Dissertation Title

“The application and setting of administrative fines for the purposes of the Regulation 2016/679 (General Data Protection Regulation)”

Aikaterini Margariti

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES
A thesis submitted for the degree of
Master of Laws (LL.M.) in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation

February 2019
Thessaloniki – Greece
I hereby declare that the work submitted is mine and that where I have made use of another’s work, I have attributed the source(s) according to the Regulations set in the Student’s Handbook.

February 2019
Thessaloniki - Greece
Abstract

This dissertation was written as part of the LL.M. in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation at the International Hellenic University.

This Dissertation deals particularly with the administrative fines that are imposed by the supervisory authorities in case of infringement of the General Data Protection Regulation’s provisions. To help the unfamiliar reader understand the notions and the purposes of this new Regulation, this thesis provides a general description of the basic terms and tracks the changes between the previous legal regime and the Regulation. Following, it examines the basic principles set out in the GDPR for the imposition of administrative fines and it analyzes in detail the two different levels of fines indicated in article 83 paragraphs 4 and 5, presenting every provision the infringement of which could lead to those fines.

Subsequently, this research investigates the different approach when the fines are imposed on natural persons or undertakings and examines thoroughly the assessment criteria used by the supervisory authorities when deciding the imposition of a fine. Finally, the thesis explores the rest of the provisions of article 83 GDPR, as well as article 84 and it concludes on the importance of the administrative fines to ensure compliance with the General Data Protection Regulation.

Aikaterini Margariti

10th of February 2019
Preface

This dissertation could not have been finished without the help and support of my supervisor professor, the academic staff, the academic library of International Hellenic University, and my family. It is my great pleasure to acknowledge people who have given me guidance, help and support and who have faith in me.

First of all, I would like to express my sincere appreciation and deepest gratitude to my supervisor professor Dr. Komninos G. Komnios for his extremely valuable guidance and suggestions, which were very helpful and precious to me in order to finish this dissertation.

Similarly, I would like to thank professor Dr. Athanasios Kaissis for providing me with the opportunity to attend the LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation, which enabled me to acquire valuable knowledge on international commercial law, banking law and ADR, and also for his encouragement and unwavering support all the way through our studies at the LLM program.

Special thanks should be given to the Academic Library of International Hellenic University, which provided me with variety of resources, the Library Staff, the Academic Staff and Assistants in general, who were always willing to help me and guide me through my research.

Of course, I am deeply grateful to my family, my parents and my brother. They always stand by me, urge me to reach my goals, have faith in me (even when I don't) and encourage me to overcome myself. They are my inspiration.

Last but certainly not least, I would like to thank my friends for being there wherever I needed them. Without their support and encouragement during all this process I would not be able to complete this Dissertation.

Aikaterini Margariti

10th of February 2019
Contents

ABSTRACT .............................................................................................................................. III

PREFACE ................................................................................................................................. V

INTRODUCTION ......................................................................................................................... 1

1. PERSONAL DATA BREACHES LEADING TO IMPOSITION OF SANCTIONS .............. 5
   1.1. PERSONAL DATA BREACHES ......................................................................................... 5
   1.2. SANCTIONS IMPOSED UNDER THE DATA PROTECTION DIRECTIVE (DIRECTIVE 95/46/EC) .... 6
   1.3. SANCTIONS IMPOSED UNDER THE GENERAL DATA PROTECTION REGULATION ............ 7
      1.3.1. THE CORRECTIVE MEASURES OF ARTICLE 58 PARAGRAPH 2 GDPR ....................... 7
      1.3.2. THE ADMINISTRATIVE FINES OF ARTICLE 83 GDPR ............................................. 8

2. BASIC PRINCIPLES CONCERNING THE IMPOSITION OF SANCTIONS ............ 11
   2.1. IMPOSITION OF “EQUIVALENT SANCTIONS” ............................................................. 11
   2.2. “EFFECTIVE, PROPORTIONATE AND DISSUASIVE” ADMINISTRATIVE FINES .................... 12
   2.3. ASSESSMENT OF EACH INDIVIDUAL CASE ................................................................ 12
   2.4. ACTIVE PARTICIPATION AND INFORMATION EXCHANGE AMONG SUPERVISORY AUTHORITIES... 13

3. THE REGULATION’S TIERING SYSTEM ............................................................................ 15
   3.1. LEVEL 1 FINES – INFRINGEMENTS OF ARTICLE 83 PAR. 4 .......................................... 15
      3.1.1. THE OBLIGATIONS OF THE CONTROLLER AND THE PROCESSOR CONCERNING: .................. 15
      3.1.2. THE OBLIGATIONS OF THE CERTIFICATION BODY PURSUANT TO ARTICLE 42 AND 43 GDPR. 16
      3.1.3. THE OBLIGATIONS OF THE MONITORING BODY PURSUANT TO ARTICLE 41 PAR. 4 GDPR..... 16
   3.2. LEVEL 2 FINES – INFRINGEMENTS OF ARTICLE 83 PAR. 5 AND PAR. 6 ....................... 17
      3.2.1. THE BASIC PRINCIPLES FOR PROCESSING, INCLUDING CONDITIONS FOR CONSENT, PURSUANT TO ARTICLES 5, 6, 7 AND 9; .................................................................................................................. 18
      3.2.2. THE DATA SUBJECTS’ RIGHTS PURSUANT TO ARTICLES 12 TO 22; ......................... 18
      3.2.3. THE TRANSFERS OF PERSONAL DATA TO A RECIPIENT IN A THIRD COUNTRY OR AN INTERNATIONAL ORGANIZATION PURSUANT TO ARTICLES 44 TO 49; ......................................................... 19
      3.2.4. ANY OBLIGATIONS PURSUANT TO MEMBER STATE LAW ADOPTED UNDER CHAPTER IX; ...... 20
3.2.5. **Non-compliance with an order or a temporary or definitive limitation on**  
processing or the suspension of data flows by the supervisory authority pursuant to  
Article 58(2) or failure to provide access in violation of Article 58(1). ....... 20
3.2.6. **Article 83 paragraph 6 of the GDPR** ........................................ 20
3.3. **Infringement of several provisions** .............................................. 21

4. **THE RECEIVER OF THE ADMINISTRATIVE FINES** .................... 23

4.1. The administrative fine is imposed on a person ............................... 23
4.2. The administrative fine is imposed on an undertaking ....................... 23

5. **Assessment Criteria for the imposition of the Administrative Fines** .... 27

5.1. The nature, gravity and duration of the infringement ...................... 27
5.1.1. The scope or purpose of the processing concerned ....................... 29
5.1.2. As well as the number of data subjects affected ............................ 30
5.1.3. The level of damage suffered by them ........................................ 30
5.2. The intentional or negligent character of the infringement .............. 30
5.3. Any action taken by the controller or processor to mitigate the damage suffered by data subjects ............................................................ 31
5.4. The degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32 ................................................................. 32
5.5. Any relevant previous infringements by the controller or processor ...... 32
5.6. The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement ........................................... 34
5.7. The categories of personal data affected by the infringement .......... 34
5.8. The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement ................................................................. 35
5.9. Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures ................................................................. 36
5.10. **Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42** ................. 37
5.11. Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. ................................................................. 38

6. THE PROVISIONS OF PARAGRAPHS 7, 8 AND 9 OF ARTICLE 83 OF THE GDPR ....... 41

6.1. The imposition of administrative fines on public authorities – Article 83 par. 7 GDPR 41

6.2. Judicial remedy and due process – Article 83 par. 8 GDPR ................................. 42

6.3. The Member State’s national law not providing for administrative fines – Article 83 par. 9 GDPR ........................................................................................................... 43

7. THE IMPOSITION OF OTHER PENALTIES .............................................................. 45

8. CONCLUSIONS ........................................................................................................ 47

BIBLIOGRAPHY ......................................................................................................... 49
Introduction

In 2019 we live in the Internet era, where the technological and social phenomena (such as social networks, cloud computing, the new possibilities of data mining and big data analysis) have created new ways for data processing, since the technical infrastructure of the Internet in combination with the ever-advancing computer technology facilitate the collection, processing and use of vast amounts of personal data\(^1\), making personal data a valuable asset due to their nature, which allows them to easily cross borders and makes them essential to the global digital economy\(^2\). The right to the protection of personal data is a fundamental right recognized by the EU legal order\(^3\) and should be separated by the right to respect for private life, despite their similarities (in any case of personal data processing the right to data protection is triggered, regardless the impact on privacy, while in order for the right to privacy to be activated, a private interest or the “private life” of an individual has to be compromised\(^4\)). It is clear that data protection is a flaming issue of everyday life and there are several rules set out around the world to ensure this protection.

