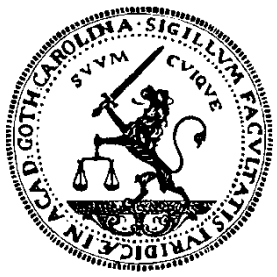

FACULTY OF LAW

Lund University

Amanda Espinasse

The conflicts between the Whistleblower Protection Directive and the GDPR

COVID-19, a legal basis to infringe on the rights of the data subject in order to secure the protection of whistleblowers?

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program

30 higher education credits

Supervisor: Annegret Engel

Semester of graduation: Spring semester 2020

Contents

Summary

On the 7th of October 2019, the Council of Europe published a press release, "*Better protection of whistle-blowers: new EU-wide rules to kick in in 2021"*. In the press release, the Council of Europe stated that a new directive, the Whistleblower Protection Directive, would increase protection of whistle-blowers. At the same time, companies and authorities were still struggling with the complicated regulations of the General Data Protection Regulation (GDPR). The question that caught my attention to the subject was therefore, *would it be possible to work in compliance with both the Whistleblower Protection Directive and the GDPR?*

My research questions are; *1. What are the conflicts between the Whistleblower Protection Directive regarding reporting channels and the GDPR? 2. What are the conflicts between the Whistleblower Protection Directive regarding investigations and the GDPR? 3. Is it possible for companies to work in compliance with both the Whistleblower Protection Directive and the GDPR? 3.(a) If the third question is answered in the affirmative, how shall they act?*

When investigating the conflicting articles, it is clear that they protect two different interests. On the one hand, the whistleblowers that otherwise may suffer from retaliation. On the other hand, the data subjects that otherwise may have their personal data unjustly collected and processed.

Through the thesis I highlight five different conflicts. These are presented descriptively and analysed continuously together with literature, reports and articles. The majority of the conflicts are solved by prioritizing the protection of whistleblowers due to public interest. COVID-19 is one example that I use to show how crises like pandemics prove that anti-corruption is in the public interest.

Sammanfattning

Den 7:e oktober 2019 publicerade Europarådet ett pressmeddelande, ”*Better protection of whistle-blowers: new EU-wide rules to kick in in 2021”.* I pressmeddelandet framgick det att ett nytt direktiv, Visselblåsardirektivet, skulle komma att förbättra skyddet för visselblåsare. Samtidigt arbetade företag och myndigheter fortfarande hårt för att anpassa sig till den relativt nya dataskyddsförordningen, GDPR. När jag läste detta pressmeddelande väcktes därför en fråga hos mig, s*kulle det bli möjligt att arbeta utifrån både direktivet och förordningen samtidigt?*

Mina frågeställningar är; *1. Vilka konflikter finns det mellan Visselblåsardirektivet kopplat till rapporteringskanaler och GDPR? 2. Vilka konflikter finns det mellan Visselblåsardirektivet kopplat till utredningar och GDPR? 3. Är det möjligt för företag att arbeta utifrån både direktivet och förordningen samtidigt? 3.(a) Om tredje frågan besvaras jakande, hur ska de arbeta?*

När jag undersökt konflikter mellan direktivet och förordningen har det blivit tydligt att de skyddar två olika subjekt. Det ena skyddar visselblåsare som annars kan råka ut för repressalier. Det andra skyddar datasubjekt som annars kan få sin personliga data samlad och använd i strid mot GDPR.

I examensarbetet belyser jag fem olika konflikter. Dessa presenteras och analyseras kontinuerligt tillsammans med litteratur, rapporter och artiklar. Majoriteten av konflikterna löses genom att prioritera skyddet för visselblåsare motiverat utifrån samhällsintresse. Jag använder bland annat COVID-19 för att exemplifiera hur kriser, såsom pandemier, visar att antikorruption är ett samhällsintresse.

Preface

Sista terminen i Lund blev minst sagt inte som den var tänkt. Jag minns att jag sa i januari att ”*Det enda som kan förstöra denna våren är något oförutsebart*”. Corona blev minst sagt något oförutsebart som förstörde våren. Dock kan jag med handen på hjärtat säga att pandemin fört med sig vissa fina saker, och då syftar jag inte på att den löste en av mina frågeställningar för mitt examensarbete. Pandemin har fått mig att uppskatta mycket jag tidigare alltid tagit för givet, och för det är jag tro det eller ej evigt tacksam.

Tack till mina vänner i Lund som gjort studenttiden till den absolut bästa, och till mina barndomsvänner som alltid stöttat och peppat mig.

Tack till min familj för att ni alltid funnits där och trott på mig.

Grazie Chiara Ragni per avermi inspirato per il mio saggio. Lei è una professoressa e un vero modello per me.

Last but not least, thank you to my supervisor Annegret Engel for helping me with essential and prized thoughts.

Abbreviations

Article 29 Working Party	Article 29 Data Protection Working Party.
CoE	Council of Europe.
CJEU	Court of Justice of the European Union.
Data Protection Directive	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.
DPA	Data Protection Authority.
DPIA	Data Protection Impact Assessment.
EDPB	European Data Protection Board.
EDPS	European Data Protection Supervisor.
EU	European Union.
FEUF	Treaty on the Functioning of the European Union.

GDPR	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).
OECD	The Organisation for Economic Co-Operation and Development
TEU	Treaty on the European Union.
TI	Transparency International.
UNODC	United Nations Office on Drugs and Crime.
Whistleblower Protection Directive	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.

1 Introduction

1.1 Background

"The EU is committed to having a well functioning democratic system based on the rule of law. That includes providing a high level of protection across the Union to those whistle-blowers who have the courage to speak up. No one should risk their reputation or job for exposing illegal behaviours." Anna-Maja Henriksson, Finland's Minister of Justice, 2019.[1]

On the 7th of October 2019, The Council of Europe[2] published a press release, "*Better protection of whistle-blowers: new EU-wide rules to kick in in 2021"*. The CoE stated that the European Union[3] needs to guarantee a high level of protection for employees reporting breaches of EU law in order to ensure public health, nuclear safety and financial services. The protection would be enforced with a new directive[4], *Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law*.[5] The Member States have until October 2021 to implement the directive. The CoE accentuated that the Whistleblower Protection Directive would include high requirements regarding safe channels for reporting breaches, both in public and private authorities, internal and external. At this time, according to the CoE, only ten

[1] The Council of Europe, *Better protection of whistle-blowers: new EU-wide rules to kick in in 2021,* 2019.
[2] Hereinafter *CoE.*
[3] Hereinafter *EU.*
[4] An EU-directive, unlike a regulation, does not have direct effect except in certain exceptional situations, i.e. the case of *Van Duyn v Home Office*, C-41/74. Directives contain a result that shall be incorporated in the Member States in a certain time. It is up to the Member States how this shall be done. See Article 4.3 of the Treaty on the European Union (Hereinafter *TEU).*; Article 288 of the Treaty on the Functioning of the European Union (Hereinafter *FEUF)*. See also Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 178 ff.
[5] Hereinafter *the Whistleblower Protection Directive.*

of the Member States of the EU had comprehensive laws protecting whistle-blowers.[6]

However, the imposition of a new directive does not make older regulations vanish. It has already been a challenge to work in compliance with the *Regulation (EU) 2016/679 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*[7]. As if this has not been difficult enough, companies will now have to work in compliance with both the GDPR and the new directive. Pursuant to Article 17 of the Whistleblower Protection Directive, any processing of personal data carried out pursuant to the directive shall be carried out in compliance with the GDPR.[8]

> *"The directive's interaction with GDPR, particularly in relation to data subject rights, may finally resolve most of the ambiguity and help to establish GDPR definitions consistent across all Member States." Vera Cherepanova, experienced compliance officer, 2019.*[9]

Well, will it?

1.2 Purpose and Aim

In this thesis, conflicts between the Whistleblower Protection Directive and the GDPR will be observed. The purpose is to advice companies in if, and in that case how, it is possible to work in compliance with both the

[6] The Council of Europe, *Better protection of whistle-blowers: new EU-wide rules to kick in in 2021,* 2019.
[7] Hereinafter *GDPR.* A regulation is applicable in all the EU Member States and has direct effect. Unlike directives, they do not need to be incorporated in the Member State laws, since it already has legal force in itself. See Article of the 288 FEUF. See also Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 177 f.
[8] See also Motive 83 of the Whistleblower Protection Directive.; The European Data Protection Supervisor, *Whistleblowing*.; The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 4.
[9] Cherepanova, *Yes, GDPR has already changed the whistleblowing landscape,* 2019.

Whistleblower Protection Directive and the GDPR, in order to protect whistleblowers and act preventively regarding anti-corruption.

To fulfil this aim, the following research questions will be examined:

1. What are the conflicts between the Whistleblower Protection Directive regarding *reporting channels* and the GDPR?
2. What are the conflicts between the Whistleblower Protection Directive regarding *investigations* and the GDPR?
3. Is it possible for companies to work in compliance with both the Whistleblower Protection Directive and the GDPR?
    (a) If the third question is answered in the affirmative, how shall they act?

1.3 Method and Material

The outset for this thesis has been parts of EU legal method. The EU legal method is an umbrella term for the methods used by the Court of Justice of the European Union[10]. Consequently, it is not reliable to use the method broadly, since there are several methods of interpretation that fit into the phenomena of EU legal method. Therefore, I will present which methods of EU legal method I have used when I have written this thesis.[11]

One basic premise of the EU legal method is you shall not interpret a regulation only by the letter of the law. You shall also look at the context and the purpose of the regulation. With this outset, it is possible to use different methods for interpretation, i.e. autonomous interpretation, analogical interpretation, teleological interpretation and systematic interpretation.[12]

[10] Hereinafter *CJEU*.
[11] Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 158 f.
[12] Ibid.

First, since the legal sources of the EU often are ambiguous, fundamental principles can be used to fill these gaps.[13] In this thesis, I have therefore used the proportionality principle to evaluate what interests to prioritize in cases of conflicting interests of the directive and the regulation.

Secondly, in some parts, I have used interpretation by the letter of the law. This is not a recommended method since, as mentioned above, the EU legal acts shall not be interpreted solely by the letter of the law. I am well aware of this and consequently, in these parts, I have complemented the interpretation with the proportionality principle and in the light of their purposes.[14]

Thirdly, and most importantly, I have written the majority of the thesis with a teleological method. This is the most commonly used method by the CJEU. The method aims to interpret a provision by the purpose of the provision. This is a method that is suitable to use when a context or content of a provision is unclear. In this case, the context of the Whistleblower Protection Directive is unclear in relation to the GDPR. Also, the content both of the Whistleblower Protection Directive and the GDPR is ambiguous. Typically, this method is used in order to compromise different interests of the Member States, but it is also used to encourage the aim of a regulation, fill out uncertainties and avoid negative consequences that may otherwise occur. The uncertainties of the directive and the regulation have accordingly been interpreted in the light of their purposes, and the purposes have then been compared in relation to each other.[15]

In addition to the parts of EU legal method, I have been using influences of a comparative legal method. Pursuant to Michael Bogdan, comparative legal method is in general usable for all types of comparative assessments of all

[13] Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 163 ff.
[14] Ibid., p. 159.
[15] Ibid., p. 158 f. & 168.

types of legal sources.[16] Bogdan believes comparative legal method is crucial due to EU law in order to assess the effect of different legal sources which comprises the same area.[17] The influences of the method has been conducted with a material micro approach. Meaning, an assessment of the material content of isolated parts of the legal sources.[18] In order to achieve a successful compartment, there must be an unified part of the objects of compartment, called *tertium comparationis*.[19] In this case, the directive and the regulation are in conflict since they regulate the same areas, i.e. the collection of personal data. With this said, I have *not* been using an absolute comparative legal method, since I have not compared sources of law of different countries or systems.[20] The analysis is however conducted with influences of a comparative legal method since two different sources of law, the directive and the regulation, are being compared. There are also influences of a comparative legal method where i.e. legislative acts of Sweden and Germany are brought up. However, the method is neither here used absolute, since the aim of this thesis is not to present differences and similarities in different countries. I only use these countries to exemplify laws in order to create an understanding for the need of the new directive.

The thesis is written with a continuous analysis. Consequently, the chapters include both referred information as well as my own thoughts and conclusions. This has been suitable for two reasons. First, my research questions have not been examined before. Because of this, there is not much descriptive material from earlier research to present independently. Secondly, since I have compared the Whistleblower Protection Directive and the GDPR it has been more suitable to present the conflicting articles together with my thoughts on the conflicts.

