INTERNATIONAL
HELLENIC
UNIVERSITY

General conditions for imposing administrative fines in the context of 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.

Konstantina Kalamata

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

Master of Laws (LLM), in Transnational and European Commercial Law, Mediation, Arbitration and Banking Law.

February 2019

Thessaloniki – Greece

Student Name: Konstantina Kalamata

SID: 1104160051

Supervisor: Prof. Komninos Komnios

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 LLM in Transnational and European Commercial Law, Mediation, Arbitration and Banking Law at the International Hellenic University.

The purpose of this thesis is to provide a comprehensive analysis and examine the general conditions for imposing administrative fines in the context of 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». Chapter 1 refers to the general framework and further assessment criteria which the Supervisory Authority take into account in the fining procedure and the different levels of administrative fines provided for by GDPR for different infringements of its provisions . Reference is also made to the principles of specificity and predictability that should be govern the procedure for the imposition of fines Chapter 2 refers to recipients of the administrative sanctions and the procedure taken place for imposing the fines.

I would like to express my sincere gratitude to my supervisor, Prof. Komninos Komnios for assisting my dissertation. His expertise, understanding and patience were really helpful for me in any stage of my research. I would like to thank him for his continuous support, motivation, his immediate response to my questions and his valuable guidance.

In parallel, I would also like to thank all the teaching staff of the LL.M in Transnational and European Commercial Law, Mediation, Arbitration and Banking Law of International Hellenic University for their help and support, which was a motivation for me to advance my knowledge.

I would also like to give special thanks to my family and my friends, for their support and encouragement during my post-graduate studies.

Keywords: sanctions, supervisory authorities, processor, controller, proportionality.

Konstantina Kalamata

Preface

The rules of the Directive 95/46/EU «on the protection of individuals with regard to «the processing of personal data and on the free movement of such data» were not directly applicable but had to be implemented by the Member States into their national data protection law. The different application of rules by Member States resulted in great divergences among the different data protection regimes that shake the desired legal certainty in the field of data protection law. The need for a strong legal regime which it could harmonize the different Member States legislation lead to the drafting of the new General Data Protection Regulation which strengthen the level of protection of rights and interests of data subjects and enhance the legal certainty in the field of data protection law.

Table of Contents

Introduction

The rapid pace of technological developments and globalization has resulted in dramatic changes for collecting, processing, exchanging and using personal data. The almost unlimited technical possibilities of using and commercializing personal data and the growing importance and value of personal data for businesses on the one hand require a strong regime for protecting personal data on the other[1]. The need for further harmonization and a greater level of protection of fundamental rights in the field of data protection law, led the European legislator to adopt the General Data Protection Regulation (hereafter, the ''*GDPR*'')[2] . The GDPR became effective on May, 28, 2018, and is directly applicable into the domestic legislation of the Member States.[3] However, the introduction of a few *opening clauses* which allow the Member States to adopt further national laws and to impose further specifications on particular topics, restrain the full harmonization of data protection regime within the Union. The transition from the legal status of the Directive 95/46/EU to that of GDPR, also brought changes to the mechanisms of enforcement of the new law. The GDPR adopting the model of European law on free competition has introduced an autonomous and effective administrative fining system in order to consolidate the uniform application of the substantive provisions of the GDPR throughout the European Union.

The Directive 95/46/EU already contained a provision which required Member States to «*adopt suitable measures to ensure the full implementation of the above Directive and lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive»*[4].However, the general wording of the provision and its failure to specify precisely the

---

[1] Rucher D./Kugler T., «New European General Data Protection Regulation: *A Practitioner's Guide Ensuring Compliant Corporate Practice. » C.H BECK HART NOMOS,* (2018), 1-3.

[2] The data protection law under the previous data protection Directive 95/46/EU and its various national implementations was fragmented across Europe. Given that the common rules provided for by the Directive were not directly applicable but need to be implemented by the Member States into their national data protection laws the implementation in practice resulted to significant divergences in the national interpretation and application of data protection rules and therefore in the level of protection throughout the Union.