In the European Union the European Data Protection Directive (Directive 95/46/EC) was adopted in 1995 and it soon became a global leading paradigm for privacy protection. The Directive, that required that every EU Member State had to adopt “equivalent” to one another privacy laws and that data could be exported to third party countries only under the condition that "an adequate level of protection" for European citizens' data could be ensured, had worldwide impact and influence. Nevertheless, two decades later and considering all the technological advances and

---

3 See article 8 of the EU Charter of Fundamental Rights.
the new possibilities of the Internet era, the Directive seemed out of date and could not adequately provide for the protection needed\(^5\).

Thus, the Data Protection Directive was replaced by the EU Regulation 2016/679, the General Data Protection Regulation (in short: GDPR). The GDPR was adopted in April 2016 after four years of discussions. The fact that it is a regulation is of high importance, since regulations are directly applicable to all their addressees and there is no need for any implementation measures to be adopted by the EU Member States\(^6\).

When the Data Protection Directive was in force, every Member State had its own legal system and judicial and enforcement culture, creating a confused and vague regulatory environment (not knowing which of the 28 different systems was applicable in every case). The GDPR on the other hand establishes a single legal framework throughout the EU, eliminating the legal uncertainty and making the system stable and coherent\(^7\).

The GDPR, which became effective on the 25\(^{th}\) of May 2018 deals with the problems that were created because of the non-uniform implementation of the Data Protection Directive and ensures that the citizens’ rights are preserved, while introducing new rights and obligations concerning the digital environment. The new Regulation also tries to strengthen some basic principles (such as transparency), to enhance the supervisory role of the Data Protection Authorities (DPAs) and covers the critical matter of personal data being transferred to non EU Member States, too. What is more, the GDPR aims at reducing the administrative burdens for DPAs and enterprises and at regulating the controllers’ and processors’ responsibilities and their liability, by introducing stricter sanctions and penalties\(^8\).

The GDPR did not alter the primary rules and principles that were set under the Data Protection Directive, nor the essence of fundamental concepts and the definition of some authorities. The Regulation also preserved the principles of “reason” and

---


\(^8\) Synodinou, 2017, p. 5.
“security” while the main subject of the legislation was the absolute control over the personal data. However, the GDPR introduced a major reform concerning the administrative fines that could be imposed in case of violation of the Regulation’s provisions, involving a significant increase compared to the prior regime (under the Data Protection Directive). The fact that they can go up to 20 million euro or to 4% of the total worldwide annual turnover of an undertaking made the administrative fines for the purposes of the General Data Protection Regulation one of the most discussed topics of today.

The aim of this thesis is to define in which cases it is necessary to set some administrative fines and their maximum levels in order to ensure the better application and enforcement of the General Data Protection Regulation. Moreover to make perfectly clear the necessity for compliance with GDPR for all Member States and to determine whether the application of administrative fines in case of infringement will prove helpful in order to achieve this goal.

Thus, this thesis consists of eight Chapters, each placed in a logical order to guide the reader through the topic. After this introduction, Chapter 1 explores some of the GDPR’s general terms, such as “personal data” and “data breach”, and overviews the imposition of sanctions under the Personal Data Directive and the corrective measures and administrative fines provided for under the General Data Protection Regulation. In Chapter 2 the basic principles set out in the GDPR are presented, while Chapter 3 includes an analysis of the two levels of administrative fines indicated in article 83 GDPR and of all the provisions, the violation of which could lead to the imposition of these fines. Thereafter, Chapter 4 examines the receiver of the administrative fines and interprets the notion of the “undertaking” under the Regulation. In Chapter 5 the assessment criteria set out in article 83 par. 2 GDPR are described in detail and Chapter 6 deals with the issues of administrative fines being imposed on public authorities, the procedural safeguards against the supervisory authorities’ decisions and some Member States’ national laws not providing for administrative fines. Finally, Chapter 7 provides for a brief analysis of the other penalties that may apply to this

---

Regulation’s infringements, while Chapter 8 includes the Conclusions and some final remarks.
1. Personal Data Breaches leading to imposition of Sanctions

The General Data Protection Regulation (hereafter GDPR) concerns the protection of natural persons with regard to the processing of personal data and the free movement of such data\textsuperscript{10}, by personal data meaning “any information relating to an identified or identifiable natural person (‘data subject’)”\textsuperscript{11}. Hence, the Regulation’s provisions apply only to the protection of natural persons’ personal data, not covering the processing of legal\textsuperscript{12} or deceased persons’ data\textsuperscript{13}. According to article 3 of the GDPR the Regulation applies to the processing of (a) “personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not”, or (b) “personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, or to the monitoring of their behavior as far as their behavior takes place within the Union”, or (c) “personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law”. So, in order to strengthen the enforcement of the Regulation, the supervisory authorities may impose sanctions in the case that a controller\textsuperscript{14} or a processor\textsuperscript{15} infringes one of its provisions\textsuperscript{16}.

1.1. Personal Data Breaches

According to article 4 no. 12’s definition a personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized

\textsuperscript{10} See article 1 par. 1 GDPR.
\textsuperscript{11} See article 4, no. 1 GDPR.
\textsuperscript{12} See Recital 14 GDPR.
\textsuperscript{13} See Recital 27 GDPR.
\textsuperscript{14} A controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, according to Article 4, no. 7 of the GDPR.
\textsuperscript{15} A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, according to Article 4, no. 8 of the GDPR.
\textsuperscript{16} See Recital 148 GDPR.
disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

Such a breach could be the outcome of accidental or deliberate causes and would affect the confidentiality, integrity or availability of personal data. A data breach would occur in case any personal data was lost, destroyed, corrupted, disclosed, passed on without proper authorization or was made unavailable. In case of any personal data breach the GDPR introduces the controller’s or processor’s obligation of notification towards the supervisory authorities “without undue delay and not later than 72 hours after having become aware of it” and towards the data subject (“if the personal data breach is likely to result in a high risk to the natural persons’ rights and freedoms”) “without undue delay”, so that the rights and freedoms of the data subject are protected through a better level of transparency. The failure to notify the supervisory authority (or the data subject if needed) on time is punishable with sanctions imposed by the GDPR. A sanction could be a corrective measure, an administrative fine or even a criminal penalty, depending on each individual case’s circumstances.

1.2. Sanctions imposed under the Data Protection Directive (Directive 95/46/EC)

The Data Protection Directive did not require for specific sanctions for the violations of its provisions, but left their regulation to each Member State’s discretion. Article 24 of the Directive indicates that “The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive”. Hence, every Member State implemented its own sanctions in their national laws, resulting in big contrasts on the maximum level that

18 Ibid.
19 See article 33 par. 1 GDPR.
20 See article 34 par. 1 GDPR.
21 Voigt, 2017, pp. 65-seq.
22 See article 24 of the Directive 95/46/EC.
could be imposed among the Member States. The consequence of this provision was that there were 28 different administrative and judicial systems in the EU, not allowing the DPAs to have equal enforcement powers and thus creating legal uncertainty.

1.3. Sanctions imposed under the General Data Protection Regulation

On the other hand the GDPR sets out uniform rules addressed to all Member States concerning the imposition of sanctions in case of infringement of its provisions and in order to strengthen its rules. More specifically, Recital 148 indicates that “administrative fines may be imposed by the supervisory authorities in addition to or instead of other appropriate measures”. So, the Regulation provides to the supervisory authority the possibility to impose sanctions, including high administrative fines and criminal penalties in addition to or instead of other corrective measures, according to article 58 par. 2 (i) GDPR.

1.3.1. The corrective measures of Article 58 paragraph 2 GDPR

Article 58 paragraph 2 of the Regulation includes a list with the supervisory authority’s corrective powers against alleged violations of the GDPR’s provisions. According to the said article these powers are:

(a) to issue warnings to a controller or processor whose intended processing operations are likely to infringe the GDPR;

(b) to issue reprimands to a controller or processor where their processing operations have infringed the GDPR;

(c) to order the controller or the processor to comply with the data subject’s requests to exercise its rights under the GDPR.