---

[16] Bogdan, *Komparativ rättskunskap,* 2003, p. 18. Note that it is controversial if the method also can be defined as a legal science. See Ibid., p. 22 f. In this thesis however, it is only being used as a complement to other methods for research regarding EU-law.
[17] Ibid., p. 33 f.
[18] Ibid., p. 56 f.; Samuel, *An Introduction to Comparative Law Theory and Method,* 2014, p. 50 ff.
[19] Bogdan, *Komparativ rättskunskap,* 2003, p. 57 f.
[20] Ibid., p. 10.; Samuel, *An Introduction to Comparative Law Theory and Method,* 2014, p. 50 ff.

The material I have used has mainly been the Whistleblower Protection Directive and the GDPR. Both the articles and the motives. Furthermore, I have been using guidelines from authorities to present different interpretations. Articles have been used in order to emphasize various perspectives on the controversial parts. Literature has mainly been used in order to present theories about strategies regarding anti-corruption and tools for interpretation of the GDPR. Note that I have been using some sources that were published *before* the Whistleblower Protection Directive and the GDPR came. These have *not* been used in order to present the legal position, but to substantiate arguments regarding protection of different interests.

1.4 Disposition

In the first chapter, I attempt to give the reader an insight in the preconditions and premises of the thesis regarding i.e. purpose, material and method. The chapter also includes reflections of the value of the thesis.

In the second chapter, I present quintessential parts of the directive on the Whistleblower Protection Directive and the GDPR, i.e. the purposes and definitions. Furthermore, I examine different kinds of corruption and investigate whether anti-corruption should be counted as a public interest or not.

In the third chapter, I examine the conflicts regarding reporting channels of the Whistleblower Protection Directive and the GDPR. *In the fourth chapter,* I examine the conflicts regarding investigations of the Whistleblower Protection Directive and the GDPR. Both of the chapters are written with continuous analysis by accentuating the conflicts, presenting the content of the articles, investigating different interpretations and providing a solution.

In the fifth chapter, I conclude by answering my research questions in order to expressively fulfil the purpose of the thesis. Furthermore, future research is requested.

1.5 Demarcations

The Whistleblower Protection Directive is limited to reporting channels and investigations. The demarcation is necessary mainly because of the space of the thesis. Furthermore, reporting channels and investigations will be the predominant parts of the practical work due to the directive. Therefore, I found those parts as the most important and interesting for companies to have examined. Consequently, I will not present further information regarding the directive or the regulation.

I will *not* compare the EU acts with domestic law in one specific Member State. Some domestic law will be presented as *examples*, i.e. Germany, which is one of the Member States that will have to alter a lot due to the directive.[21] Sweden will be brought up since it is counted as one of few Member States with comprehensive protection of whistleblowers regardless of the directive. [22] By presenting these examples I aim to increase insight in *how* laws protecting whistleblowers can be formulated, but not to examine differences and similarities.

I will not examine the founding principles and the acts of EU law. My outset is that the reader of this thesis has basic knowledge of the EU acts.[23] I will however present the proportionality principle since it is used continuously in the analysis.

The perspective for this thesis is *for* companies in order to *help* companies. My aim is to explain how to act preventively and thoughtfully in order to avoid non-compliance with the GDPR once the directive is implemented. I

[21] The Data and Technology group of Baker McKenzie Germany, *The new EU Whistleblowing Directive: Considerations from a German compliance, employment and data protection law perspective*, 2020.
[22] The Council of Europe, *Better protection of whistle-blowers: new EU-wide rules to kick in in 2021,* 2019.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 21.
[23] For readers without basic knowledge in EU law I recommend the European Parliament, *Sources and scope of European Union law,* 2020.; Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 39-133.

would hereby also like to notify that I will not examine provisions of accountability and data protection impact assessment[24] in detail, since it is not a main part of my research questions. I will however mention them as *excursus* since they are important aspects of working in compliance with the GDPR.[25] Note that this thesis of course can be used for other purposes, i.e. for the Member States when incorporating the directive in their international laws.

Other limitations will be presented continuously through the thesis. This is in order to help the reader understand other perspectives and problems in relation to the subject. Please note that I will provide the reader with further information and recommended literature in some footnotes.

1.6 Previous research

While writing this thesis I have come to understand that there is a lack of research in the area. Since the directive on Whistleblowing protection is new there is not much written regarding the directive, and accordingly neither compared to the GDPR.

There is however a lot written on whistleblower protection and anti-corruption. I will use this previous research to substantiate my arguments connected to the importance of protecting whistleblowers and that anti-corruption is a public interest.

Regarding previous research on the GDPR, the Article 29 Data Protection Working Party[26], has written a great number of guidelines regarding interpretation of the articles. The reports have been helpful in order to understand and to interpret provisions of the GDPR.

---

[24] Hereinafter *DPIA*.
[25] Article 5.2 of the GDPR.; The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 11 f.
[26] Hereinafter *Article 29 Working Party*. The group was set up under Article 29 of the *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* (Hereinafter Data Protection Directive). It is an independent European advisory body on data protection and privacy. See Article 30 of the Data Protection

1.7 Value of research

The reliability of the research is high for two main reasons. First, the method is accurately presented, which enhances the result to be the same in repeated investigations. Secondly, the majority of the information has two or more sources to substantiate. Validity is ensured by expressively presenting and examining the research questions in the last chapter, and by that the thesis has been conducted with suitable methods and material.

An identified risk of lack of reliability is that the subject is un-explored. Consequently, the analytic parts mainly consist of my own conclusions and by that means there can be another approach with a different conclusion. I however respond to this possible critique by reminding the reader that my conclusions are based on reliable sources with the method provided.

I would like to reserve myself to two things regarding that the Whistleblower Protection Directive is not incorporated in the Member State Laws. Firstly, it is up to the Member States, not to the companies, to legislate in a manner that is in compliance with the GDPR. However, Member States tend not to take GDPR into consideration when legislating, since the GDPR has direct effect. I am because of this sure that the research *is* valuable because of one main reason. If the Member States, when incorporating the directive into their national laws, will not take GDPR into consideration and make it workable for the companies. The companies will then need guidelines on how to work in compliance with the new law as an effect of the directive, and the GDPR.

I would also like to reserve myself to the fact that the Whistleblower Protection Directive is not yet incorporated in Member State Laws. It can therefore be even harder for companies to work in compliance with the directive and the GDPR. I would also like to observe that there may be other conflicts regarding other articles than the ones I examinee in this thesis. The

Directive.; the Article 29 Data Protection Working Party, *Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen I artikel 7 I direktiv 95/46/EG,* 2014, p. 1.

research is however innovative since there is a lack of research in the area and is therefore valuable for companies in order to act in compliance, since it currently does not exist other recommendations.

2 Outsets

2.1 The Whistleblower Protection Directive

2.1.1 Whistleblowing

Whistleblowing can help in revealing and avoiding corruption. Although, only ten of the Member States have comprehensive laws protecting whistleblowers. I.e. France, Hungary, Sweden and Slovakia. Due to this, the Whistleblower Protection Directive will put high pressure on the Member States.[27]

Robert Vaughn – writer of *"The successes and failures of whistleblower laws"* – emphasizes that whistleblowing is something complex that needs to be seen through different perspectives. Vaughn believes it is crucial to understand that the complex characterization of whistleblowing has been problematic for a long time, i.e. to question authorities which was shown in Nazi Germany during World War Two. In the same way that inhabitants would not question orders of genocide, employees often do not question orders from employers.[28] Fear of questioning authorities has i.e. been proven in *the Milgram Experiment*.[29]

In 2011, Swedish lawyers agreed that the protection of whistleblowers was faulty and in need of improvement. They emphasized that employees are important for the employers, and that whistleblowers do not want to harm employers. In fact, reporting breaches is helpful for employers since it can

[27] The Council of Europe, *Better protection of whistle-blowers: new EU-wide rules to kick in in 2021,* 2019.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 21.
[28] Vaughn, *The Successes and Failures of Whistleblower Laws*, 2012, p. 1 ff.
[29] The test aimed to investigate when test persons would refuse to cause pain to someone, when they got directions from a third person with authority to do this. Milgram wanted to disprove the general thesis that World War Two was conducted because inhabitants of Germany were more disciplined than others. The result was that 65 percent of the test persons proceeded to cause maximal pain through electric shocks, although the person receiving them was screaming and begging not to be a part of the experiment anymore. The experiment has been criticized. However, it was acknowledged for recognizing the influence of authorities on people, to see the correspondence between individuals and institutions. Most importantly, it highlighted the importance of whistleblowing and the protection for federal employees. See Ibid., p. 10-17.

prevent the company to suffer from future financial crises that corruption can otherwise cause.[30]

Although Sweden has been counted as one of the best countries on whistleblower protection, the Swedish law protecting whistleblowers[31] is not comprehensive. It has during the years gotten a lot of critique. When the preparatory material of the law came a lot of commentators were critical. The Parliamentary Ombudsman was one of the sceptic commentators, stating the preparatory material of the Law had several deficiencies regarding protection of employees and applicability. The Swedish Chancellor of Justice was concerned if the Law would infringe the Constitutional law and the Association of Lawyers stated that the Law in itself would not provide proper protection.[32]

Note that The European Court of Human Rights has been an important part of the history of whistleblowing.[33] This shall however not be examined further due to the demarcations.

2.1.2 Whistleblower

In order to examine the Whistleblower Protection Directive, it a prerequisite to examine what a *whistleblower* is.

There is no legal universal definition of whistleblower. The word is however frequently used in reports and legal sources.[34] One of the first definitions was

[30] Slorach et al., *Rätten att slå larm – en handbok om yttrandefriheten på jobbet – råd för whistleblowers,* 2011, p. 11 f.
[31] Lagen (2016:749) om skydd mot repressalier för arbetstagare som slår larm om allvarliga missförhållanden.
[32] Viklund, *EU-direktiv om visselblåsare på väg,* 2019, p. 43 f.
[33] The jurisprudence from the European Court of Human Rights regarding the freedom of speech connected to whistleblowing is comprehensive. Furthermore, the European Convention on Human Rights has an impact on the EU Member States. See Larsson, *Skydd för visselblåsare i arbetslivet – en konstitutionell och arbetsrättslig studie,* 2015, p. 51.
[34] I.e. SOU 2014:31, *Visselblåsare – Stärkt skydd för arbetstagare som slår larm om allvarliga missförhållanden,* 2014.; Larsson, *Skyddet för visselblåsare i arbetslivet – en konstitutionell och arbetsrättslig studie,* 2015. p. 22.; The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016.

proposed by Janet Near and Marcia Miceli. Their definition was the following:

> *"[...] the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practises under the control of their employers, to persons or organizations that may be able to effect the action."*[35]

Whistleblower is not defined in the Whistleblower Protection Directive. There is however a definition of a "*reporting person*". The definition of a reporting person in Article 5.7 is the following:

> *"'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".*

The CoE's recommendation on the protection of whistleblowers has provided the following definition:

> *"Whistleblower means any person who reports or discloses information on a threat or harm to the public or private sector."*[36]

The definition above from the CoE, supplemented with the definition of reporting person from the Whistleblower Protection Directive, is the definition that will be used in this thesis. When comparing the definitions, it is notable that the Whistleblower Protection Directive includes public disclosure on breaches which the definition from the CoE does not. I will include this in my definition of whistleblower. I also count people who reports or discloses information internal and external, and people who report in purpose of retaliation.[37]

---

[35] Near & Miceli, *Organizational Dissidence: The Case of Whistle-blowing,* 1985, p. 4.
[36] The Council of Europe Recommendation CM/Rec (2014)7, *on the protection of whistle-blowers*, 2014, appendix (a).
[37] Note there are a lot of other definitions of whistleblower, i.e. Transparency International's definition. See Transparency International, *Whistleblowing in Europe legal protections for whistleblowers in the EU,* 2013.; Jubb's definition. See Jubb, *A restrictive Definition and Interpretation,* 1999 p. 83.

2.1.3 The purpose of the directive

"The purpose of this Directive is to enhance the enforcement of Union 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." Article 1 of the Whistleblower Protection Directive.

