 44–50.

[116] By comparison with Enron and WorldCom cases, which motivated the implementation of whistleblowing mechanisms in the financial sector in the US, we can see that the whistleblower, in both cases, held a position of decision-making. Sherron Watkins was Vice President of Enron Corporation' business development and Cynthia Cooper was Vice President of WorldCom's Internal Audit Department. See A. Lachapelle, *La dénonciation à l'ère des lanceurs d'alerte fiscale: de la complaisance à la vigilance* (Larcier 2021), 181–182.

[117] Art. 38(3) GDPR. About the protection of the DPO against reprisals, see namely K. Rosier, 'Délégué à la protection des données: une fonction multifacette' in K. Rosier and C. de Terwangne (eds), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie* (1st edn, Larcier 2018), 582–583.



In this way, the EU lawmaker recognizes that the DPO is not the only person right to speak up. Blowing the whistle is a collective concern.

## 4. CONCLUSION

While representing a key player in vigilance mechanisms,[118] 'whistleblowers' have not been given any role in the 'governance structure' established by the initial 'Data Protection Directive' and by the GDPR.

However we have shown that by putting the focus on the awareness raising of members of staff, the GDPR creates a setting for the development of whistleblowing. By promoting a new corporate culture based on transparency and reporting, the GDPR further initiates progressive decentralization of law enforcement in Europe. In order to perform their duties, all the key actors of the governance system need to rely on the vigilance of the staff members which are best placed to freely raise public interest concerns. But we cannot expect them to blow the whistle without being protected.

Above all, we have seen that the DPA certainly receives disclosures and initiates investigations on their basis. Indeed, there is no rule in any European country that prohibits a public authority from considering information received incidentally from a 'source of information'. But the problem is that this source might be in a vulnerable position in countries where there is no legal framework and therefore, no protection.

## ACKNOWLEDGEMENTS

The author would like to give warm thanks to Jean Herveg, Michèle Ledger and Yves Poullet for proofreading this chapter.

[118] F. Chateauraynaud and D. Torny, *Les sombres précurseurs. Une sociologie pragmatique de l'alerte et du risque*, (2nd edn, EHESS 2013).