---


24 See Recital 148 GDPR.


27 See articles 12 to 23 GDPR for the Data Subject’s rights.
(d) to order the controller or processor to bring processing operations into compliance with the GDPR, where appropriate, in a specified manner and within a specified period;
(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation, including a ban on processing;
(g) to order the rectification, erasure or restriction of processing of personal data pursuant to Arts. 16 to 18 GDPR and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to articles 17 par. 2 and 19;
(h) to withdraw a Certification or order the certification body to withdraw a certification issued pursuant to articles 42 and 43, or to order the certification body not to issue a Certification if the necessary requirements are not or no longer met;
(i) to impose an administrative fine pursuant to Art. 83 GDPR, in addition to, or instead of other corrective measures referred to above, depending on the circumstances of each individual case;
(j) to order the suspension of data flows to third country recipients or to an international organization.  

The provisions under (a) and (b) are the least severe corrective measures since no direct obligations for the controller or the processor are triggered to ceasing or altering their processing activities. In fact, the GDPR seems to guide the supervisory authorities to impose the above mentioned reprimands in cases of minor infringements, while preferring to impose administrative fines when more severe infringements occur.

1.3.2. The administrative fines of Article 83 GDPR

Recital 150 of the GDPR states that “in order to strengthen and harmonize administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related

---

28 See article 33 GDPR.
29 See article 58 par. 2 GDPR.
31 See Recital 148 second sentence GDPR.
administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement”. Hence, article 83 of the GDPR indicates the level of fines, the total maximum ceilings of the fine to be imposed and the circumstances that have to be taken into account by the national authorities when deciding whether to impose a fine or not\(^\text{32}\). These provisions ensure a harmonized sanctioning regime across the European Union, leaving it to Member States to set out the rules on other penalties for violations that are not subject to administrative fines\(^\text{33}\).


2. Basic Principles concerning the imposition of sanctions

In the case of violation of one of the provisions of the GDPR the competent supervisory authority has to determine which corrective measure(s) properly addresses the infringement. The supervisory authority has at its disposal many tools as described in article 58 par. 2, elements (a)-(j) of GDPR (one of which is the imposition of administrative fines\(^{34}\)) in order to deal with the controller’s or processor’s non-compliance and should always have in mind the following principles\(^{35}\):

2.1. Imposition of “equivalent sanctions”

Recital 10 of the GDPR indicates that “in order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection should be equivalent in all Member States”\(^{36}\). Also, Recital 11 requires “equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States”\(^{37}\) in order for an equivalent level of protection to be achieved. Furthermore, Recital 13 of the GDPR argues that the application of equivalent sanctions in every Member State and their supervisory authorities’ cooperation is a way “to prevent divergences hampering the free movement of personal data within the internal market”\(^{38}\).

It is obvious that the sanctions imposed being equivalent is a matter of high importance for the establishment of consistency when the supervisory authorities use their corrective powers. The Regulation demands that controllers and processors cooperate trying to ensure the consistency of application and enforcement of the GDPR\(^{39}\). The cooperation mechanism that is set forth by the Regulation ensures the consistency in cross border cases, while in national cases the same guidelines will be

\(^{34}\) See article 58 par. 2 (i) GDPR.
\(^{36}\) See Recital 10 GDPR.
\(^{37}\) See Recital 11 GDPR.
\(^{38}\) See Recital 13 GDPR.
\(^{39}\) See article 57 par. 1 (g) GDPR.
applied by the supervisory authorities with a view to ensuring the consistency of application and enforcement of the Regulation\textsuperscript{40}.

2.2. “Effective, proportionate and dissuasive” administrative fines

The first paragraph of article 83 of the GDPR indicates that the administrative fine imposed on a case should be effective, proportionate and dissuasive according to the parameters of the specific case\textsuperscript{41}. It is only reasonable that the nature, the gravity and the consequences of the breach are taken into consideration and that all the facts of the case are assessed by the supervisory authority in a manner that is consistent and objectively justified before the imposition of the administrative fine\textsuperscript{42}. What is more, the supervisory authority will assess what is effective, proportional and dissuasive in each case based on the objective pursued by the corrective measure chosen, which can be either to reestablish compliance with the rules, or to punish unlawful behavior or even both of them\textsuperscript{43}. This procedure should be followed when the supervisory authority deals with both national cases and cases involving cross-border processing of personal data. Moreover, it is acknowledged that a Member State’s national legislation may require additional conditions on the enforcement procedure such as address notifications, deadlines for making representations, appeal etc. Nevertheless, the achievement of effectiveness, proportionality or dissuasiveness should not under any circumstance be deterred due to such requirements\textsuperscript{44}.

2.3. Assessment of each individual case

There is a wide range of infringements (included in article 83 par. 4-6) that could cause the imposition of administrative fines. Additionally, the infringement of other provisions than those mentioned in article 83 par. 4-6 could justify the imposition of administrative fines if a Member States’ national law allowed so. Either way, when a

\textsuperscript{40} Article 29 WP, p. 5.
\textsuperscript{41} See article 83 par. 1 GDPR.
\textsuperscript{42} Article 29 WP, p. 6.
\textsuperscript{43} Ibid.
\textsuperscript{44} Ibid.
provision of the GDPR has been violated, the supervisory authority has to assess all the facts of the case individually. In article 83 par. 2 it is stated that “when deciding whether to impose an administrative fine, and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following…”\(^{45}\). Recital 148 of the GDPR also emphasizes the supervisory authority’s responsibility to choose the most appropriate measure(s)\(^{46}\). During this process the supervisory authority has to consider all of the corrective measures that there are at its disposal and choose to impose the administrative fine either in addition to a corrective measure (of those mentioned in article 58 par. 2) or on its own\(^{47}\).

Fines should be used in appropriate circumstances and on a balanced approach in order for an effective and dissuasive as well as a proportionate reaction to the infringement to be achieved. However, this does not mean that the administrative fines should be used as a last resort and that the supervisory authorities should be discouraged from issuing fines. Fines should be used in ways that preserve their effectiveness as a tool\(^{48}\).

### 2.4. Active participation and information exchange among Supervisory Authorities

In some Member States the national supervisory authorities did not have fining powers in case of data breaches before the GDPR and thus this new procedure raises various issues in terms of resources and organization. This is why each Member State’s supervisory authority should participate to the cooperation mechanisms set out in the Regulation and collaborate with other Member States’ supervisory authorities and the European Commission (when required) in order to support formal and informal information exchanges and help those who need it. For instance, in the case that a supervisory authority’s decision is subject to appeal before national courts, the supervisory authority could use another Member State’s greater experience through the proactive information sharing and the case law on the use of the fining powers to

\(^{45}\) See article 83 par. 2 GDPR.
\(^{46}\) See Recital 148 GDPR.
\(^{47}\) Article 29 WP, p. 6-7.
\(^{48}\) Ibid p. 7.
deal with it. This cooperation and information exchange results in a higher level of consistency and a harmonized approach towards the administrative fines is achieved\textsuperscript{49}.

\textsuperscript{49} Ibid p.8.
3. The Regulation’s tiering system

The General Data Protection Regulation sets uniform rules applicable to all Member States concerning the potential administrative fines in case of infringement of the Regulation’s provisions. Compared to earlier drafts, the administrative fines that are designated in article 83 of the GDPR appear to have been significantly increased. The new Regulation sets out two different levels of administrative fines.\(^{50}\)

3.1. Level 1 fines – infringements of article 83 par. 4

Article 83 par. 4 of the GDPR indicates that “infringements of the following provisions shall be subject to administrative fines up to 10,000,000 euros, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher”\(^{51}\). This frame is set for violations of the following provisions:

3.1.1. The obligations of the controller and the processor concerning:

(a) The conditions applicable to child’s consent in relation to information society services, as for children’s consent to be lawful, stricter conditions have to be met. Article 8 of the Regulation introduces special conditions concerning children’s consent in relation to information society services. When the processing of a child’s personal data aims to marketing purposes or to creating personality or user profiles and when their data are collected using services directly offered to a child, specific protection for should apply for the child’s data.\(^{52}\)

(b) The processing which does not require identification. Pursuant to article 11 of the GDPR a controller whose processing purposes do not or no longer require the identification of a data subject shall not be obliged to maintain, acquire or process the additional information that could lead to the identification of the data subject.\(^{53}\)

---


\(^{51}\) See Article 83 par. 4 GDPR.

\(^{52}\) Voigt, 2017, p. 98.

(c) The controller’s or processor’s general obligations (article 25 – 31 GDPR), the obligations relating to the security of personal data (article 32 – 34 GDPR), the data protection impact assessment and prior consultation (article 35 – 36 GDPR), the data protection officer (article 37 – 39 GDPR),
(d) The certification (article 42 GDPR) and
(e) The certification bodies (article 43 GDPR).