Employees at private or public organisations are often the first to acknowledge harms or threats to the public interest. The whistleblowers thus have an important role in exposing and preventing these harms or threats. The pivotal reason that potential whistleblowers do not take action is the fear of retaliation. It is accordingly crucial to protect whistleblowers in order to achieve transparency and acquire information that can disclose breaches of EU law.[38]

In order to achieve effective protection of whistleblowers, it is quintessential to safeguard secure reporting channels. The purpose is to eliminate and prevent breaches by secure protection of whistleblowers.[39] It is important to protect whistleblowers in the Member States with minimum standards since breaches often can be cross-bordered.[40]

2.1.4 The material scope and conditions

The directive is comprehensive and detailed. The public layer market will have to implement i.e. internal reporting channels, rules for protection of whistleblowers and certain employees with responsibility for reports of breaches. Accordingly, the Whistleblower Protection Directive will seriously affect the private sphere. Many of the Member States do provide protection

[38] Motive 1 of the Whistleblower Protection Directive. See also the European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 4.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 238 ff.
[39] Motive 3 of the Whistleblower Protection Directive. See also the European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 4.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 238.
[40] Motive 4 of the Whistleblower Protection Directive.

for whistleblowers, but not as extensive as the Whistleblower Protection Directive requires.[41]

Article 2.1 of the Whistleblower Protection Directive comprises protection for persons reporting breaches of EU law. I.e. breaches that fall within the scope of the EU acts that concern public procurement, financial services, protection of environment, public health and protection of privacy and personal data.[42]

Furthermore, there are conditions for the protection of reporting persons provided in Article 6.1 of the Whistleblower Protection Directive. Conditions regarding protection in the articles are that the reporting persons must have had reasonable grounds to believe that the information on the breach that they reported was true, and that the information was included in the scope of the directive. Subsequently, the reporting person must report internally in accordance with Article 7, externally in accordance with Article 10 or make a public disclosure in accordance with Article 15 of the Whistleblower Protection Directive.[43]

Pursuant to Article 6.2 of the Whistleblower Protection Directive, the Member States can decide to provide anonymous reporting channels. Reporting persons whom report anonymously, but later on are identified and suffer from retaliation, shall be provided protection as long as they meet the conditions of Article 6.1 of the Whistleblower Protection Directive.[44]

2.2 Corruption

2.2.1 The different kinds of corruption

The phenomena of corruption can appear as vague and with an ambiguity in how the word shall be used. The reason for this is that there is no universal definition of corruption. Despite this, it is accepted to use the word. The most

[41] Viklund, *EU-direktiv om visselblåsare på väg,* 2019, p. 47.
[42] See also Motive 6, 7, 10, 13, 14, 20, 52 & 62 of the Whistleblower Protection Directive.
[43] See also Ibid., Motive 32 & 33.
[44] See also Ibid., Motive 34.

common and acknowledged definition is the one provided by Transparency International[45]. TI means, that *corruption is the abuse of entrusted power for private gain*. Furthermore, this can occur on different scales and types. I.e. bribery, extortion, nepotism, embezzlement, conflict of interest, fraud and illegal gifts of money to political parties.[46]

When determining the level of corruption, it is possible to divide cases into *grand corruption* and *petty corruption.* Grand corruption takes place on the highest political level and is commonly involved in the private sector as well. Another phenomenon of this is *state capture*, meaning that the highest politicians in co-operation with private actors take over the state mechanism in order to earn private gains. Petty corruption is on a lower level, i.e. facilitation payments like smaller bribes to public officials.[47]

Corruption brings several negative consequences. It seriously undermines good governance since it erodes popular confidence in the public institutions, it favours inefficient economic decision making, it enhances unequal distribution of development gains and it stimulates the illegal export of capital. Furthermore, it disorders the economic decision-making process, since decisions in selecting the most economic suppliers will be obstructed. Consequently, corruption can cause allocative inefficiency by enable fewer effective actors to beat more effective ones through bribery rather than fair competition.[48]

Breaches of corruption are hard to reveal since both parts, i.e. the briber and the receiver of the bribe, want to conceal the corruption. Thus, reporting channels for whistleblowers are a prerequisite in order to disclose corruption.[49] Those who most likely are able to discover breaches are usually

[45] Hereinafter *TI.*
[46] Transparency International, *What is corruption?.* See also Cars & Engstam Phalén, *Mutbrott,* 2020, p. 21.
[47] Transparency International, *Grand Corruption*.; Transparency International, *Petty Corruption.*; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 21.
[48] Motive 15 the Whistleblower Protection Directive.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 21 ff.
[49] Cars & Engstam Phalén, *Mutbrott,* 2020, p. 238.

employees within the company involved with corruption. At the same time, it is hard to blow the whistle without decent protection, since it can appear disloyal to the employer and cause negative consequences.[50]

2.2.2 Anti-corruption as a public interest

2.2.2.1 Introduction

If anti-corruption is classified as a public interest or not is controversial. Public interest is not defined in the GDPR. However, some situations are exemplified, i.e. health care.[51] In the Whistleblower Protection Directive, it is stated that whistleblowers often are the first to detect threats or harms to the public interest. Therefore, it is important to protect them since their reports can safeguard the welfare of society. It is also stated that these breaches otherwise seriously may harm the public interests.[52] More specifically, it is specified in the motives of the Whistleblower Protection Directive, that procedures provided for follow-up on reports fall within the scope of an important objective of general interest of the EU and Member States. It aims to enhance enforcement of EU Law in areas where breaches can harm the public interest.[53]

According to the European Data Protection Supervisor[54], whistleblowers believe they act in the public interest when they are reporting on breaches.[55] The Organisation for Economic Co-Operation and Development[56] means that corruption seriously hazards the foundation of societies. The organisation has stated that corruption erodes the prerequisites of economies, societies and well-being of inhabitants. The consequences are distorted markets, financing of wars and terrorism and inequalities. Corruption is therefore according to

[50] Motive 1 of the Whistleblower Protection Directive. See also the European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 4.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 238.
[51] Motive 45 & 52 of the GDPR.
[52] Motive 1, 3, 5, 37, 84 & 108 of the Whistleblower Protection Directive.
[53] Ibid., Motive 84.
[54] Hereinafter *EDPS*.
[55] The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 4.
[56] Hereinafter *OECD*.

the OECD a threat to the global security, human dignity and to the environment. Corruption consequently creates a lack of trust in the public authorities which in turn setts preconditions for i.e. populism and nationalism.[57]

TI has several times ascertained that whistleblowers play an essential role in exposing corruption. This means that whistleblowers have helped in saving billions of euros in public funds and in rescuing countless of lives. TI has on multiple occasions emphasized the importance of protecting whistleblowers from retaliation like being fired, sued, assaulted or even killed, since they play this essential role.[58]

2.2.2.2 COVID-19 and pandemics

The COVID-19 virus has highlighted the question regarding anti-corruption as a public interest. TI believes it is. It means, that unless anti-corruption measures are implemented during crises like pandemics, corruption causes deaths.[59]

TI has stated that extraordinary outbreaks, like the COVID-19 pandemic, often reveal cracks in health systems and private sectors. According to TI this may deprive people of health care and seriously aggravate the consequences of pandemics. The virus has caused devastating numbers of infected and deaths all over the world. This extreme situation has been threatening medical care. Many countries have been lacking testing equipment and capacity for massive intensive care. Unfortunately, in earlier similar global crises like the Swine flu and Ebola, we have seen that natural persons can see their opportunity to profit from others' misfortune.[60]

---

[57] The Organisation for Economic Co-operation and Development, *In the Public Interest: Taking Integrity to Higher Standards – opening remarks at the 2017 OECD Global Anti-Corruption & Integrity Forum,* 2017.
[58] Transparency International, *Building on the EU directive for Whistleblower protection, analysis and recommendations,* 2019, p. 1.; Transparency International, *Whistleblowing in Europe legal protection for whistleblowers in Europe,* 2013.
[59] Transparency International, *Coronavirus sparks high risk of corruption across Latin America,* 2020.
[60] Ibid. See also that the Australian Commonwealth Ombudsman has been stating that corruption is an act that shall be disclosed in the public interest. See the Australian Commonwealth Ombudsman, *Agency guide to the public interest disclosure act,* 2016, p. 3.

2.2.2.3 Public procurement and price gougning

Corruption can cause *price gouging.* In fragile public procurement processes, corruption increases risks for suppliers to demand higher prices for i.e. health equipment knowing governments are in a great need of it. With anti-corruption arrangements price gouging can be prevented. Therefore, by having transparent and open processes, opportunities for corrupt companies to be contracted can be mitigated.[61]

TI believes that sharing information on deficiencies prevents price gouging. In order to make this possible, protection of whistleblowers is necessary. One example of this is the case of the whistleblower from Wuhan in China, Li Wenliang. Li Wenliang, a health care provider, was in an early stage trying to raise awareness regarding the severity of the up-coming COVID-19 pandemic. Unfortunately, he was silenced.[62] According to TI, this exemplifies why it is important to discuss vulnerabilities and protect whistleblowers in susceptible situations. Therefore, governments shall act with transparency, since it is in the public interest i.e. to prevent price gouging of medication.[63]

2.2.2.4 Misusing of beneficial rules

Price gouging is not the only problem caused by corruption in crises like pandemics. The Swedish Government has imposed new rules regarding short time layoff due to the COVID-19 virus. The aim of the regulation is to facilitate the economic situation that makes companies suffer from something non-expected, i.e. a pandemic. The regulation enables the opportunity for employers to demand employees to work less, but with close to full salary compensated by the Swedish Government. I.e. if an employee shall work 60% of their normal hours, the employee will have 92,5% of their regular salary. The Swedish Government then covers 75% of the total cost for the decrease of the working hours.[64]

[61] Transparency International, *Corruption and the Coronavirus – How to prevent the abuse of power during a global health pandemic,* 2020.
[62] Ibid.
[63] Ibid.
[64] Regeringskansliet, Finansdepartementet, *Om förslaget korttidspermittering,* 2020.

It has however been disclosed that companies have been misusing the beneficial rules. Tim Brooks, Head of Department of the Swedish Agency for Economic and Regional Growth, has accentuated the importance of recognizing these companies. According to the Swedish Minister of Finance, both authorities and politicians have noticed indications of the cheating. *How? Through whistleblowers.* Employees have been calling both authorities and politicians to reveal that they have been forced into a short time layoff while working full hours at the same time with threats of losing their employments.[65]

2.2.2.5 Conclusion

As presented above, anti-corruption is highly crucial for several reasons. I.e. since it is presented as a general public interest in the Whistleblower Protection Directive. One of the reasons for this is that corruption can infringe on public procurement negatively and may even cause deaths. This has certainly been shown in pandemics like COVID-19. *Accordingly, anti-corruption and protecting whistleblowers is according to me a public interest.*

I would like to note that I am aware of the fact that the European Data Protection Board[66] has communicated that COVID-19 shall *not* affect the GDPR. The argument is that even in exceptional times, protection of personal data of the data subject is important.[67] This is however not a contrary argument to my arguments, since the argument of the EDPB is connected to employers trying to trace infections between their employees. My outset is another, since it regards information from whistleblowers regarding anti-corruption. Furthermore, my argument is not based on COVID-19. I only use

[65] Blixt, *Visselblåsare har varnat för att bolag fuskar med korttidspermitteringar. Nu ryter finansministern till mot bolagen som planerar att inte följa reglerna,* 2020.
[66] Hereinafter *EDPB.*
[67] The European Data Protection Board, *Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak, 2020.* For interested readers, John Timmons and Tim Hickman at White&Case in London has written an article on COVID-19 and Data Protection Compliance. A result of the virus is that employers are collecting and processing new types of information that is counted as personal data. I.e. health status and travel locations. Accordingly, some issues connected to the GDPR has been identified due to the pandemic. See Timmons & Hickman, *COVID-19 and Data Protection Compliance,* 2020.

COVID-19 as an example of a situation where it becomes clear that anti-corruption is in the public interest.