[3] 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.

[4] Article 24 of Directive 95/46/EU.

type and intensity of sanctions, left a wide discretion to Member States when deciding the imposition and the amount of administrative fines. The discrepancies in the sanctioning system, which are rather attributable to the differences in the criminal and administrative law of Member States, lead in some cases to the lack of legitimacy of the competent Supervisory Authority to impose administrative fines or its impossibility to enforce the sanctions imposed.[5]

In order to address the differences in the field of the sanctioning system for breaches of EU legislation as well as to ensure an effective protection of personal data throughout the Union and a consistent monitoring of the processing of personal data in the internal market, the GDPR introduces a system of *equivalent sanctions* in all Member States [6]. The consistent application of the fining practice throughout the EU is ensured through the consistency mechanism[7]. The doctrine of equivalence is central in determining the extent of the obligations of the supervisory authorities to ensure consistency in their use of corrective powers according to article 58 (2) in general and the application of administrative fines in particular[8]. The system should also have preventive-dissuasive function enhancing thereby the enforcement of the GDPR rules.

The article 83 specifies the sanctioning power of the supervisory authorities provided for in article 58 (2) (i). An important tool for the supervisory authorities in regard to application and setting of administrative fines are the guidelines of the Article 29 Working Party9 published on 3 October

[5] The enforceability of the act of the Data Protection Authority is explicitly provided for in Article 21 para 2 of Law 2472/1997.

[6] Recital 11 and 13 of GDPR.

[7] Article 63 states that: « *In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section»*. The consistency mechanism in GDPR is outlined as a means to the consistent appliance of the GDPR in all Member States by obliging the supervisory authorities to cooperate with each other and with the Commission. The main instrument to ensure a consistent appliance of the GDPR is the establishment of the Board (art.68 para1) which replaces the Art.29 Working Party.

[8] Recital 150 states that: «*the consistency mechanism may also be used to promote a consistent application of administrative fees».*

[9] The Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy and consists of the European Data Protection Supervisor, EC (representatives) and EU Member State representatives. Its tasks are described in Article 30 of the Directive 95/46/EU and Article 15 of Directive 2002/58/EU.

2017 (*the Guidelines*). The guidelines provide an insight into how supervisory authorities will determine whether an administrative fine must be imposed under the GDPR. Their use by the supervisory authorities ensure a better application and enforcement of the GDPR and expresses their common understanding of the provisions of Article 83 of the GDPR as well as its interplay with articles 58 and 70 and their corresponding recitals 10 The EDPB, with a view of achieving a consistent approach to the imposition of the administrative fines has agreed on a common understanding of the assessment criteria in article 83 (2) and therefore the guidelines are used as a common approach by the EDPB and individual supervisory authorities.

[10] According to article 70 (1), (f): The European Data Protection Board (hereafter ''EDPB'') *is empowered to issue guidelines, recommendations and best practices in order to encourage consistent application of GDPR* and article 70 (1), (k) specifies the provision for guidelines regarding the setting of administrative fines.

Chapter 1. The substantive provisions relating administrative fines

1.1 Article 83 para 1

From a business point of view, administrative fines constitute one of the most controversial issues of the GDPR since fines can easily amount to millions of euros. Article 83 establishes a differentiated and flexible system with regard to the imposition of administrative fines which entitles directly the supervisory authorities for imposing administrative fines, without, in principle to give leeway to national legislators[11].

Like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the breach and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. Article 83 para 1, lays down the general framework regarding the imposition of administrative fines providing that:

«*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation … shall in each individual case be effective, proportionate and dissuasive».* The guidelines of Article 29 Working Party determine that the ''*assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the administrative fine that is either to reestablish compliance with the rules or to punish unlawful behavior (or both)*. Also, they recognize *that national legislator may set additional requirements on the enforcement procedure to be followed by the supervisory authorities. However, such requirements should not hamper in practice the achievement of effectiveness, proportionality or dissuasiveness.*

[11] However in article 83 para 9 is defined that «*Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts…* ».