3.1.2. The obligations of the certification body pursuant to article 42 and 43 GDPR.

The certifications bodies, which are accredited by the competent supervisory authorities for a maximum of 5 years, with the possibility to renew their accreditation, are one of the bodies (other than the supervisory authorities and the European Data Protection Board) that may carry out the certification procedure. For the accreditation of a certification body to be completed, it has to meet the requirements set out in article 43 par. 2 of the GDPR and the further detailed criteria that will be defined by the competent supervisory authority. The supervisory authority may revoke the accreditation in case the certification body fails to meet or no longer meets the accreditation’s conditions or where the body’s actions infringed one of the provisions of the GDPR. The certification bodies have to inform the supervisory authority about issuing and renewing a Certification and are responsible for the proper assessment that could lead to a Certification or its withdrawal, while providing the supervisory authority with reasons determining the granting or withdrawal of the requested Certification.

3.1.3. The obligations of the monitoring body pursuant to article 41 par. 4 GDPR.

According to article 41 par. 1 of the GDPR the competent supervisory authority may accredit independent bodies to monitor compliance with a code of conduct. The

---

54 Ibid p. 78.
55 Ibid.
56 Ibid.
57 Ibid.
monitoring bodies have to take appropriate actions in case of an infringement of the code of conduct by a controller or a processor and shall inform the competent supervisory authority of such actions\textsuperscript{58}. A monitoring body may be accredited to monitor compliance with a code of conduct when the body meets the conditions indicated in the second paragraph of article 41 GDPR, as well as the conditions set out by the competent supervisory authority and shall lose its accreditation shall if it does not meet or no longer meets the conditions for accreditation or where its actions infringed the Regulation\textsuperscript{59}. The monitoring bodies may permit the supervisory authorities to reduce their workload, since they will be monitoring an entity’s compliance with the codes of conduct, while the supervisory authorities will monitor the entity’s compliance with the GDPR\textsuperscript{60}.

In case of violation of one of the above mentioned obligations a controller or processor may be punished with fines of up to 10 million euro or up to 2% of the total worldwide annual turnover (in the case of an undertaking) pursuant to article 83 par. 4 of the GDPR.

3.2. Level 2 fines – infringements of article 83 par. 5 and par. 6

The fifth paragraph of article 83 GDPR includes a list of more serious violations and thus sets the maximum level of administrative fines “up to 20.000.000 euro or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding year, whichever is higher”\textsuperscript{61}. These higher administrative fines are imposed in case of infringements concerning\textsuperscript{62}:

\textsuperscript{58} See article 41 par. 4 GDPR
\textsuperscript{59} Voigt, 2017, p. 75-76.
\textsuperscript{60} Ibid.
\textsuperscript{61} Rücker, 2018, pp.186-seq.
\textsuperscript{62} See article 83 par. 5 GDPR.
3.2.1. The basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

The basic principles that shall govern any data processing activity under the Regulation are established in article 5 GDPR and demand that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject and shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Furthermore, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, accurate and, where necessary, kept up to date, kept in a form that permits identification of data subjects for no longer than necessary for the processing purposes and be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures. Also, the lawfulness of the processing should be guaranteed by applying at least one of the provisions of article 6 par. 1 GDPR, as well as the conditions for consent as set out in article 7 of the Regulation. Finally, in the case of processing special categories of data the controller or the processor has to meet all the requirements of article 9 GDPR.

3.2.2. The data subjects' rights pursuant to Articles 12 to 22;

The data subject’s rights are found under Chapter 3 of the Regulation and are as follows: the information provided to the data subject shall increase the transparency of data processing activities for individuals and permit them to effectively exercise their rights and the data subject shall be informed of the existence of any processing

---

63 See article 5 par. 1 (a) GDPR.
64 See article 5 par. 1 (b) GDPR.
65 See article 5 par. 1 (c) GDPR.
66 See article 5 par. 1 (d) GDPR.
67 See article 5 par. 1 (e) GDPR.
68 See article 5 par. 1 (f) GDPR.
69 See article 12 GDPR.
operations on its personal data when they are collected from the data subject\textsuperscript{70} and when they have not been obtained by the data subject\textsuperscript{71}. Also, there are the rights of access by the data subject\textsuperscript{72}, the right to rectification\textsuperscript{73}, the right to erasure\textsuperscript{74}, the right to restriction of processing\textsuperscript{75} and the right to be notified regarding rectification re erasure of personal data or restriction of processing\textsuperscript{76}, as well as the right to data portability\textsuperscript{77}, the right to object\textsuperscript{78} and the right not to be subject to a decision based solely on automated processing\textsuperscript{79}. In case of infringement of any of these rights an administrative fine could be imposed pursuant to article 83 par. 5 GDPR.

3.2.3. The transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49;

It is only logical that multinational entities and corporations include cross-border data transfers in the course of their business activities, transferring data even to third countries that are not EU Member States\textsuperscript{80}. For a cross-border data transfer to be justified the transfer has to correspond to the requirements for data processing within the EU and to be based on the data subject’s consent and the transfer has to additionally comply with the conditions laid down in articles 44 et seq. GDPR\textsuperscript{81}. Hence, the Regulation ensures a high level of data security. The importance of the protection of the personal data that are transferred to third countries is made clear by the EU legislator punishing the infringement of articles 44 to 49 with the vast fines of the fifth paragraph of article 83 GDPR\textsuperscript{82}.

\begin{thebibliography}{99}
\bibitem{70} See article 13 GDPR.
\bibitem{71} See article 14 GDPR.
\bibitem{72} See article 15 GDPR.
\bibitem{73} See article 16 GDPR.
\bibitem{74} See article 17 GDPR.
\bibitem{75} See article 18 GDPR.
\bibitem{76} See article 19 GDPR.
\bibitem{77} See article 20 GDPR.
\bibitem{78} See article 21 GDPR.
\bibitem{79} See article 22 GDPR.
\bibitem{80} Voigt, 2017, p. 116-117.
\bibitem{81} Ibid.
\bibitem{82} Ibid.
\end{thebibliography}
3.2.4. Any obligations pursuant to Member State law adopted under Chapter IX;

Although the GDPR is a Regulation, in many cases it leaves the regulation of several matters to each Member State’s national law. The GDPR contains many opening clauses in its general provisions that explicitly leave room to national legislations (such as in article 6 par. 2, article 9 par. 4, article 84 par. 1 etc)\(^{(83)}\), but also articles 85 to 91 which include specific processing situations that are left to the competence of each Member State’s national legislation. The violation of one of these obligations by a controller or processor is punished by the fines indicated in article 83 par. 5, too.

3.2.5. Non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

Article 83 par. 5 (e) GDPR includes the case where the supervisory authority has already addressed one of the corrective measures under article 58 par. 2 to the controller or processor and they failed to comply with it, as well as the case where they should provide access to the supervisory authority according to article 58 par. 1 and failed to do so. The reason why such a high administrative fine may imposed on one of these cases is because the controller or processor had already had the chance to comply with the Regulation (by being punished with a lighter sanction), but still violated their obligations.

3.2.6. Article 83 paragraph 6 of the GDPR

Moreover, the same level of administrative fines (up to 20.000.000 euro or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding

\(^{(83)}\) Ibid p. 219-seq.
financial year, whichever is higher) is imposed also in the case of non-compliance with
an order by the supervisory authority as referred to in article 58 par. 2 of the GDPR\textsuperscript{84}.

3.3. Infringement of several provisions

Article 83 par. 3 states that “If a controller or processor intentionally or negligently, for
the same or linked processing operations, infringes several provisions of this
Regulation, the total amount of the administrative fine shall not exceed the amount
specified for the gravest infringement”. This provision regards the absorption or
accumulation of administrative fines and inserts the principle of culpability\textsuperscript{85}. The
article requires that the controller or processor “intentionally or negligently” breaches
the Regulation, making it clear that for an administrative fine to be imposed culpability
such as intent or negligence is required\textsuperscript{86}.

Moreover, for par. 3 of article 83 to be applied, the controller or processor has to
violate several provisions of the GDPR with the same or linked processing operations.
In this case the principle of absorption applies and the amount of the administrative
fine imposed should not excel the amount of the fine that would be imposed for the
gravest of the breaches\textsuperscript{87}. On the other hand, if the controller or processor infringed
several provisions of the GDPR by various processing operations that are not linked
to each other the applicable principle is not the principle of absorption, but the principle
of accumulation. Hence, the amounts of the fines of every violation will be added to
each other and the third paragraph of article 83 of the GDPR will not apply\textsuperscript{88}.