Note, that when processing personal data lawfully due to performance of a task carried out in the public interest, the data subject shall be entitled to object to the processing. It should be an obligation for the controller to demonstrate that the interest of public interest overrides the interests of the data subject in such cases.[68]

2.3 The GDPR

2.3.1 Personal data

In order to understand *how* it is legal to collect and use personal data, it is crucial to define *what* personal data is. Personal data is defined in Article 4.1 of the GDPR. Pursuant to the article, *personal data is any information that is related to an identified or identifiable natural person*. An identifiable natural person is a person who can be identified directly or indirectly. Indirect identification can be done by i.e. economic identity, location data, identification number or social identity.[69]

2.3.2 The purpose of the regulation

The GDPR went into force on the 25th of May 2018.[70] The regulation aims to protect two interests. On the one hand, natural persons regarding collection and processing of their personal data. The right is also stated as a fundamental right pursuant to Article 8.1 of the Charter of the Fundamental Rights of the European Charter and Article 16.1 of the Treaty on the Functioning of the European Union. On the other hand, creating prerequisites for free movement of personal data in the EU.[71]

---

[68] Article 21.1 of the GDPR. See also Motive 69 & 156 of the GDPR.
[69] See also Motive 26 of the GDPR.; The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 6.; Frydlinger et al., *GDPR, Juridik, organisation och säkerhet enligt dataskyddsförordningen,* 2018, p. 33 f.
[70] Article 99.1 of the GDPR.
[71] Article 1 of the GDPR. See also Motive 1 of the GDPR.

In the motives of the GDPR, the importance of customising regulations in favour of natural persons is being emphasized.[72] This shall be done with consideration of public interest, other rights and the proportionality principle.[73] Pursuant to this, the CJEU has several times interpreted cases of personal data breaches in the light of other rights and freedoms and the proportionality principle.[74] I.e. *The Google Spain case*.[75]

Several organs have communicated guidelines in order to facilitate for companies to fulfil the regulation. Although, there are certain uncertainties in interpretation of the regulation.[76]

2.3.3 The material scope and conditions

The GDPR applies to collection and processing of personal data. Both manually and automated, Article 2.1 of the GDPR. The material scope is thus comprehensive and wide. The regulation applies for nearly all kinds of treatment of personal data. Exceptions are specified in Article 2.2 of the GDPR.[77]

Processing is defined in Article 4.2 of the GDPR with any operation or set of operations which is performed on personal data. Collection, storage, use and erasure is included in the definition.

The territorial scope is defined Article 3.1 of the GDPR. The territorial scope is processing of the personal data in the context of activities of an establishment of a controller in the EU, regardless if the processing takes place in the EU or not. Pursuant to Article 3.3 of the GDPR, the regulation

[72] Motive 4-6 of the GDPR.
[73] Ibid., Motive 4. See also Frydlinger et al., *GDPR, Juridik, organisation och säkerhet enligt Dataskyddsförordningen,* 2018, p. 29 f.
[74] See also Motive 4 of the GDPR.
[75] Case C-131/12, *The Google Spain case*. Please note that in this case, the CJEU thought the personal data rights were more important than the right to information of internet users and Google's economic interests. However, the case shows the type of considerations that shall be done. Another case where the CJEU did a similar consideration is the case of *Digital Rights Ireland*, C-293/12.
[76] I.e. GDPR.eu, *Everything you need to know about GDPR and compliance.*
[77] I.e. processing of the personal data in the course of an activity that is not in the scope of EU law. See IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guide,* 2017, 19 ff.

also applies when the processing of personal data takes place in a Member State while by a controller which is not established in a Member state.[78]

2.3.4 The proportionality principle

As mentioned above, the proportionality principle is a hugely consequential part of the GDPR.[79] The principle is in general essential when investigating the EU legal sources and for *how* it is legal to act. The principle requires that *an action shall not be more restrictive than what is necessary in order to reach the aim of the action*, *and the aim needs to be proportionate in relation to the effect.*[80]

2.3.5 Excursus: accountability

Crucial to keep in mind is that companies need to demonstrate how they are respecting the data protection obligations of the GDPR. This applies to all operations that include collection and processing of personal data. It is a general requirement that organisations need to be transparent and explicit regarding how they process the personal data while operating the reports from whistleblowers.[81]

According to the EDPS, there are certain questions that shall be considered:

a. How do we protect involved persons confidentiality?
b. What is the purpose of using the whistleblowing channel?
c. What information is necessary for the allegations and which excessive information can be avoided?
d. What personal information is included in the specific report?
e. Who are affected by the specific report?
f. How long do we need to keep the report?

[78] See also IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guide,* 2017, 19 ff.
[79] Motive 4 of the GDPR.; Frydlinger et al., *GDPR, Juridik, organisation och säkerhet enligt Dataskyddsförordningen,* 2018, p. 29 f.
[80] Article 5.4 of the TEU. See also Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 62 f., 80 ff. & 260.
[81] Article 5.2 of the GDPR.; The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 11 f.

g. What are the risks the whistleblowing case may cause and how can we prevent ourselves from them?[82]

Furthermore, in order to demonstrate accountability, there are four things that shall be documented:

1. A policy or internal rules or decision on whistleblowing.
2. Limitations to the right of access.
3. Any deferral of information to the individual.
4. The risk assessment conducted for the specific procedure.[83]

2.3.6 Excursus: DPIA

In Article 35.1 of the GDPR, it is stated that, where a type of processing is likely to contain a high risk to infringe on the rights and freedoms of persons, the controller must carry out a DPIA. This is considered as an important tool for the accountability since the DPIA demonstrate that appropriate measures have been taken. These measures shall ensure compliance with the GDPR provisions. In some states, i.e. Germany and France, it is specified that whistleblowing facilities represent high risk processing, consequently, a full DPIA is required.[84]

2.4 The GDPR and the Whistleblower Protection Directive

Since the GDPR is complemented in the Member State Laws in different ways, different problems can occur in different Member States, thus some countries have more severe requirements than the GDPR requires. According to the Data and Technology group of German Baker McKenzie Law Firm, it can be problematic that the requirements of the GDPR will remain unaffected regardless of the Whistleblower Protection Directive. The group means that it is unclear how the requirements of the GDPR will be aligned with the new directive. According to the German Data Protection Authorities, a person that

[82] The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 11 f.
[83] Ibid.
[84] See also Motive 4, 90, 91, 92 & 94, of the GDPR.; Cherepanova, *Yes, GDPR has already changed the whistleblowing landscape,* 2019.

is being mentioned in a whistleblowing report has the right to receive information regarding the identity of the whistleblower. This is not in compliance with the Whistleblower Protection Directive, since the whistleblower has a right not to be mentioned by name in order to obtain protection.[85]

Cherepanova alleges that already in 2018 people and companies started wondering how the GDPR would work in compliance with whistleblowing protection. The questions were regarding how to balance individual's privacy against companies need to pursue investigations regarding work against anti-corruption.[86]

[85] The Data and Technology group of Baker McKenzie Germany, *The new EU Whistle-blowing Directive: Considerations from a German compliance, employment and data protection law perspective*, 2020.
[86] Cherepanova, *Yes, GDPR has already changed the whistleblowing landscape,* 2019.

3 Reporting channels

3.1 Disposition

In this chapter I analyse conflicts between the Whistleblower Protection Directive regarding reporting channels and the GDPR.

The introduction includes information regarding the concerned articles. Subsequently, I first present the articles, secondly the conflicts, and thirdly analyse the problematic parts and suggest possible solutions. The analysis is continuous meaning thoughts are presented through the chapter.

3.2 The articles

3.2.1 Reporting channels

In a press release from the CoE, it submitted the demands regarding reporting channels. It stated that the Whistleblower Protection Directive will aim to demand companies to create effective and efficient reporting channels.[87]

Article 7 of the Whistleblower Protection Directive provides requirements regarding internal reporting channels. Pursuant to Paragraph 2, the Member States shall prioritize internal reporting channels above external reporting channels. The encouragement relies on the provisions that the breach can be addressed effectively internally, and that the reporting person does not risk retaliation. Information relating to this shall be provided in the context of the information given by legal entities in the private and public sector pursuant to point (g) of Article 9.1, and by competent authorities pursuant to Article 12.4(a) and Article 13 of the Whistleblower Protection Directive.

Furthermore, there are specific requirements regarding how internal reporting channels shall be constituted. These requirements are presented in Article 8 of the Whistleblower Protection Directive. According to Paragraph 1, the Member States shall ensure legal entities in the private and public sector to

[87] The Council of Europe, *Better protection of whistle-blowers: new EU-wide rules to kick in in 2021,* 2019.

create procedures regarding follow-up, subsequent consultation and agreements with the social partners, if provided by national law. These channels shall, according to Paragraph 2, enable employees to report information on breaches. The requirements are mandatory for companies with 50 or more workers, pursuant to Article 8.3 of the Whistleblower Protection Directive.

3.2.2 The rights of the data subject

According to Article 12.1 of the GDPR, the data subject has a right to transparent information, communication and modalities regarding exercising of the rights of the data subject. The information shall be provided in a plain and concise language by the controller. Information requested by the data subject under Article 15 to 22 of the GDPR shall be given by the controller without delay and within one month. The period can be extended by two months further if deemed necessary due to the complexity and number of requests.

By the time the personal data is being obtained, the controller shall provide the data subject with certain information. I.e. contact details of the controller, purpose of the processing for which the personal data is intended and the legal base for the processing.

3.3 Analysis

3.3.1 The right to know the source of information

3.3.1.1 The conflicting articles

The first conflicting Articles are Article 9.1(a) of the Whistleblower Protection Directive and Article 14.2(f) of the GDPR. The articles aim to protect two different interests. The Whistleblower Protection Directive protects the reporting person, while the GDPR protects the reported person.

Article 9.1 of the Whistleblower Protection Directive provides certain requirements for the internal reporting channels. Pursuant to Article 9.1(a) of

the Whistleblower Protection Directive, the channels must be designed in a secure manner and ensure the confidentially of the identity of the reporting person. According to Article 14.2(f) of the GDPR, if personal data is provided from someone other than the data subject, the data subject has a right to know from which source the personal data originates. This information shall be provided within reasonable time after obtaining the personal data, but at least within one month, deemed to specific circumstances, Article 14.3(a) of the GDPR. This conflict is problematic in two perspectives, the letter of the law, and the conflicting interests.

3.3.1.2 The letter of the law

First, in Article 14.2(f) of the GDPR it is stated that the data subject has a right to know from *which* source the information came, not from *who*.

Pursuant to the Article 29 Working Party, *which source* means *the specific source*. The group has however stated that if the source of the information is not named other information can be provided. The information shall then be the nature of the source, i.e. the type of organization-/sector/industry and if it is publicly or privately held.[88] Accordingly, it is in situations of anonymity only essential to provide the data subject with the information that the report came from *a whistleblower*, not *which whistle-blower*.

Situations of anonymity will however be examined later. This means that in this analysis, given that the whistleblower is not anonymous, *it is not possible to protect the whistleblower and make an exception from Article 14.2(f) of the GDPR with this argument.*

3.3.1.3 The conflicting interests

The other problematic part is that the interests are in conflict. Accordingly, in order to work in compliance, an exception is needed that can be used to prioritise one of them, the whistleblower, or the data subject. In Article 14.5 of the GDPR certain exceptions are provided from Article 14.2 of the GDPR.

[88] The Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679,* 2018, p. 40.

Pursuant to Article 14.5(b) of the GDPR, information regarding the information giver does not need to be provided to the data subject under certain circumstances. I.e. if the provision of such information is impossible or would involve a non-proportional effort. In particular, for archiving purposes in the public interest.[89] If this exception is used, the controller has an obligation to take appropriate actions to protect the rights, freedoms and legitimate interests of the data subject.

Accordingly, a possible way to motivate the exception of Article 14.5(b) of the GDPR is due to public interest. In order to make this exception applicable, the solution must be examined in three steps with affirmative answers.

1. *Is anti-corruption in the public interest?*
   →If yes,
2. *Is protecting whistleblowers crucial for safeguarding purposes in the public interest?*
   →If yes,
3. *Is providing the data subject with information regarding the whistleblower impossible for safeguarding the protection of whistleblowers?*
   →If yes,
   →The exception of Article 14.5(b) of the GDPR is applicable.

1. *Is anti-corruption in the public interest?*

As examined in Chapter 2.2.2, anti-corruption shall be counted as a public interest. This has been proven especially in times of the Swine Flu, Ebola and the COVID-19 virus and is subsequently stated in the Whistleblower Protection Directive. This is i.e. because corruption otherwise can jeopardize

[89] Note that purposes of archiving in the public interest is not defined in the directive, in any recital or by the Article 29 Working Party. Archiving is defined as "*Place or store (something) in an archive".* An archive is defined as "*The place where historical documents or records are kept",* See Lexico powered by Oxford. In this case, collecting reports from whistleblowers means storing records of suspicions of breaches that can further on be evidence for prosecution, and can therefore be a processing for safeguarding public interests.

public procurement and enhance the risk of companies cheating with beneficial regulations.[90]

→ Yes, anti-corruption is a public interest.