The principle of proportionality, as principle of the primary European Union law defines the mode of action of the relevant supervisory authority. Also, the macro-prudential function-apart from the preventive and dissuasive purposes- of administrative fines is limited by the principle of proportionality [12]. In this context the administrative fine should be significantly higher than any profit/cost savings of the infringer while the imposition of an administrative fine to a first-time infringer cannot be considered per se disproportionate[13]. Where administrative fines are imposed on undertakings, the supervisory authority should not make allowance for the potential poor economic situation of an undertaking when deciding the appropriate amount of the fine.

On the other hand, where administrative fines are imposed on natural persons « *the supervisory authority should take account of the general level of income in the Member States as well as the economic situation of the person when considering the appropriate amount of the fine*[14].

1.2. Article 83 para 2

1.2.1 Discretion of the supervisory authority in imposing administrative fines.

Article 83 (1) states that: «*The administrative fines shall, depending on the circumstances of the individual case, be imposed in addition to, or instead of the corrective measures referred to article 58 para 2 of GDPR».* The wording of the provision raised the question of whether, in the event of a breach of the relevant provisions of Article 83 (4)-(6) of the GDPR, the supervisory authority is required or on the contrary has the discretion under the light of feasibility to decide on the imposition of the administrative fine[15]. It is argued that, on the basis of the grammatical interpretation of article 83(2) in conjunction with Recital 148, the supervisory authority is required to impose a fine in case of a breach and in preference in relation to the corrective measures of article 58 (2) of the GDPR [16.] Given that the administrative fines shall be imposed in addition to or

---

[12] Komnios K., «The general conditions for imposing fines under the GDPR: Contribution to the interpretation of article 83 of the GDPR», *ΔΙΜΕ,* 2017/4, 504.

[13] Komnios K.,*The general conditions for*…, ep.cit. 503

[14] Recital 150

[15] Komnios K., The general conditions for…, ep.cit.505

contribution to the interpretation of Rule 83 of the Rules

[16] Recital 148 defines that: « *In order to strengthen the enforcement of the rules of this Regulation penalties including administrative fines should be imposed for any infringement of this Regulation,*

instead of corrective measures of Article 58 the above interpretative version requires the imposition of fine in each case [17]. However, the same article referring to elements to be taken into account «*when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case»,* weakening also the argument based on the grammatical interpretation of the provision [18] .In the same spirit the provisions of Recital 148 and 150 reinforce the view that the imposition or not of administrative fines ultimately rests with the supervisory authority [19]**.** Based on the above, it is clear that the imposition of a fine is at the discretion of the supervisory authority concerned. However, the supervisory authorities should use a consolidated and balanced approach in their use of corrective measures, so as to achieve both an effective and dissuasive as well as a proportionate reaction to breach. The point is not to qualify the fines as last resort nor to shy away from issuing fines but on the other hand not to use them such in a way that would underestimate their effectiveness as a tool [20].

1.2.2 Assessment criteria

The GDPR provides for potentially massive new fines for violations of its provisions which involve a significant increase from the prior EU data protection regime. The frame for administrative fines is set according to the type of infringement. With the exception of the provisions of Articles 10 and 24, any other breach of the provisions of GDPR regarding specific obligations and prohibitions of controllers and processors according to article 83 (4) (5) shall be subject to an administrative fine. For the infringements not expressly mentioned in the above provisions, the supervisory authority cannot in principle impose an administrative fine [21].

---

in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation».

[17] On the contrary, the imposition or not of the measures referred to in Article 58 (2) shall be at the discretion of the competent supervisory authority.

[18] Article 83 (2) (b)**.**

[19] Recital 148 the Regulation clarifies that: « *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». Additionally,* Recital 150 states that: «*Each supervisory authority should have the power to administrative fines...*» and consequently no obligation.

[20] See Article 29 Working Party Guidelines

[21] Recital 150 of the GDPR.