3.4 Conclusions

The differentiation of the higher level of the fines in paragraphs 4 – 6 of article 83 of
the GDPR indicate that the breaches of paragraph 4 are considered to be lighter than
those of paragraph 5. However, the violation of an obligation set out in par. 4 may be
subject to level 2 administrative fines, if it was previously dealt with by an order of the

\textsuperscript{84} See article 83 par. 6 GDPR.
\textsuperscript{85} Feiler Lukas, Forgo Nikolaus, Weigl Michale “The EU General Data Protection
\textsuperscript{86} Ibid.
\textsuperscript{87} Ibid.
\textsuperscript{88} Ibid p. 295-296.
supervisory authority according to article 58 par. 2, nevertheless the controller or the processor did not comply with that order\textsuperscript{89}.

At this point it is important to state that these three paragraphs of article 83 of the GDPR set out the upper limit of the administrative fines that can be imposed in case of infringement of one of the above mentioned provisions. So, every violation of the Regulation will not be fined with 10 or 20 million euro nor 2\% or 4\% of the undertaking’s worldwide annual turnover accordingly, but the administrative fine could be a lot smaller than these sums, as long as it is appropriate for the specific breach (effective, proportionate and dissuasive\textsuperscript{90}) and the objective pursued by the supervisory authority is achieved. Thus, the competent supervisory authority is the one who determines the imposition and the amount of the administrative fine in each individual case\textsuperscript{91}.

\textsuperscript{89} Iglezakis, 2018, p. 235.

\textsuperscript{90} See chapter 2.2 p.12 of this Thesis.

\textsuperscript{91} See Recital 150 GDPR.
4. The receiver of the administrative fines

An infringement of one of the Regulation’s provisions could lead to the imposition of administrative fines. Recital 150 of the GDPR states that the supervisory authority can impose an administrative fine to a natural person or to an undertaking.

4.1. The administrative fine is imposed on a person

According to Recital 150: “Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine”. The EU legislator made sure that there is a different treatment when the administrative fines are imposed to natural persons, setting some special requirements before the imposition. First, the supervisory authority should take into consideration the general level of income in the Member State where the person who violated the provision of the Regulation lives in, before the decision on the amount of fine is made. Then, the supervisory authority should evaluate the specific individual’s economic situation, too, so that the administrative is not of unbearable burden to him. This provision stays in line with the basic principles of GDPR that the administrative fine imposed should be effective, proportionate and dissuasive and that there should be an assessment of every individual case in order to impose the appropriate fine.

4.2. The administrative fine is imposed on an undertaking

Article 83 of the GDPR indicates that in the case that an infringement is made by an undertaking the administrative fines can go up to 2% (for breaches mentioned in par. 4) or 4% (for breaches of par. 5 and 6) of the total worldwide annual turnover of the preceding financial year. Pursuant to Recital 150 of the GDPR “an undertaking should

---

92 See Recital 150, 4th sentence of the GDPR.
be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes”\textsuperscript{93} and thus the term undertaking should be used as the term undertaking under EU competition law. So, the notion “undertaking” includes not only legal entities but also encloses any entity engaged in an economic activity, disregarding the entity’s legal status and its way of finance\textsuperscript{94}. In this way, when there is a controlled entity that has decisive influence concerning the data processing activities of its controlled undertakings, the different entities might be considered as a single ‘undertaking’ under article 83 of the GDPR\textsuperscript{95}. Of course, such an interpretation of the term “undertaking” would affect gravely the calculation of the maximum amount of administrative fines. Taking into consideration the turnover of an undertaking (being interpreted under article 101 et seq. of TFEU) practically means that the basis of the calculation will be the global group-wide turnover\textsuperscript{96}. For example, in case of violation of article 83 par. 5 of the GDPR (which provides for administrative fines up to 4% of the turnover) by an undertaking that is part of a group with a total annual worldwide turnover of 2 billion euro, a fine of 80 million euro could be imposed to the undertaking, since the worldwide annual turnover of the entire group of companies will be considered for the calculation of the fine.

The fact that the term “undertaking” is interpreted in accordance with article 101 et seq. of the TFEU means that the antitrust term of “undertaking” applies\textsuperscript{97}. With regard to the case law of the Court of Justice of the European Union (CJEU) on antitrust law, the term “undertaking” has significant consequences on the attribution of infringements\textsuperscript{98}. According to CJEU’s case law, when a controlled entity (that does not make its own decisions concerning data protection based on its own conduct on the market, but follows the instructions of its mother company) violates antitrust law, the parent company is co-responsible for the controlled entity’s anticompetitive actions. In such a case, as well as in case of wholly-owned subsidiaries, the supervisory authority could calculate the amount of the fine based on the total worldwide turnover of the

\textsuperscript{93} Ibid, 3\textsuperscript{rd} sentence.
\textsuperscript{94} Voigt, 2017, p. 212.
\textsuperscript{95} Ibid.
\textsuperscript{96} Feiler, 2018, p. 296.
\textsuperscript{97} Ibid.
\textsuperscript{98} Ibid.
group of entities and impose the administrative fine on the parent/controlling company\(^99\).

However, it is well known that the Recitals have no force of law, but are just some preliminary statements that introduce the main parts of the legislation they are part of. Keeping that in mind and based on article 4 no 19’s definition on the ““group of undertakings” meaning a controlling undertaking and its controlled undertakings”\(^100\) some argue that every group entity should face its own administrative fines which should be calculated based on its own total worldwide annual turnover\(^101\).

---

\(^{99}\) Ibid pp. 296-297.

\(^{100}\) See article 4 no. 19 GDPR.

\(^{101}\) Voigt, 2017, p. 213.
5. Assessment criteria for the imposition of the administrative fines

The General Data Protection Regulation introduces in article 83 par. 2 a list of criteria that should be used by the supervisory authorities in order to decide whether an administrative fine should be imposed or not and, if so, to determine the amount of the fine\textsuperscript{102}. This list is non-exhaustive and contains factors that are relevant for sentencing\textsuperscript{103}. Firstly, the supervisory authorities have to assess whether there has been an infringement of the provisions set out in paragraphs 4 to 6 of article 83. Then, the authorities have to overview the criteria listed in the second paragraph of article 83, taking into consideration all the circumstances of each individual case and conclude on the imposition of the fine or not. If the supervisory authorities decide to impose a fine, they can use the first assessment’s results in their second evaluation regarding the amount of fine. In this way, they avoid a second assessment of the same criteria\textsuperscript{104}.

So, according to article 83 par. 2 “when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:"

5.1. The nature, gravity and duration of the infringement

The controller’s and processor’s obligations issued in the GDPR are categorized based on their nature in paragraphs 4 to 6 of article 83. When the supervisory authorities assess the infringements of these provisions they may come to the conclusion that in the particular case a higher or a more reduced corrective measure needs to be imposed. If an administrative fine is chosen as the appropriate measure for the specific case, the nature of the breach will lead the supervisory authority to the tiering system

\textsuperscript{102} See article 83 par. 2 GDPR.
\textsuperscript{103} Feiler, 2018, p. 295.
\textsuperscript{104} Article 29 WP, p. 9.
of article 83 par. 4 – 6 of the GDPR to determine the higher administrative fine that can be imposed\textsuperscript{105}.

Recital 148 states at its second sentence: “in a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine”. A minor infringement may be a violation of one of the Regulation’s provisions listed in paragraphs 4 or 5 of article 83 that is assessed by the supervisory authority based on the criteria of article 83 par. 2 as not affecting the essence of the violated obligation. When a breach is evaluated as a minor infringement, the supervisory authority has the possibility (not an obligation) to replace the fine with a reprimand\textsuperscript{106}.