2. *Is protecting whistleblowers crucial for safeguarding purposes in the public interest?*

As also presented in Chapter 2.2.2, protection of whistleblowers is crucial for safeguarding purposes in the public interest. The ones who most likely can discover corruption are whistleblowers, and anti-corruption is counted as a public interest. Therefore, it is highly important to protect whistleblowers from retaliation.[91]

→ Yes, protecting whistleblowers is crucial for safeguarding purposes in the public interest.

3. *Is providing the data subject with information regarding the whistleblower impossible for safeguarding the protection of whistleblowers?*

Yes, it is not possible to safeguard the protection of whistleblowers if they can suffer from retaliation, which they can do if their identity is being revealed.[92]

→ Yes, it is impossible to provide the data subject information regarding the whistleblower in order to safeguard the protection of whistleblowers.

→ The exception of Article 14.5(b) of the GDPR is applicable.

---

[90] I.e. Motive 1, 3, 5, 37, 84 & 109 of the Whistleblower Protection Directive.; Transparency International, *Coronavirus sparks high risk of corruption across Latin America,* 2020.; *Transparency International, Corruption and the Coronavirus – How to prevent the abuse of power during a global health pandemic*, 2020.; Blixt, *Visselblåsare har varnat för att bolag fuskar med korttidspermitteringar. Nu ryter finansministern till mot bolagen som planerar att inte följa reglern*a, 2020.; Regeringskansliet, Finansdepartementet, *Om förslaget korttidspermittering,* 2020.

[91] I.e. Motive 84.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 238 f.; The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 8 f.; Transparency International, *Building on the EU directive for Whistleblower protection, analysis and recommendations,* 2019, p. 1.; Transparency International, *Whistleblowing in Europe legal protection for whistleblowers in Europe,* 2013.; Peretz et al., *The Whistleblowers, Exposing Corruption in Government and Industry,* 1989, p. 240 ff.

[92] Ibid.

Every action interfering with the GDPR needs to be evaluated with the proportionality principle. The purpose of the principle is that actions shall not be more restrictive than necessary due to the aim of the action.[93] The action in this case it to neglect the data subject the right to receive information regarding the source of the collected personal data. The aim is to protect the whistleblower. It is proportional to neglect the right of the data subject, since it is not possible to take action in another way and still protect the whistleblower, as examined above. The action is therefore in compliance with the proportionality principle.

3.3.1.4 Conclusion

As examined above, it is possible to make an exception from the obligation to provide the data subject with information regarding from which source the personal data came. In consideration of public interest, it is justified to prioritise protection of the whistleblower, instead of the data subject.[94]

The purpose of safeguarding the public interest would in this case be to reveal corruption in order to work preventively. Consequently, *the purpose of the Whistleblower Protection Directive, to reveal corruption, justifies neglecting rights of the GDPR and prioritise the Whistleblower Protection Directive*. Note that the controller still needs to take appropriate measures to protect the rights and freedoms of the data subject.

[93] Motive 4 of the GDPR.; Article 5.4 of the TEU.; Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 62 f., 80 ff. & 260.
[94] The German Data Protection Authority has another approach regarding this conflict. The authority means, that in order to provide the data subject with information regarding the whistleblower, the whistleblower must give its consent to this. According the authority, the solution is to give whistleblowers two options when submitting a report. To identify themselves and give consent to disclose their identity to the alleged person or submit the report anonymously. See Cherepanova, *Yes, GDPR has already changed the whistleblowing landscape,* 2019. I however do not find this solution satisfying since a whistleblower most likely does not want to give its consent to be disclosed, and also, anonymous reports are not mandatory to handle.

3.3.2 Anonymous reports

3.3.2.1 The conflicting articles

Another pair of conflicting articles are Article 9.1(e) of the Whistleblower Protection Directive, and Article 14.2(f) of the GDPR. These articles are in conflict since the Whistleblower Protection Directive provides an opportunity for the Member States to impose anonymous reporting channels, whilst at the same time, the GDPR requires the right of the data subject to receive information regarding from which source the personal data originates.

Pursuant to Article 9.1(e) of the Whistleblower Protection Directive, the proceeding of internal reporting shall include diligent follow-up on anonymous reporting, when provided in national law. As already examined above, it is stated in Article 14.2(f) of the GDPR that the data subject has a right to know from which source the information originates.

Accordingly, it is not mandatory for the Member States to constitute anonymous reporting channels. Consequently, if a state decides *not* to demand possibilities for anonymous reports, there is no conflict with Article 14.2(f) of the GDPR. If a Member State however *does* demand possibilities for anonymous reports, there may be a conflict with Article 14.2(f) of the GDPR.

3.3.2.2 The conflicting interests

Similarly, as mentioned above, there are conflicting interests. On the one hand, protection of the whistleblower. On the other hand, protection of the data subject.

Once again there are three questions that need to be answered in the affirmative in order to use the exception:

1. *Is anti-corruption a public interest?*

   →If yes,

2. *Is protecting whistleblowers crucial for safeguarding purposes in the public interest?*

   →If yes,

3. *Is having **anonymous** reporting channels crucial for safeguarding the protection of whistleblower?*

   →If yes,

   → the exception of Article 14.5(b) of the GDPR is applicable.

The additional problematic part with this article compared to the previous, is that it is not mandatory. Accordingly, it is harder to motivate that the provision is essential in order to fulfil the purposes of public interest.

Creating a way to report a breach anonymously is a controversial way of organising whistleblower protection. Coleman has written a great amount on the subject of how anonymity can appear and what consequences it can create.[95] Some believe it should be encouraged, some forbidden. Anonymous reports can be beneficial since it can contribute valuable information that employees otherwise may not dare to share under their own names. At the same time, it can be a disadvantage since it can be arduous to follow up. The EDPS believes it is not suitable for whistleblowing to be anonymous. According to it, whistleblowers shall feel safe to identify themselves without being afraid of retaliation. The EDPS believes anonymous reporting channels minimize opportunities for successful investigations, i.e. being able to ask further questions.[96]

[95] Coleman, *Hacker, Hoaxer, Whistleblower, Spy – The many faces of anonymous,* 2014, p. 1 ff. For the interested readers I recommend Ibid., p. 203 ff. regarding WikiLeaks.
[96] The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 6.

Anonymity can, according to Vaughn, additionally complicate the task of the investigator to double check information and ask further questions in order to accomplish an effective and successful investigation. Furthermore, it may make the investigations more expensive because there is a risk that the person in charge of the incoming reports must sort out what information is false and what information is true. In addition, it is a high risk that the report gets lost among several other anonymous reports. Vaughn however alleges, that if a whistleblower system is working properly, the whistleblower should not be afraid of consequences, since they should be protected.[97] I do not agree on the statement that many anonymous reports make the investigations more expensive. In the opposite, the more reports, the better chance to disclose corruption that otherwise can be expensive.

TI has recommended the Member States to require private or public entities and competent authorities to both accept and follow up on anonymous reports of breaches. TI has raised awareness of concerns regarding that anonymity can reduce the feeling of liability, causing false reports. However, research has shown that false reports are uncommon.[98]

Note that recommendations from TI in general go further than the directive requires.[99]

1. *Is anti-corruption a public interest?*

→ Yes, anti-corruption is a public interest.[100]

[97] Vaughn, *The Successes and Failures of Whistleblower Laws,* 2012, p. 309 ff.
[98] Transparency International, *Building on the EU directive for Whistleblower protection, analysis and recommendations,* 2019, p. 8 f.
[99] Ibid.
[100] I.e. Motive 1, 3, 5, 37, 84 & 109 of the Whistleblower Protection Directive.; Transparency International, *Coronavirus sparks high risk of corruption across Latin America,* 2020.; *Transparency International, Corruption and the Coronavirus – How to prevent the abuse of power during a global health pandemic*, 2020.; Blixt, *Visselblåsare har varnat för att bolag fuskar med korttidspermitteringar. Nu ryter finansministern till mot bolagen som planerar att inte följa reglern*a, 2020.; Regeringskansliet, Finansdepartementet, *Om förslaget korttidspermittering,* 2020.

2. *Is protecting whistleblowers crucial for safeguarding purposes in the public interest?*

→ Yes, protecting whistleblowers is crucial for safeguarding purposes in the public interest.[101]

3. *Is having anonymous reporting channels crucial for safeguarding the protection of whistleblower?*

Since it is not mandatory to have anonymous reporting channels, and whereas it is a controversial mechanism, my conclusion is *that there are not enough arguments to conclude that it is a required action regarding anti-corruption.*

→ The exception of Article 14.5(b) of the GDPR is *not* applicable.

3.3.2.3 The letter of the law

Article 14.5(b) of the GDPR may provide another solution. The data subject does not have a right to know from which source the information came if it is likely to render impossible to provide it. If a report is anonymous, it is not possible to identify the source, and therefore, it is impossible to provide the information. As mentioned above, the Article 29 Working Party has stated that if the specific source is not named, the controller shall provide the data subject with the type of organisations/sector/industry and if it is publicly or privately held instead.[102]

Accordingly, with this interpretation, if a member state *does* demand requirements for anonymous reports, there may not be a conflict with Article 14.2(f) of the GDPR. Interpretation with only the letter of the law is a criticized method.[103] However, in ambiguous interpretation fundamental principles i.e.

---

[101] I.e. Motive 84.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 238 f.; The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 8 f.; Transparency International, *Building on the EU directive for Whistleblower protection, analysis and recommendations,* 2019, p. 1.; Transparency International, *Whistleblowing in Europe legal protection for whistleblowers in Europe,* 2013.; Peretz et al., *The Whistleblowers, Exposing Corruption in Government and Industry,* 1989, p. 240 ff.

[102] The Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679,* 2018, p. 40.

[103] Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 158.

the proportionality principle can be used to fill in the gaps.[104] Having anonymous reporting channels is not mandatory, however, the consequence is that the data subject does not get information regarding the identification of the whistleblower, which it would not have been provided with anyhow. See Chapter 3.3.1.4. Therefore, the action of having anonymous reporting channels is not more restrictive to the data subject than not having it. Accordingly, the action is in compliance with the proportionality principle. In additional the interpretation is substantiated with the thoughts of the Article 29 Data Protection Working Party.

3.3.2.4 Conclusion

The conclusion is that it is not possible to justify breaches of the GDPR connected to anonymous reports due to public interest. However, I believe that *it is possible to provide the right to information provided in Article 14.2(f) of the GDPR with other data than the name of the whistleblower, if there are anonymous reporting channels. Therefore, the articles are in compliance and none of the interests need to be prioritized above the other.*

I believe, a consequence from uncertain non-mandatory rules, is that it can cause a lack of interest to incorporate it for the Member States. If the directive does not provide clear directions on how to incorporate anonymous channels, and they in addition to that can appear to be in conflict to the GDPR, this can cause a fear of incorporating them for the Member States.

[104] Hettne, in Otken Eriksson, *EU-rättslig metod, Teori och genomslag i svensk rättstillämpning*, 2016, p. 159.

4 Investigations

4.1 Disposition

In this chapter, conflicts regarding the GDPR and investigations that comes as a result of a report from a whistleblower is examined. I am accentuating three conflicts. The conflicts regard the right to be forgotten, the right to access and valid consent. I will first present information regarding investigations, and then provide concerned articles of the GDPR continuously in each subchapter.

Note that the Whistleblower Protection Directive does not provide guidelines for *how* investigations shall be done. It is however described in the directive *that* investigations shall be done.