In general, the imposition of administrative fines has to be always effective, proportionate and dissuasive [22]. Article 83 (1) The supervisory authority when deciding whether to impose a fine and deciding on its amount «*due regard should be given to the circumstances of each individual case» as well as to the specific criteria listed in article 83 (2).* The conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of fines, avoiding thereby the need to assess the same criteria twice. In particular, the supervisory authority should take account of: a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them, b) any intentional or negligent nature of the infringement, c) any action taken by the controller or processor to mitigate the damage suffered by data subjects, d)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, e) any relevant previous infringements by the controller or processor, f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement, g) the categories of personal data affected by the infringement, h)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, i) 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, j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanism pursuant to Article 42 and k) 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 [23].

1.2.2.1 The nature, gravity and duration of the infringement.

A decisive criterion which must be taken into account by the supervisory authority in imposing the administrative fines against controllers and processors, is the nature of the infringement. The GDPR, in setting up two different maximum amounts of administrative fines (10/20 million Euros) already indicates that a breach of some provisions of the Regulation may be more serious than for other provisions. Notwithstanding, the competent supervisory authority by

[22] Article 83 (1)

[23] Komnios K., *The general conditions for*…, ep.cit. 503

assessing the facts of the case in light of the general criteria provided in article 83 para 2, may decide that in the particular case there is a higher or a more reduced need to react with a corrective measure in the form of a fine. Where a fine has been chosen as one or one of several appropriate corrective measures, the tiering system of the Regulation will be applied to determine the maximum fine that can be imposed according to the nature of the infringement in question [24].

The notion of ''minor infringements'' in Recital 148 may constitute infringements of one or several of the provisions of the GDPR enumerated in article 83(4) or (5)[25].

The supervisory authority, however, taking into account the assessment criteria in article 83(2) may decide to abstain from imposing an administrative fine on the grounds that in the concrete circumstances of the case, the breach for instance, does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question. Therefore, in such cases the fines may be superseded by a reprimand. The present provision does not impose the obligation on the supervisory authority to replace a fine by a reprimand in every case of a minor infringement (''*a reprimand may be issued instead of a fine''*). By the contrast, the provision establishes discretion for the supervisory authority to impose a less burdensome corrective measure after assessing the concrete circumstances of the specific case. The supervisory authority also has the discretion to replace the fine by a reprimand in the event that the data controller is a natural person and the fine likely to be imposed would constitute a disproportionate burden. In principle, the authority taking into account the circumstances of the case at hand, has to assess whether a fine should be imposed. Should it find in favor of levying a fine then the supervisory authority must also assess whether the fine to be imposed constitute a disproportionate burden to a natural person. The GDPR does not define a specific price tag for specific infringements only the upper amount of fines. This can be indicative of the relatively lower degree of gravity for the breach of obligations listed in article 83(4) in comparison with those set out in article 83(5). However, the effectiveness, proportionality and dissuasiveness of the fine will depend on the circumstances of the case. Emphasis should be given in cases where infringements that normally due to their nature fall within the scope of article 83 (4), *namely involving a fine of up to 10 million Euros or up to 2% of total annual worldwide turnover of the preceding financial year,* might end up qualifying for the higher applicable cap (20 million) in certain circumstances. This would be likely to be the case where such breaches have previously been addressed with an order by the supervisory authority to which the controller or the processor failed to comply with.

[24] Articles 83 (4)-(6)

[25] See Article 29 Working Party Guidelines

The application of article 83(4) must take into account the procedural provisions of national law. In particular, the procedural law of each Member State defines how an order is issued, how it is notified, from which point it takes effect, whether there is a grace period to work on compliance. Notably, the effect of an appeal on the enforceability of an order should be taken into account. Similarly, the substantive provisions of national law may in practice have an impact on this assessment. [26] With regard to the gravity of the infringement will be sought the effects on the data subject as well as the damage can be restituted [27]. The purpose of the processing, on the other hand, will be considered on the basis of its legality and will be taken into account the duration of the infringement .