As far as the gravity of the infringement is concerned, the Regulation divides the violations in two categories, those of article 83 par. 4 and those of article 83 par. 5. The differentiation of the higher level of the fine that can be imposed in these cases indicates that the infringements of the 4\textsuperscript{th} paragraph have a relatively lower degree of gravity, compared to the ones included in par. 5 of article 83 GDPR\textsuperscript{107}. However, it is possible that a violation of one of the obligations set out in article 83 par. 4 is fined as a breach of one of the provisions of article 83 par. 5, when the violation in question had already been addressed in an order from the supervisory authority (according to article 83 par. 6 of the GDPR). The controller or processor’s failure to comply with this order is the reason why a breach with a lower level of gravity is treated as a more severe one\textsuperscript{108}. But, a violation’s gravity depends also on “the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them”\textsuperscript{109} and can be even affected by the national law of a Member State. Furthermore, in the case of infringement of several provisions by the same or linked processing operations the supervisory authority may apply an administrative fine within the limit of the gravest violation (according to article 83 par. 3 of the GDPR)\textsuperscript{110}. If for example, a controller or processor infringed with the same

\textsuperscript{105} Ibid.
\textsuperscript{106} Ibid.
\textsuperscript{107} Ibid.
\textsuperscript{108} Ibid p. 10.
\textsuperscript{109} See article 83 par. 2 (a) GDPR.
\textsuperscript{110} Article 29 WP, p. 10.
processing operation article 6 (listed in the obligations of article 83 par. 5) and article 11 (listed under article 83 par. 4), the supervisory authority may impose a fine up to 20 million euro or up to 4% of the total worldwide annual turnover (in the case of an undertaking), hence the fine corresponding to the gravest infringement (of article 6 of the GDPR).

The duration of an infringement may be indicative of certain facts such as that the data controller’s conduct was willful, or that the controller or the processor failed to take the appropriate preventive measures, or even that they could not put in place the technical and organizational measures that are required pursuant to article 24 of the GDPR\textsuperscript{111}. It is then clear that the duration of a violation should be taken into consideration when the supervisory authority decides about the imposition and the amount of a fine.

In addition to the nature, the gravity and the duration of the infringement article 83 par. 2 (a) indicates that the supervisory authority should also take into account:

5.1.1. The scope or purpose of the processing concerned

The scope or purpose of processing basically refers to the principle of purpose of limitation as set out in article 5 par. 1 (b) of the GDPR. This means that the reason for and the objective of the data collection has to be clear from the outset and in accordance with the existing law and that in the case of processing of personal data for a different purpose from the originally specified one, the new use has to be fair, lawful and transparent (purpose specification and compatible use)\textsuperscript{112}. The supervisory authority should examine if these two essential components of the principle are followed and even proceed to a deeper analysis of the purpose of the processing when assessing the criteria of article 83 par. 2 of the Regulation\textsuperscript{113}.

\textsuperscript{111} Ibid p. 11.
\textsuperscript{112} Voigt, 2017, pp. 88-90.
\textsuperscript{113} Article 29 WP, p. 11.
5.1.2. as well as the number of data subjects affected

The number of data subjects affected is an important element of the assessment since it can help the supervisory authority determine whether the infringement was an isolated event or part of a systematic breach. Of course, even an isolated event could have consequences on a lot of data subjects depending on the individual case’s circumstances and that is why the supervisory authority should consider this parameter, too, when concluding to the imposition of a fine\textsuperscript{114}.

5.1.3. The level of damage suffered by them.

The level of the damage suffered by the data subjects is the final component the supervisory authority has to take into account to determine the gravity of the infringement. Recital 75 of the GDPR indicates that “The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or nonmaterial damage…” and then lists various behaviors that could lead to the data subject’s damage\textsuperscript{115}. In the case that the data subject has or is likely to suffer damage due to the violation of the Regulation’s provisions, the supervisory authority has to take into account the level of the damage when deciding which corrective measure will be implemented\textsuperscript{116}. Yet, we should not forget that the supervisory authority is not competent to award compensation in case of the data subject’s damage and that it is not the authority’s obligation to establish a causal link between the infringement and the suffered damage\textsuperscript{117}.

5.2. The intentional or negligent character of the infringement

Article 83 par. 2 (b) of the GDPR sets as a criterion for the imposition or not of the administrative fine the “intentional or negligent character of the infringement”. The

\textsuperscript{114} Ibid p. 10.
\textsuperscript{115} See Recital 75 GDPR.
\textsuperscript{116} Article 29 WP, p. 11.
\textsuperscript{117} Ibid.
term “intentional” covers both the controller’s or processor’s knowledge that his action was infringing the Regulation and his willfulness to do so. An intentional violation indicates the controller’s or processor’s contempt for the provisions of the law and thus is more likely to warrant the application of an administrative fine. On the other hand, a negligent behavior demonstrates that the data controller or processor had no intention to cause the infringement, but the breach happened anyway, due to their not being careful or not giving enough attention. A negligent infringement is less severe than an intentional one and it is up to the supervisory authority to decide whether a fine will be imposed\textsuperscript{118}.

The supervisory authority has to evaluate various elements (such as the objective elements of the controller’s or processor’s conduct when they breached the provision in question) in order to be driven to safe conclusions concerning the willfulness or the negligence of the infringer. Other factors that would help with the assessment of a violation being intentional or negligent could be the emergent case law and the practice in the field of data protection under the application of the Regulation\textsuperscript{119}. In 2019 and with the GDPR being in force for almost a year, every enterprise should have adopted structures and resources adequate to avoid the infringement of any of the Regulation’s provisions and thus controllers and processors should not be able to legitimize their data protection law violations by claiming a shortage of resources and trying to convince the supervisory authorities that the said infringement happened due to negligence\textsuperscript{120}.

5.3. \textit{Any action taken by the controller or processor to mitigate the damage suffered by data subjects}

In element (c) of the second paragraph of article 83 the Regulation states that “\textit{any action taken by the controller or processor to mitigate the damage suffered by data subjects}” should also be taken into consideration by the supervisory authority in order

\textsuperscript{118} Ibid pp. 11-12.
\textsuperscript{119} Ibid.
\textsuperscript{120} Ibid.
to determine whether they impose the administrative fine\textsuperscript{121}. What is more, under article 24 of the Regulation the data controllers and processors are obligated to implement technical and organizational measures to ensure the level of security needed for the specific risk, to carry out impact assessments and mitigate risks arising from the processing of data. In the case that the data subject suffers damage because of a violation, the responsible party has to do everything in their power to reduce the consequences for the individual(s). The supervisory authority should definitely make an assessment of such responsible behavior or the lack of it when choosing the corrective measure(s) and when calculating the amount of the sanction that will be imposed\textsuperscript{122}.

The mitigating factors should be assessed by the supervisory authority while deciding on the appropriate corrective measure, too. When the supervisory authority cannot determine based on the other criteria whether the administrative fine should be imposed in addition to another corrective measure of article 58 of the GDPR, or as a standalone, the mitigating factors could prove very helpful by indicating the degree of responsibility of the controller or processor after the infringement has occurred. Thus, the data controllers or processors that have affirmed the violation and taken actions to correct or limit the consequences for the data subject should be dealt with some flexibility\textsuperscript{123}.

5.4. The degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32

Articles 25 and 32 of the Regulation indicate that the controller and the processor have certain responsibilities such as implementing technical and organizational measures according to the principles of data protection by design or by default and ensuring the appropriate level of security by applying the relevant data protection policies at the

\textsuperscript{121} See article 83 par. 2 (c) GDPR.
\textsuperscript{122} Article 29 WP, pp. 12-13.
\textsuperscript{123} Ibid.
appropriate level of management in the organization\textsuperscript{124}. The “\textit{state of the art, the cost of implementation and the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity for rights and freedoms for the natural persons posed by the processing}” should be taken into account by the controller or the processor\textsuperscript{125}. The obligations set out in these two articles are obligations of means, since the controller or the processor have to make the necessary assessments and reach the appropriate conclusions and the supervisory authority has to determine whether they “did what it could be expected to do” based on the circumstances of every individual case\textsuperscript{126}.

The supervisory authority should also take into consideration a “best practice” procedure if it has been applied, along with the industry standards and the codes of conduct in the respective field or profession. These factors could lead to safer conclusions as to what is common practice in the field and on the controller’s or processor’s level of knowledge concerning the different means of addressing typical security issues linked with the processing, while contributing to the assessment of the degree of the controller’s or processor’s responsibility\textsuperscript{127}.

5.5. \textit{Any relevant previous infringements by the controller or processor}

According to article 83 par. 2 (e): “\textit{any relevant previous infringements by the controller or the processor}” should be taken into account during the assessment process. This criterion sets a quite wide scope of assessment considering that any infringement of the GDPR that happened in the past could prove to be “relevant” for the supervisory authority’s investigation, as it could be a sign of lack of insufficient knowledge or disregard for the provisions of the Regulation\textsuperscript{128}. It is crucial for the supervisory authority to examine whether the same infringement was committed by the controller or the processor earlier or if a different infringement was committed in the same

\textsuperscript{124} Ibid p. 13.
\textsuperscript{125} See article 25 and article 32 GDPR.
\textsuperscript{126} Article 29 WP, p. 13.
\textsuperscript{127} Ibid.
\textsuperscript{128} Ibid p. 14.
manner in order to decide on the imposition and on the amount of an administrative fine.