4.2 The articles and guidelines

Pursuant to Article 8.6 of the Whistleblower Protection Directive, legal entities in the private sector can share resources for reports and investigations if they have between 50 to 249 workers. Due to Article 9.1(c-d) of the Whistleblower Protection Directive, regarding internal reporting channels, there shall be an impartial person or department for safeguarding diligent follow-up on the reports. The follow-up shall enable feedback to the whistleblower, Article 9.1(f) of the Whistleblower Protection Directive.[105]

The United Nations Office on Drugs and Crime[106] has written guidelines on investigations of corruption, and how handling reports properly is a precondition of successful investigations. The UNODC believes that once a report from a whistleblower is submitted, handling it thoroughly is crucial for combating corruption effectively. Investigations directly affect the immediate

[105] Similar provisions are provided for external reporting channels in Article 11 of the Whistleblower Protection Directive.
[106] Hereinafter *UNODC*.

case, but more importantly, they show the whistleblowers that they are taken seriously.[107]

In order to combat corruption through investigations, evidence needs to be gathered and evaluated through an investigation. Investigations regarding corruption are often complex and require experts within the subject. However, it is important for the competent investigator to focus on the protection of the parties involved. At the Conference of International Investigators held in 2003, ten guidelines were summarized as crucial for investigations. The guidelines were that evidence shall be filed and that evidence that is likely to be used for judicial hearing shall be secured.[108]

4.3 Analysis

4.3.1 The right to be forgotten

4.3.1.1 The conflicting interests

In the Whistleblower Protection Directive it is specified that investigations of reported material shall be done properly in order to avoid breaches of EU law. At the same time, the data subject has a right to obtain the erasure of the personal data concerning the data subject. The erasure shall be done without undue delay, Article 17.1 of the GDPR. Accordingly, the reported material, including the personal data, needs to be investigated in order to reveal breaches. At the same time, the data subject has the right to obtain erasure of the material.[109]

---

[107] The United Nations on Drugs and Crime, *Investigation of corruption, Handling reports as a precondition for successful investigations,* 2020. Please note that I will not present the technical parts regarding investigations comprehensive since guidelines for investigations can be different depending on national laws. For interest readers, I recommend The United Nations *Handbook on Practical Anti-Corruption Measures for Prosecutors and Investigators,* 2004.

[108] The United Nations, *Handbook on Practical Anti-Corruption Measures for Prosecutors and Investigators,* 2004, p. 45.

[109] See also Wendleby & Wetterberg, *Dataskyddsförordningen, GDPR, Förstå och tillämpa i praktiken,* 2019, p. 139 ff.

4.3.1.2 When is the personal data no longer necessary?

One problematic article is Article 17.1(a) of the GDPR. Pursuant to the article, if the personal data no longer is necessary in relation to the purpose for which it was collected, it has to be erased. According to Article 17 of the Whistleblower Protection Directive, personal data which is manifestly not relevant for handling a specific report shall not be collected. If the data is being accidentally collected, it shall be deleted without undue delay.[110]

The problematic question is, *is it possible to save information that is not currently necessary due to the purpose but can be in the future?* One possible solution is Article 17.3(b) of the GDPR. The Article provides an opportunity to be excused from the obligation to erase the personal data. This is i.e. for the performance of tasks carried out in public interest due to a legal obligation, in this case, obligations due to the Whistleblower Protection Directive. *Here, two questions shall be examined.*

1. *Is anti-corruption in a public interest?*
   →If yes,
2. *Is saving reports for the future crucial for safeguarding purposes in the public interest?*
   →If yes,
   → the exception of Article 17.3(b) of the GDPR is applicable.

[110] *Example:* Imagine that the Employee A leaves a report regarding the Employer B. Due to Article 9.1(d) of the Whistleblower Protection Directive, there shall be a diligent follow-up on the report by the competent Person C. Person C finishes the follow-up, but the investigation does not lead to prosecution against Employer B. The personal data was collected in a purpose, that Employee A thought that Employer B had done a breach. This shall mean, that the personal data no longer is necessary in relation to the purpose for which is was collected and shall be erased pursuant to Article 17.1(a) of the GDPR. Then imagine that Employee D leaves a report regarding Employer E, which Person C investigates which concludes in prosecution. The breach seems to be a co-operation with several of the employers, but the report on Employer B is now deleted. The report from Employee A on Employer B could have attached Employer B to the same crime as Employer E.

1. *Is anti-corruption a public interest?*

→ Yes, anti-corruption is a public interest.[111]

2. *Is saving reports for the future crucial for safeguarding purposes in the public interest?*

Pursuant to Article 11.1(f) and 12.1(b) of the Whistleblower Protection Directive, external reporting channels shall enable the possibility to store information in compliance with Article 18 of the Whistleblower Protection Directive in order to make further investigations. Article 18 of the Whistleblower Protection Directive covers regulations for record keeping of reports. Pursuant to Paragraph 1, Member States shall ensure that legal entities in the private and public sector and competent authorities keep records of every report received, in compliance with Article 16 of the Whistleblower Protection Directive.

In Article 16 of the Whistleblower Protection Directive, requirements regarding confidentiality are listed. In Paragraph 1, it is stated that the Member States shall ensure that the identity of the reporting person is not disclosed. According to Paragraph 2, it is prejudiced to make an exception from Paragraph 1, if this information is necessary and proportional due to Union or National law when doing the national investigations. Pursuant to paragraph 3, the reporting person shall know that their identity is being revealed, but not if revealing it can jeopardise the investigation.

→ Saving information for future investigations may be necessary to safeguard purposes in the public interest, it depends on the circumstances in the specific case.

→ The exception of Article 17.3(b) of the GDPR may be applicable.

[111] I.e. Motive 1, 3, 5, 37, 84 & 109 of the Whistleblower Protection Directive.; Transparency International, *Coronavirus sparks high risk of corruption across Latin America,* 2020.; *Transparency International, Corruption and the Coronavirus – How to prevent the abuse of power during a global health pandemic*, 2020.; Blixt, *Visselblåsare har varnat för att bolag fuskar med korttidspermitteringar. Nu ryter finansministern till mot bolagen som planerar att inte följa reglern*a, 2020.; Regeringskansliet, Finansdepartementet, *Om förslaget korttidspermittering,* 2020.

4.3.1.3 Conclusion

Since it is solely possible with external channels to store information for further investigations, and since the possibility has an exception as well, I cannot conclude that saving information for future investigations is an essential tool in order to combat corruption. Accordingly, it depends on the specific case, and the competent person needs to make a proportional assessment in the specific case.[112]

When doing the case-to-case assessment, it is important to take the type of information that is being held in the reports into account. If the report is being granted, an assessment shall also be done regarding which information that shall be removed from the report. I.e. information about the whistleblower or witnesses.[113]

Note that if the conclusion in the specific case is that it due to the circumstances is necessary to save the information, it is important to also investigate if it is in compliance with the proportionality principle. I.e., if the information from a whistleblower in a specific assessment is not crucial due to earlier reports. It may not be justified to save it if the information most likely can be collected further on.

4.3.2 The right to access

4.3.2.1 The conflicting interests

Furthermore, according to Article 15 of the GDPR, the data subject has a right to access the personal data. The provisions are specified in Paragraph 1.[114] These are i.e. that the data subject has a right to know the purpose of the processing, the categories of the personal data that is being collected, the recipients of the data, the period of storage of the information, the possible

[112] The European Data Protection Supervisor, *Guidelines on processing personal information within a whistleblowing procedure,* 2016, p. 8 f.
[113] Ibid.
[114] See also the European Data Protection Supervisor, *Whistleblowing.;* Wendleby & Wetterberg, *Dataskyddsförordningen GDPR, Förstå och tillämpa I praktiken,* 2019, p. 130 ff.

rights to request rectification or erasure of personal data or restriction of the processing, the right to lodge a complaint and available information from the source of the personal data. Furthermore, due to Article 15.3 of the GDPR, the controller shall provide a copy of the personal data. This shall not adversely affect rights and freedoms of others pursuant to Article 15.4 of the GDPR.[115] Neither the GDPR or the Article 29 Working Party specify who *others* are, or which *rights and freedoms* that shall not be affected.

The complex part about this right of the data subject is however not only the rights of the whistleblower, but also that such information can jeopardize the investigation.[116]

How can this be solved? Article 23 of the GDPR provides certain restrictions for Article 15 of the GDPR. Pursuant to Paragraph 1 of Article 23 of the GDPR, the Member States have a possibility to legislate in a manner which restricts the obligations and rights granted in i.e. Article 15 of the GDPR. This shall subsequently be done in the light of the aims of the right of Article 15 of the GDPR thus the restriction shall be done to respect the essence of fundamental rights and freedoms and with a necessary and proportionate measure in a democratic society to safeguard certain provisions.

4.3.2.2 National security

One of these provisions is national security, Article 23.1(a) of the GDPR. According to Vaughn, National defence is strongly connected to

[115] Note that this right is not the same as the right to data portability. See Article 20 of the GDPR. Data portability only relates to data provided from the data subject. This is another situation, since the information comes from someone other than the data subject, i.e. a whistleblower. See the Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* 2017, p. 17.

[116] *Example: Corruption is often organized with more than one person involved. Imagine that Employee A turns in a report on Employer B. The Competent Person C receives the report and starts the investigation. At the same time Employer B asks for its right to have access of the personal data. The Competent Person C does an assessment, with the conclusion that Employer B can have access to the personal data without jeopardizing the investigation. Employer B gets the information regarding what is being investigated. Employer B then calls Employer D, E & F, and tells them. D, E & F, which are involved in the same corruption as Employer B, then has a chance to destroy evidence of their involvement.*

whistleblowing. The synchronizations between them is distinct in many countries, especially in the United States. This depends on multiple factors. National security is connected to terrorism, war and diplomatic and military relations in the different countries. These are however dependent on something. *Information.* Faulty information, or hidden information, can conceal corruption, i.e. abuse of power, violation of civil liberties and criminal conduct. More importantly, the right information can reveal these matters of corruption. These abuses can otherwise threaten democratic institutions, and therefore, national security.[117]

Vaughn alleges that the encouragement of whistleblowing regarding national security can be seen in two different perspectives. On the one hand, employees who have connections to authorities for national security shall not be encouraged to reveal information, since this can harm national security. On the other hand, if employees who have connections to authorities for national security are encouraged to blow the whistle, abuses connected to corruption can safeguard national security.[118]

An issue according to Vaughn is that these kinds of disclosures can be classified as leaking, rather than whistleblowing. Since the differences are subtle, it can be hard to tell if the disclosure will be protected under whistle-blowing regulations or not.[119]

When it comes to national security and the private sector, Vaughn exemplifies with the 9/11 terrorist attacks on the United States implicated private-sector

[117] Vaughn, *The Successes and Failures of Whistleblower Laws*, 2012, p. 211 f.
[118] Ibid. I.e. the case of Edward Snowden. Snowden was an American whistleblower who leaked highly classified information from the National Security Agency when he worked at the Central Intelligence Centre. The information contained disclosure regarding global surveillance. The United States federal prosecutors pressed charges against Snowden and the Department of State revoked his passport. He flew to Russia where he later on was granted the right of asylum. He has later on been tributed for his courage to blow the whistle. See Jemsby, *Wallström: Han har initierat en viktig debatt,* 2014.; Transparency International, *Germany: Whistleblower Prize 2013 for Edward Snowden,* 2013.; BBC, *Edward Snowden: Leaks that exposed US spy programme,* 2014.
[119] Vaughn, *The Successes and Failures of Whistleblower Laws*, 2012, p. 229 f. I.e., the WikiLeaks disclosure fell outside the regulations for protecting whistleblowers.

activities. This incident highlighted the vulnerability in infrastructure connected to private companies, i.e. in this case aviation companies.[120]

4.3.2.3 Prevention and investigation of criminal offences

Another provision is prevention and investigation of criminal offences, Article 23.1 (d) of the GDPR. Corruption is often a gateway to other crimes. I.e. accounting frauds, which are commonly connected to corruption. Usually, the Member States accordingly have many acts of corruption, i.e. bribery, legislated as crimes.[121]

Accordingly, anti-corruption is a way of preventing and investigating criminal offences. The restriction is applicable in matters connected to anti-corruption. The investigations are an important part of preventing and investigating criminal offence whereas if reports are not investigated, it is impossible to detect and investigate the suspected corruption.

4.3.2.4 Objects of general public interest

As presented above, anti-corruption is in the public interest.[122] UNODC has stated that handling reports and investigations properly is crucial in order to combat corruption effectively.[123] In Article 23.1(e) of the GDPR, a requisite regarding restrictions against Article 15 of the GDPR is important objectives of general public interest of the Union or a Member State. It is specified in the Whistleblower Protection Directive, that protecting whistleblowers is

[120] Vaughn, *The Successes and Failures of Whistleblower Laws*, 2012, p. 232.
[121] See also The United Nations Office on Drugs and Crimes, *Links between organized crimes and corruption,* 2018.; Cars & Engstam Phalén, *Mutbrott,* 2020, p. 29.
[122] I.e. Motive 1, 3, 5, 37, 84 & 109 of the Whistleblower Protection Directive.; Transparency International, *Coronavirus sparks high risk of corruption across Latin America,* 2020.; *Transparency International, Corruption and the Coronavirus – How to prevent the abuse of power during a global health pandemic*, 2020.; Blixt, *Visselblåsare har varnat för att bolag fuskar med korttidspermitteringar. Nu ryter finansministern till mot bolagen som planerar att inte följa reglern*a, 2020.; Regeringskansliet, Finansdepartementet, *Om förslaget korttidspermittering,* 2020.
[123] The United Nations Office on Drugs and Crimes, *Investigation of corruption, Handling reports as a precondition for successful investigations,* 2020.

counted as an important objective of general public interest within the meaning of 23.1(e).[124]

4.3.2.5 Conclusion

My conclusion is that investigations are necessary and proportional instruments regarding anti-corruption, and that anti-corruption is strongly connected to national security, prevention and investigation of criminal offences and objects of general public interest. *It shall therefore be possible to except the data subject´s right of access, Article 15 of the GDPR, pursuant to Article 23.1 (a, d & e) of the GDPR.*

4.3.3 Valid consent

4.3.3.1 The conflicting interests

The next conflict between the GDPR and investigations is connected to valid consent. The problematic part is that the consent may be collected for one purpose, and then used for another for the investigations.

Due to Article 4.11 of the GDPR, there are four requirements that need to be fulfilled in order for a consent to be valid. One of those requirements is that the consent needs to be given voluntarily.[125] One aspect of that is that an agreement cannot provide certain different treatments of personal data regarding more than one purpose. Due to this, the collector cannot create a package deal due to the consent, since the consent needs to be specific.[126] Furthermore, according to Article 5.1(b) of the GDPR, the purpose of the consent shall be legitimate and announced before the consent is given. This is called limitation of purpose.[127]

[124] Motive 84 of the Whistleblower Protection Directive.
[125] See also the European Data Protection Board, *Consent,* 2018, p. 4 f.; Wendleby & Wetterberg, *Dataskyddsförordningen GDPR, Förstå och tillämpa I praktiken,* 2019, p. 76 ff.
[126] The European Data Protection Board, *Consent,* 2018, p. 10 f.
[127] See also the European Data Protection Board, *Consent,* 2018, p. 12.; IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guide,* 2017, p. 206 ff.

The next problem is the specific requisites regarding transparency. The purpose is that the data subject leaving the consent has to have all the information regarding the collection and treatment of the data.[128] After the *Google vs. Spain case*, it has become clear that transparency is one of the keys in order to work successfully in compliance with the GDPR.[129]

4.3.3.2 Guidelines from the Swedish Inspection of Data Protection

Earlier, the Swedish Inspection of Data Protection communicated guidelines regarding whistleblowing and the GDPR. These guidelines were however deleted from the website at the same time as the Whistleblower Protection Directive came.[130]

In the earlier recommendations, it was stated that the personal data could be used by others than the collector of the valid consent. This was although only in certain circumstances. I.e. if the personal data was connected to persons of great importance to the company and if it was motivated due to concerns of breaches regarding i.e. accounting, bribes, or the interests of the organisation or life or health of individuals.[131]

4.3.3.3 Consent of the wrong purpose

When investigating a report, the investigator may have to use information with another purpose than the one given. This is problematic due to the provisions regarding valid consent. However, processing personal data for other purposes than for which is was collected, may be allowed for tasks carried out in the public interest.[132]

---

[128] The European Data Protection Board, *Consent,* 2018, p. 13.; IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guide,* 2017, p. 93 ff.
[129] Cherepanova, *Yes, GDPR has already changed the whistleblowing landscape,* 2019.
[130] Lindblom, Datainspektionens författningssamling, *Föreskrifter om behandling av personuppgifter som rör lagöverträdelser,* 2018.
[131] Ibid.
[132] Motive 50 of the GDPR.

The conflict may be solved by motivating the processing of another legal ground than valid consent. Pursuant to Article 6.1(e) of the GDPR, the processing of the personal data can be lawful when it is necessary regarding the performance of a task carried out in the public interest or exercise of official authority. According to the Article 29 Working Party, the article can be appropriate in the public sector in certain circumstances. The task or function must then have a clear basis in law.[133] I find this statement problematic for two reasons. First, because it is not stated in the article that it can only be used in the public sector. The requirements are formulated alternative, not cumulative. Secondly, it is neither stated in the article that it needs to have a clear basis in law. However, I believe the Whistleblower Protection Directive is a clear basis in law.

In the German guidelines, *On Whistleblowing Hotlines,* it is provided that collection of personal data through whistleblowing mechanisms is permissible, if the collection has a connection to i.e. international accounting control, fraud or bribery. This is justified in Article 6.1(f) of the GDPR, since it is necessary due to a legitimate interest pursued by the controller. However, the regulator did not clarify if this could be applied to other things such as anti-trust law, privacy law or harassment cases.[134]

Article 6.1(f) of the GDPR provides exceptions from legal consent if the collection and processing is necessary in legitimate interests pursued by the controller or any third party. When using this article, the controller must carry out a balance test to examine that the interest of the collection and processing are overridden by interests of the data subject or fundamental rights and freedoms.[135]

[133] See also the Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* 2017*,* p. 14.
[134] Cherepanova, *Yes, GDPR has already changed the whistleblowing landscape,* 2019.
[135] See also Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* 2017*,* p. 14 ff.

The balance test[136] shall not be in favour of either the data subject or the data controller. The test is a case by case assessment, and the conclusion can either be that the interest is overridden by the controller or the data subject. Both parts need to be taken into account genuinely. However, the Article 29 Working Party has acknowledged that there can be strong cases in favour of the controller to claim that its legitimate interests overrides the data subject's. *This is i.e. when the interest of the controller is in the public interest.* In these situations, it is important that the controller makes a careful analysis and take the rights of the data subject into account. The proportionality principle also needs to be safeguarded.[137]

The controller needs to evaluate positive and negative consequences regarding the data subject, i.e. discrimination or exposure. Other things that shall be considered are the balance of power between the data subject and the controller and how many that will take part of the personal data. Furthermore, accountability shall be a part of the test.[138] The Article 29 Working Party illustrates some scenarios, which shows that even direct marketing can, in some cases, be carried out with this article.[139]

I believe that the interest of the controller in cases of investigations overrides the interest of the data subject. This is since actions of anti-corruption is in the public interest which is essential when investigating the balance of interest.

---

[136] Note, that the directions of the balance test are for Article 7 of the Data Protection Directive. The test is however still useful for the GDPR according to the Article 29 Data Protection Working Party. See the Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* 2017*,* p. 14.

[137] The Article 29 Data Protection Working Party, *Overview of results of public consultation on Opinion on legitimate interest of the data controller, Opinion 06/2014*, 2014, p. 3 ff.; The Article 29 Data Protection Working Party, *Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen I artikel 7 I direktiv 95/46/EG*, 2014, p. 35 ff.

[138] Ibid.

[139] The Article 29 Data Protection Working Party, *Overview of results of public consultation on Opinion on legitimate interest of the data controller, Opinion 06/2014,* 2014, p. 6.

4.3.3.4 Conclusion

Since anti-corruption is a public interest[140], and investigations are necessary in order to combat corruption[141], *processing of personal data with another purpose – than the ordinary one given in connection to the valid consent – shall be lawful pursuant to Article 6.1(f) of the GDPR.*

The action shall also be in compliance with the proportionality principle, since there is no other possible action that can be taken and still achieve the aim of the public interest. This is since investigations are crucial for combating corruption.

I would like to emphasize that the balance test is a complicated test that needs to be evaluated properly for every company thoughtfully. My conclusion is that the result of the test most likely will be that the interest of the investigator will override the interest of the data subject. However, the specific test still needs to be done in order to present the accountability.[142]

[140] I.e. Motive 1, 3, 5, 37, 84 & 109 of the Whistleblower Protection Directive.; Transparency International, *Coronavirus sparks high risk of corruption across Latin America,* 2020.; *Transparency International, Corruption and the Coronavirus – How to prevent the abuse of power during a global health pandemic*, 2020.; Blixt, *Visselblåsare har varnat för att bolag fuskar med korttidspermitteringar. Nu ryter finansministern till mot bolagen som planerar att inte följa reglern*a, 2020.; Regeringskansliet, Finansdepartementet, *Om förslaget korttidspermittering,* 2020.

[141] The United Nations Office on Drugs and Crimes, *Investigation of corruption, Handling reports as a precondition for successful investigations,* 2020.

[142] For detailed guidelines regarding the balance test I recommend, the Article 29 Data Protection Working Party, *Overview of results of public consultation on Opinion on legitimate interest of the data controller, Opinion 06/2014*, 2014.; the Article 29 Data Protection Working Party, *Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen I artikel 7 I direktiv 95/46/EG*, 2014.

5 Conclusions

5.1 Research questions

"The directive's interaction with GDPR, particularly in relation to data subject rights, may finally resolve most of the ambiguity and help to establish GDPR definitions consistent across all Member States." Vera Cherepanova, experienced compliance officer 2019.[143]

Well, will it?

Both the Whistleblower Protection Directive and the GDPR have ambiguous provisions which are complicated to interpret. Accordingly, they are even harder to interpret in the light of each other, and it will therefore be hard to work in compliance with them.

What are the conflicts between the Whistleblower Protection Directive regarding reporting channels and the GDPR?

I identified two different conflicts between the Whistleblower Protection Directive regarding reporting channels and the GDPR. One regarding the rights of the data subject and one regarding anonymous reporting.

What are the conflicts between the Whistleblower Protection Directive regarding investigations and the GDPR?

I identified three different conflicts between the Whistleblower Protection Directive regarding investigations and the GDPR. One regarding the right to be forgotten, one regarding the right to access and one regarding valid consent.

Is it possible for companies to work in compliance with both the Whistleblower Protection Directive and the GDPR?

According to me it is possible. It will however not be easy, and many parts are ambiguous.

[143] Cherepanova, *Yes, GDPR has already changed the whistleblowing landscape,* 2019.

If the third question is answered in the affirmative, how shall they act?

I believe companies shall prioritize protecting whistleblowers by creating detailed and secure reporting channels and carry out investigations well. It is possible to accomplish, since exceptions of the GDPR is applicable in cases of crucial actions regarding anti-corruption. In the motives of the GDPR, the importance of customising regulations in favour of natural persons is being emphasized. This shall be done with consideration of public interest, other rights and the proportionality principle. Pursuant to this, the CJEU has several times interpreted cases of personal data breaches in the light of other rights and freedoms and the proportionality principle. In this thesis, the GDPR has been interpreted in the light of protection of whistleblowers and infringements of the GDPR have been assessed with the proportionality principle.

Regarding the rights of the data subject to get information about the whistleblower, the right to access of the personal data and valid consent, it is possible to infringe these rights due to public interest. As examined, COVID-19 and other crises have showed the importance of anti-corruption. In countries with corruption, consequences can be i.e. price governing and financial crises that may cause deaths. Therefore, it is important to protect the whistleblowers, due to public interest in order to combat corruption.

Regarding anonymous reporting channels, my conclusion is that they are not essential for combating corruption. It is however a possible solution to use anonymous reporting channels due to an exception of getting information about the source, i.e. when the information does not exist. Furthermore, providing anonymous reporting channels is in compliance with the proportionality principle since the provision is not more restrictive than non-anonymous reporting channels. Since the provision is not mandatory, it will be up to the Member States to decide whether they will implement anonymous reporting channels or not as a legal provision.

Lastly, regarding the right to be forgotten, it is unclear whether it is legitimate to save information from reports for future investigations or not. It is a prov-

ision that needs to be investigated in every case due to the circumstances and to be assessed with the proportionality principle.

5.2 Excursus: accountability and DPIA

In order to work in compliance with the GDPR it is important to have accountability. As mentioned in this thesis, the EDPS has stated that there are certain questions that companies or authorities shall consider in order to have proper accountability.

a. How do we protect involved persons confidentiality?
b. What is the purpose of using the whistleblowing channel?
c. What information is necessary for the allegations and which excessive information can be avoided?
d. What personal information is included in the specific report?
e. Who are affected by the specific report?
f. How long do we need to keep the report?
g. What are the risks the whistleblowing case may cause and how can we prevent ourselves from them?

I highly recommend companies to answer these questions in order to be sure that they act in compliance with both the directive and the regulation. It is not only necessary in order to be able to narrate the accountability on potential control by a data protection authority, it is also a great tool in order to get an overview the system. It is possible to have standard answers for all reports regarding question a, b and c, while question d, e, f and g shall be investigated for every specific report.