5.6. The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

Another assessment criterion set out in article 83 par. 2 (f) is the infringer’s degree of cooperation with the supervisory authority in order to remedy the breach and mitigate its possible adverse effects. Yet, it is not quite clear how the controller’s or processor’s efforts to remedy a violation confirmed by the supervisory authority could be taken into consideration, since the Regulation does not include a provision for this, leading to the conclusion that this criterion should be used on the calculation of the amount of the administrative fine\textsuperscript{129}. Nevertheless, in the case that a controller’s or a processor’s actions deterred or limited the breach’s negative effects for the data subjects, this behavior could and should be assessed by the supervisory authority when deciding which corrective measure will be imposed. However, the supervisory authority should bear in mind that a certain level of cooperation is already required by law and that not every effort by the controller or the processor should be taken into account in order to decide whether to impose an administrative fine and its amount\textsuperscript{130}.

5.7. The categories of personal data affected by the infringement

Article 83 par. 2 (g) requires that the categories of personal data breached should be assessed by the supervisory authority, too. “Personal data” under article 4 no. 1 of the GDPR are “any information relating to an identified or identifiable natural person (‘data subject’)”. The categories of personal data included in the first paragraph of article 9 GDPR and more specifically “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership” as well as “genetic data, biometric data, data concerning health or data concerning a

\textsuperscript{129} Ibid.
\textsuperscript{130} Ibid.
natural person's sex life or sexual orientation”\textsuperscript{131} are considered to be special categories of data or sensitive personal data and they are subject to specific processing conditions as indicated in article 9 par. 2 GDPR. Furthermore, article 10 of the GDPR sets the “personal data relating to criminal convictions and offences or related security measures” as another special category, which also requires specific conditions for their processing\textsuperscript{132}. So, when the supervisory authority decides on whether to impose an administrative fine should check if the infringed data are part of one of the above mentioned special categories of personal data and then accordingly decide on the amount of the fine, too.

In addition, the supervisory authority should examine if the breached data could lead directly or indirectly to the identification of the data subject\textsuperscript{133}, since indirect identifiers demand more effort and time to lead to the identification of the natural person and are less likely to be qualified as personal data\textsuperscript{134}. Moreover, the supervisory authority should investigate whether the data were encrypted or directly available without any technical protection and whether the distribution of the breached data\textsuperscript{135} generated actual damage or distress to the data subject\textsuperscript{136} when deciding on the imposition of the fine. Nevertheless, the fact that the data that were infringed were indirectly identifiable or encrypted does not automatically mean that an administrative fine should not be imposed, as the other factors of the specific case could make the authority choose in favor of the imposition of the fine\textsuperscript{137}.

\textbf{5.8. The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement}

Article 33 par. 1 of the GDPR requires that when there is a personal data violation the controller has the obligation to notify the competent supervisory authority “without

\textsuperscript{131} See article 9 par. 1 GDPR.
\textsuperscript{132} See article 10 GDPR.
\textsuperscript{133} Article 29 WP, p. 14.
\textsuperscript{134} Voigt, 2017, p. 12.
\textsuperscript{135} Data that fall out of the categories of articles 9 and 10 GDPR.
\textsuperscript{136} Article 29 WP, p. 14.
\textsuperscript{137} Ibid p. 15.
undue delay and, where feasible, not later than 72 hours after having become aware of it” (while the processor only has to notify the controller\(^{138}\)). In the case that the controller fails to keep up with this obligation an administrative fine up to 10 million euro or 2% of the total worldwide annual turnover (for undertakings) could be imposed according to article 83 par. 4 of the GDPR\(^{139}\).

Other than the controller’s notification, a supervisory authority might become aware about an infringement by the complaints filed by the data subject affected by it, by articles published in the press, by anonymous tips or even by their own investigation\(^{140}\). Hence, it is clear that the manner used for the supervisory authority to gain knowledge of an infringement is a very important criterion for the assessment of the imposition of the fine, since the controller’s compliance with his obligation to notify the authority would probably lead to the breach being evaluated as less important than a case where the supervisory authority discovered the data violation on their own\(^{141}\).

5.9. Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

Another criterion that should be taken into account by the supervisory authority when deciding on the imposition of a fine is the compliance with the measures of article 58 par. 2 GDPR when those measures were ordered earlier with regard to the same subject matter\(^{142}\). Article 58 par. 2 gives the supervisory authority some corrective powers in case of infringement of the Regulation’s provisions. If a controller or processor had previously breached a provision and a measure was ordered against them, the supervisory authority should examine whether the controller or processor complied with the said order when assessing the current infringement and its parameters. Article 83 par. 2 (i) is basically a reminder to the supervisory authority of

\(^{138}\) See article 33 par. 2 GDPR.

\(^{139}\) Voigt, 2017, p. 65 seq.

\(^{140}\) Article 29 WP, p. 15.

\(^{141}\) Ibid.

\(^{142}\) See article 83 par. 2 (i) GDPR.
the implementation of the corrective measure they had previously issued to the same
data collector or processor. What is important for this provision to apply is that both
the previous and the infringement in question should concern the same subject
matter. Thus, if the controller or processor failed to comply with the order issued
against them, it is likely that the non-compliance will be evaluated negatively and a
higher administrative fine will be imposed.

5.10. Adherence to approved codes of conduct pursuant to Article 40 or approved
certification mechanisms pursuant to Article 42

Article 40 par. 1 of the GDPR indicates that “the Member States, the supervisory
authorities, the Board and the Commission shall encourage the drawing up of codes of
conduct intended to contribute to the proper application of this Regulation, taking
account of the specific features of the various processing sectors and the specific needs
of micro, small and medium-sized enterprises”, while article 42 par.1 of the GDPR
states that “the Member States, the supervisory authorities, the Board and the
Commission shall encourage, in particular at Union level, the establishment of data
protection certification mechanisms and of data protection seals and marks, for the
purpose of demonstrating compliance with this Regulation of processing operations by
controllers and processors. The specific needs of micro, small and medium-sized
enterprises shall be taken into account”. The codes of conduct and the data
certifications are two instruments complementary to each other, as codes of conduct
give the entities the chance to determine on their own if and how their activities
comply with the GDPR by specifying organizational and material requirements for data
processing, but shall not be used to demonstrate compliance to the supervisory
authority, while certifications do not specify any legal requirements and shall used as a
proof of compliance of certain processing activities with the GDPR directly to the
competent supervisory authority.

The adherence to an approved code of conduct (which contains “mechanisms which
enable the monitoring body to carry out mandatory monitoring of compliance with its

143 Article 29 WP, p. 15.
144 Voigt, 2017, p. 71 seq.
provisions” according to the fourth paragraph of article 40 GDPR) could be used to demonstrate whether the supervisory authority should intervene and impose an administrative fine or other corrective measure in case of an infringement. The controller’s or processor’s conformity with an approved code of conduct, could be used as a proof to the supervisory authority that the code community in charge of administering the code takes the appropriate action themselves against their member and thus, the authority would not need to impose additional measures. But we should always bear in mind that the supervisory authority is not obligated to take into consideration the previously imposed sanctions to the controller or processor by the monitoring body (in the context of codes of conduct or certifications) and is the one who finally gets to determine the imposition of a fine. However, the non-adherence with the entity’s code of conduct or certification could be used by the supervisory authority to prove that the controller’s or processor’s actions intentionally or negligently lead to the non-compliance with the Regulation.

5.11. Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Finally, article 83 indicates on paragraph 2 (k) GDPR that the supervisory authority should also take into consideration any other factor that is possible to aggravate or mitigate the consequences of the infringement in question. In fact, the provision includes some examples of the elements that should be taken into account during the supervisory authorities’ assessment. Such elements could be the financial benefits the controller or the processor gained from the violation or the losses they avoided thanks to it. The controller or processor obtaining profit, directly or indirectly, from the infringement may prove to be strong evidence indicating that an administrative fine should be imposed. What is more, information about such behavior might be critical

---

145 Article 29 WP, p. 15.
146 Ibid.
147 Ibid.
148 See article 83 par. 2 (k) GDPR.
for the decision concerning the implementation of a fine, since an infringement’s economic gain cannot be reimbursed by the supervisory authority “through measures that do not have a pecuniary component”\textsuperscript{149}. Hence, the supervisory authorities should pay attention to this parameter, too, in order to determine the appropriateness of and the amount of an administrative fine imposed for a violation of the Regulation’s provisions.