Furthermore, in order to demonstrate the accountability, there are four things that shall be documented:

1. A policy or internal rules or decision on whistleblowing.
2. Limitations to the right of access.
3. Any deferral of information to the individual.
4. The risk assessment conducted regarding the specific procedure.

I also highly recommend companies to document these four things in order to demonstrate high accountability. This shall be tailed due to i.e. the size of company and the type of company.

The accountability is also helpful in cases of obligations from a data subject. A data subject which have its personal data processes due to a task of public interest, has the right to obligate. It is then a task of the controller to demonstrate that the interest of public interest overrides the interests of the data subject. Having accountability will facilitate this task.

Furthermore, I want to emphasize that there are situations were there can be necessary to carry out a DPIA. Also, it is important not to forget to investigate if actions that are being taken are in compliance with the proportionality principle.

5.3 Further research

I encourage future research of the subject. I would highly recommend future research especially when the Whistleblower Protection Directive is implemented in October 2021. By then, it will be possible to see the lack of explanation of how the incorporation of the directive will work together with the GDPR.

Furthermore, it would be interesting both to compare different solutions in different countries, and to see how the Member States legislate with consideration of the GDPR.

Bibliography

European Union legislation

Primary law

Charter of Fundamental Rights of the European Union, (OJ 2012/C 326/2).

Consolidated version of the Treaty on the European Union, (OJ 2012/C 326/01).

Consolidated version of the Treaty on the Functioning of the European Union, (OJ 2012/C 326/01).

Secondary law

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.

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.

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).

Swedish legislation

Lagen (2016:749) om skydd mot repressalier för arbetstagare som slår larm om allvarliga missförhållanden.

Reports and recommendations

Council of Europe Recommendation CM/Rec (2014)7, "*On the protection of whistleblowers"*, 2014.

Datainspektionens författningssamling, "*Föreskrifter om behandling av personuppgifter som rör lagöverträdelser",* DIFS: 2018:2, Lindblom, Hans-Olof, 2018-05-22.

Transparency International, "*Whistleblowing in Europe legal protections for whistleblowers in the EU",* Worth, Mark, 2013-10.

Transparency International, "*Building on the EU directive for Whistleblower protection, analysis and recommendations",* Terracol, Marie, position paper #1/2019, 2019.

SOU 2014:31, "*Stärkt skydd för arbetstagare som slår larm om allvarliga missförhållanden",* 2014-05-20, updated 2015-04-02.

Literature:

Bogdan, Michael, "*Komparativ rättskunskap",* second edition, Norstedts Juridik, Stockholm, Sweden, 2003.

Cars, Thorsten & Engstam Phalén, Natali, "*Mutbrott"*, fourth edition, Norstedts juridik, Warsaw, Poland, 2020.

Coleman, Gabriella, "*Hacker, Hoaxer, Whistleblower, Spy – The many faces of anonymous",* 2015, Verso Books, London, the United Kingdom, 2014.

Frydlinger, David, Edvardsson, Tobias, Carlström, Olstedt, Caroline & Beyer, Sandra, *"GDPR, Juridik, organisation och säkerhet enligt Dataskyddsförodrningen",* second edition, Norstedts juridik, Warsaw, Poland, 2018.

Samuel, Geoffrey, "*An Introduction to Comparative Law Theory and Method",* Hart Publishing, Crydon, the United Kingdom, 2014.

Hettne, Jörgen, in Otken Eriksson, Ida, "*EU-rättslig metod, Teori och genomslag i svensk rättstillämpning",* second edition, Norstedts Juridik, Inowroclaw, Poland, 2016.

IT Governance Privacy Team, "*EU General Data Protection Regulation (GDPR), An Implementation and Compliance Guide",* second edition, IT Governance Publishing, Cambridgeshire, the United Kingdom, 2017.

Jubb, Peter, "*A Restrictive Definition and Interpretation",* 21st edition, number 1, Journal of Business Ethics, 1999.

Larsson, Per, "*Skyddet för visselblåsare i arbetslivet – en konstitutionell och arbetsrättslig studie",* 2015, Jure Förlag, Stockholm, Sweden, 2015.

Near, Janet, Miceli, Marcia, "*Organizational Dissidence: The Case of Whistle-Blowing",* Journal of Business Ethics 4, 1985.

Peretz, Glazer, Myron, Migdal & Glazer, Penina, "*The Whistleblowers, Exposing Corruption in Government and Industry"*, Basic Books, Inc., Publishers, New York, the United States, 1989.

Slorach, Martina, Flemström, Stefan, Gabinus Göransson, Håkan & Hamskär, Ingemar, "*Rätten att slå larm – En handbok om yttrandefriheten på jobbet – råd för whistleblowers"*, Tryells Tryckeri, Laholm, Sweden, 2011.

Vaughn, Robert G., "*The Successes and Failures of Whistleblower Laws"*, MPG Books Group, Bodmin, the United Kingdom, 2012.

Wendleby, Monika & Wetterberg, Dag, ”*Dataskyddsförodrningen GDPR, Förstå och tillämpa I praktiken*”, Second edition, Sanoma Utbildning, Livonia Print, Ventspils, Latvia, 2019.

Websites:

The Article 29 Data Protection Working Party, “*Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen I artikel 7 I direktiv 95/46/EG”,*
<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_sv.pdf>, published 2014-04-09, visited 2020-05-12.

The Article 29 Data Protection Working Party, “*Overview of results of public consultation on Opinion on legitimate interest of the data controller, Opinion 06/2014*”,
<https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf>, published 2014-11-14, visited 2020-05-12.

The Article 29 Data Protection Working Party, “*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”,*
<https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>, published 2017-02-06, visited 2020-04-14.

The Article 29 Data Protection Working Party, “*Guidelines on transparency under Regulation 2016/679”,*
<https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227>, published 2017-11-29, updated 2018-04-11, visited 2020-04-13.

The Australian Commonwealth Ombudsman, "*Agency guide to the public interest disclosure act 2013", version 2,* <https://www.ombudsman.gov.au/__data/assets/pdf_file/0020/37415/Agency_Guide_to_the_PID_Act_Version_2.pdf>*,* published 2016-04, visited 2020-04-18.

BBC News, "*Edward Snowden: Leaks that exposed US spy programme",* <https://www.bbc.com/news/world-us-canada-23123964>*,* published 2014-01-17, visited 2020-05-19.

Blixt, Tobias, "*Visselblåsare har varnat för att bolag fuskar med korttidspermitteringar. Nu ryter finansministern till mot bolagen som planerar att inte följa reglerna",* Breakit, <https://www.breakit.se/artikel/24502/tillvaxtverket-ska-stoppa-fusk-med-korttidsarbete-med-specialstyrka>, published 2020-04-06, visited 2020-04-13.

Cherepanova, Vera, "*Yes, GDPR has already changed the whistleblowing landscape",* <https://fcpablog.com/2019/05/22/yes-GDPR-has-already-changed-the-whistleblowing-landscape/>, the FCPA blog, published 2019-05-11, visited 2020-02-17.

The Council of the European Union, "*Better protection of whistle-blowers: new EU-wide rules to kick in in 2021",* <http://dsms.consilium.europa.eu/952/Actions/Newsletter.aspx?messageid=36421&customerid=20185&password=enc_4638464542323942_enc>*,* published 07-10-2019, visited 13-02-20.

The Data and Technology group of Baker McKenzie Germany, "*The new EU whistleblower directive: Considerations from a German Compliance,*

Employment and Data Protection Law Perspective", <https://www.bakermckenzie.com/en/insight/publications/2020/01/the-new-eu-whistleblowing-directive>*,* published 2020-01-20, visited 2020-02-27.

The European Data Protection Board, "*Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak"*, <https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_sv>, published 2020-03-16, visited 2020-04-13.

The European Data Protection Supervisor, "*Guidelines on processing personal information within a whistleblowing procedure",* <https://edps.europa.eu/sites/edp/files/publication/16-07-18_whistleblowing_guidelines_en.pdf>*, published* 2016-07, visited 2020-04-20.

The European Data Protection Supervisor, "*Whistleblowing",* <https://edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en>*,* visited 2020-04-24.

The European Parliament, "*Sources and scope of European Union law",* <https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law>*,* updated 2020-02, visited 2020-05-15.

GDPR.EU, "*Everything you need to know about GDPR compliance",* <https://GDPR.eu/compliance/>, visited 2020-04-18.

Jemsby, Carolina, "*Wallström: Han har initierat en viktig debatt",* <https://www.svt.se/nyheter/inrikes/wallstrom-han-har-initierat-en-viktig-debatt>*,* SVT, published 2014-12-12, visited 2020-05-19.

Lexino, Powered by Oxford, "*Archive",* <https://www.lexico.com/definition/archive>*,* visited 2020-05-10.

The Organisation for Economic Co-operation and Development, "*In the Public Interest: Taking Integrity to Higher Standards – opening remarks at the 2017 OECD Global Anti-Corruption & Integrity Forum",* <https://www.oecd.org/about/secretary-general/taking-integrity-to-higher-standards-opening-remarks-2017-oecd-global-anti-corruption-integrity-forum.htm>, published 2017-03-30, visited 2020-04-18.

Transparency International, *Germany: "Whistleblower Prize 2013 for Edward Snowden",* <https://www.transparency.org/en/press/transparency-international-germany-whistleblower-prize-2013-for-edward-snow>, published 2013-07-25, visited 2020-05-19.

Transparency International, "*Corruption and the Coronavirus – How to prevent the abuse of power during a global health pandemic",* <https://www.transparency.org/news/feature/corruption_and_the_coronavirus>, published 2020-03-18, visited 2020-03-20.

Transparency International, "*Coronavirus sparks high risk of corruption across Latin America",* <https://www.transparency.org/news/pressrelease/coronavirus_sparks_high_risk_of_corruption_across_latin_america>, published 2020-03-26, visited 2020-03-30.

Transparency International, "*Grand Corruption",* <https://www.transparency.org/en/corruptionary/grand-corruption>, visited 2020-04-02.

Transparency International, "*Petty Corruption",* <https://www.transparency.org/en/corruptionary/petty-corruption>, visited 2020-04-02.

Transparency International, "*What is corruption?",*
<https://www.transparency.org/en/what-is-corruption>*,* visited 2020-04-02.

Regeringskansliet, Finansdepartementet, "*Om förslaget korttidspermittering",*
<https://www.regeringen.se/artiklar/2020/03/om-forslaget-korttidspermittering/>*,* published 2020-03-16, visited 2020-04-13.

Viklund, Lars, "*EU-direktiv om visselblåsare på väg"*,
<https://pro-karnovgroup-se.ludwig.lub.lu.se/b/documents/2954412?dq=Ny%20Juridik%201%3A19&q=Ny%20Juridik%201%3A19&t=literature_for#NYJUR_2019_1_S_0035>
, Ny Juridik 1:19, published 2019, visited 2020-02-01.

Timmons, John & Hickman, Tim, "*COVID-19 and Data Protection Compliance",*
<https://www.whitecase.com/publications/alert/covid-19-and-data-protection-compliance>, White & Case London, published 2020-03-26, visited 2020-04-01.

The United Nations, "*Handbook on Practical Anti-Corruption measures for prosecution and investigators",*
<https://www.unodc.org/documents/afghanistan/Anti-Corruption/Handbook_practical_anti-corruption.pdf>*,* Vienna, published 2004-09, visited 2020-04-14.

The United Nations Office on Drugs and Crime, "*Links between organized crimes and corruption",*
<https://www.unodc.org/e4j/en/organized-crime/module-4/key-issues/links-to-corruption.html>*,* published 2018-04, visited 2020-04-18.

The United Nations Office on Drugs and Crime, "*Investigations of corruption, Handling reports as a precondition for successful investigations",*
<https://www.unodc.org/e4j/en/anti-corruption/module-6/key-issues/investigation-of-corruption.html>, published 2020-01, visited 2020-04-14.

Table of cases:

Case C-131/12, "*Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos and Mario Costeja González*", EU:C:2014:317. (Google Spain).

C-293/12, "*Digital Rights Ireland Ltd vs. Minister of Communications with others",* EU:C:2014:238. (Digital Rights Ireland).

C-41/74, "*Yvonne Van Duyn vs. Home Office",* EU:C:1974:133. (Van Duyn vs. Home Office).