\textsuperscript{149} Article 29 WP, p. 16.
6. The provisions of paragraphs 7, 8 and 9 of article 83 of the GDPR

Article 83 of the GDPR contains the general conditions for imposing administrative fines. After indicating the general factors that should be taken into account by the supervisory authority when deciding whether to impose a fine and its amount (article 83 par. 2 GDPR) and the tiering system with the highest level of the fines and the categories of the infringements that could lead to these fines (article 83 par. 3-6 GDPR), the Regulation sets out the following provisions concerning:

6.1. The imposition of administrative fines on public authorities – article 83 par. 7 GDPR

Article 83 par. 7 of the GDPR indicates that “without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State”, while Recital 150 states at its sixth sentence that “It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines”. The Regulation leaves the decision of whether the imposition of fines will be extended to public authorities to the Member States’ discretion. Each Member State may set out in its national legislation the rules for determining if and to what extend the provisions of article 83 will apply to the public authorities or bodies established in the said Member State.\(^{150}\)

It is a fact that personal data are frequently collected, hold and processed by public authorities for the purposes of public services, while the processing usually concerns sensitive data. So, it would be reasonable that the new provisions of the GDPR apply to public authorities and other public bodies, too. Hence, the infringement of one of the Regulation’s provisions by a public authority acting as a data controller or processor could be sanctioned as if the breach was caused by a private entity, if the Member State’s national law ruled so. For example, Greece’s draft law for the implementation

\(^{150}\) Iglezakis, 2018, p. 238.
of the GDPR indicates in article 69 that the Greek DPA may impose the administrative fines of article 83 par. 4 to 6 to public authorities and other public bodies\textsuperscript{151}. On the other hand, it is argued that the term “public authorities and bodies” does not include the public companies and this is why national legislators should not be the ones who determine if an administrative fine could also be imposed on public companies\textsuperscript{152}. Nevertheless, the Regulation leaves the decision to Member States and thus, each Member State may lay down its own rules on the matter.

\textbf{6.2. Judicial remedy and due process – article 83 par. 8 GDPR}

As stated in the eighth paragraph of article 83 GDPR “the exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process”. Moreover, Recital 148 mentions at its last sentence that “the imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process”. The Regulation leaves one more important matter such as the procedural safeguards to be handled according to EU and each Member State’s law\textsuperscript{153}. Actually, article 78 GDPR provides for the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning any natural or legal person\textsuperscript{154}. A supervisory authority’s legally binding decision could concern the exercise of their investigative, authorization and advisory or corrective powers\textsuperscript{155}, one of which is “the imposition of an administrative fine pursuant to Article 83”\textsuperscript{156}. So, if there is a decision drafted by the supervisory authority imposing an administrative fine against a controller or processor, they have the right to attack the said decision before the courts of the Member State where the supervisory authority that imposed the fine is established (according to

\textsuperscript{151} Ibid.
\textsuperscript{152} Feiler, 2018, p. 297
\textsuperscript{153} Voigt, 2017, p. 209.
\textsuperscript{154} See article 71 par. 1 GDPR.
\textsuperscript{155} According to article 58 GDPR.
\textsuperscript{156} See article 58 par. 2 (i) GDPR.
article 78 par 3)\textsuperscript{157}. In order to address their judicial remedy the controller or processor should follow the national procedural law of the Member State where the supervisory authority is established\textsuperscript{158}.

\textbf{6.3. The Member State’s national law not providing for administrative fines – article 83 par. 9 GDPR}

In paragraph 9 of article 83 GDPR there is a special provision concerning the cases of Denmark and Estonia, where their national laws do not allow the supervisory authority to impose administrative fines\textsuperscript{159}, according to the first sentence of Recital 151 of GDPR ("the legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation"). Article 83 par. 9 indicates that when the Member State’s national law does not provide for administrative fines, the fine may be initiated by the competent supervisory authority and imposed by the competent national courts. The court that imposes the fine has to ensure that the said fine is effective, proportionate and dissuasive for the specific case and that it has equivalent effect to the fines imposed by the supervisory authorities\textsuperscript{160}. More specifically, in the case of Denmark the court’s fines are imposed in the way criminal penalties would, while in the case of Estonia the supervisory authority is the one to impose the fine, but in the framework of a misdemeanor procedure\textsuperscript{161}. The ninth paragraph of article 83 GDPR also set an obligation for Denmark and Estonia; that they should have informed the Commission about their national law’s provisions adopted for the implementation of the Regulation, as well as any subsequent amendment that could affect them by the 25\textsuperscript{th} of May, 2018, when the General Data Protection Regulation came in force\textsuperscript{162}. In fact, the Danish Data Protection Act was implemented on 23 May 2018, while the Estonian Personal Data Protection Act entered into force only on 15 January 2019.

\textsuperscript{157}Voigt, 2017, p. 214 seq.
\textsuperscript{158}Ibid.
\textsuperscript{159}Feiler, 2018, p. 297.
\textsuperscript{160}See article 83 par. 9 GDPR.
\textsuperscript{161}See Recital 151 GDPR.
\textsuperscript{162}See article 83 par. 9 GDPR.
7. The imposition of other penalties

In case there is a controller’s or processor’s infringement of one the Regulation’s provisions that cannot be subject to administrative fines pursuant to article 83 GDPR, each Member State shall apply other penalties according to its national legislation\textsuperscript{163}. In addition, Recital 152 GDPR indicates that “where this Regulation does not harmonize administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties”. So, if a controller or processor breached a provision of the GDPR that does not fall in one of the categories set out in paragraphs 4 to 6 of article 83 GDPR or is of high importance/has serious consequences for the data subject(s), a penalty would be imposed on them pursuant to the Member State’s national law. Such penalties (of criminal or administrative nature based on the national legislator’s determination\textsuperscript{164}) should be effective, proportionate and dissuasive for each individual case. What is more, each Member State should have notified to the Commission their national laws’ provisions and any other amendment that would possibly affect them by the 25\textsuperscript{th} of May 2018, according to the second paragraph of article 84 GDPR. Hence, the EU Member States may introduce more penalties (other than the administrative fines of article 83) for infringements of the General Data Protection Regulation into their national legislation.

\textsuperscript{163} See article 84 GDPR.
\textsuperscript{164} See Recital 152 GDPR.
8. Conclusions

The Data Protection Directive was in force for twenty years and it set a minimum standard for data protection law across the EU\textsuperscript{165}. The fact that the Directive did not regulate the imposition of sanctions but left the regulation to each Member State’s national law created vagueness, since it was very difficult for the EU citizens to know whether and to what extend their rights were protected and for organizations to determine which national law was to be applied, especially when their activities included cross-border data transactions\textsuperscript{166}.

The General Data Protection Regulation, on the other hand, provides for uniform rules directly applicable to all its addresses, solving the problems caused by the Directive. The high administrative fines indicated in article 83 par. 4 and 5 GDPR point out how important it is for the EU legislator to establish a maximum level of protection for the personal data and their processing. Some may say that the administrative fines under the GDPR are extremely severe and may discourage the free data flows across the EU. What they do not understand is that the Regulation sets in article 83 only the higher level of a potential fines and does not demand that such fines are imposed on every case of infringement of one of its provisions. Furthermore, the GDPR sets many principles and detailed criteria that the supervisory authority has to take into account when deciding whether to impose a fine and its amount. Finally, the Regulation indicates that the administrative fines are imposed “in addition to or instead of other corrective measures”, depending on the specific circumstances of every individual case.

Thus, when assessing the GDPR we should not focus on the amount of the potential administrative fines, but to bear in mind that they are imposed to strengthen the enforcement of its rules and to ensure compliance with its provisions. Besides, the Regulation aims to establish the right to the personal data protection, but also to facilitate the free movement of such data throughout the European Union.


\textsuperscript{166}Ibid.
Bibliography

Books

Journal Articles

Legislation, Legislative Instruments and Codes
- Act No. 502 of 23 May 2018 - Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Danish Data Protection Act)
- Article 29 Data Protection Working Party, “Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679”.
- Directive 95/45/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
- EU Charter of Fundamental Rights (2000/C 364/01)
- Regulation 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 (General Data Protection Regulation)