Similarly, according to the case law of the Greek Supreme Administrative Court and the current legal framework relevant criteria are assessed. [28] Specifically, the imposition of an administrative fine depends on a number of factors such as the extent of the infringement, the degree of liability of the person liable, his financial standing, the effects of the fine on his reputation, fame, his creditworthiness, the magnitude of the risk created or the damage actually caused, any repeated infringements, the deliberate infringement of the supervisory authority's recommendations and orders, the potential economic benefit of the infringement, the behavior of the person responsible after the infringement to mitigate the damage caused, the probable effectiveness of the fine with regard to the prevention of future infringements and other relevant factors [29].

In particular the Superior Administrative Court held that «*intent is not a condition for the imposition of an administrative fine, but it is sufficient to establish the objective element of the damage of the subject»*[30]. There is, however, contradictory case law under which *«For the imposition of the administrative sanction according to article 21 of Law 2472/1997 suffice to establish the particular breach and it is no longer required to establish the occurrence of a*

[26] Statutory provisions of limitation may have the effect that a previous order of the supervisory authority may no longer taken into consideration due to the amount of time that lapsed since that previous order was issued. The legal regime of some jurisdictions requires that after the prescription period has passed with respect to an order, no fine may be imposed for non-compliance with that order under article 83(6). It will up to each supervisory authority in each jurisdiction to determine how such impacts will affect them.

[27] *Nemitz*in Ehmann/Selmayr, DS-GVO, Art.83 Rn.16

[28] Greek Superior Court of Justice (ΣΤΕ), 1774/2016, 3135/2015, 1367/2008, 94/2003.

[29] Kanelopoulou- Mpoti M., «Sanctions for infringing personal data in « Kotsali Personal Data».

[30] Greek Superior Court of Justice (ΣΤΕ), 4158/2000

particular damage to the data subject of the processing of his data or to invoke such damage on his part, that is, damage other than that resulting from the processing of his data»[31].

1.2.2.2 The intentional or negligent character of the infringement

Article 83 (2) (b) of GDPR refers that the degree of fault of the infringer is assessed when the fine is imposed. Examples of intentional breaches might be the amendment of personal data to give a misleading impression about whether targets have been met or the trade of personal data for marketing purpose for example selling data as ''opted in'' without checking data subject's opinions about how their data should be issued. On the other hand, circumstances which may be indicative of negligence may be: the failure to abide by existing policies, human error, failure to check for personal data in information published or failure to apply technical updates in a timely manner or failure to adopt policies. Enterprises are responsible for adopting structures and resources adequate to the nature and complexity of their business. Therefore, controllers or processors cannot legitimize breaches of data protection law by claiming a shortage of resources. Routines and documentation of processing activities follow a risk-based approach in line with the Regulation[32] .Given that the provision concerned, requires from supervisory authorities taking into account in their assessment for the imposition of fine *«the intention or negligence that caused the offense»,* it is questionable whether the liability of the infringer is necessary or not for the imposition of fines [33] **.** There is great doubt both in theory and case law as to whether objective or subjective liability of the infringer is required for the imposition of fines. In one respect the need for subjective liability is based on article 83 (2) (b) while in another respect, in order to reach the same conclusion, it invokes the principle of proportionality and the principle of liability[34].

The opposite view advocated that article 83 of GRDP introduces a system of administrative sanctions irrespective of the infringer's liability, that is *strict liability.* However, at no point of article 83 is defined the subjective attitude of the infringer as a prerequisite for the imposition of fine. On the contrary on the European Commission's proposal for a Regulation there was a clear reference to the intention or negligence of the infringer [35]**.** The absence of a corresponding

[31] Greek Superior Court of Justice (ΣΤΕ),1367/2008

[32] See Article 29 Working Party Guidelines

[33] Komnios K., *The general conditions for*…, ep.cit. 506.

[34] BeckOKDatenSR/*Hollander,* 20.Ed.1.5.2017, DS-GVO Art.83 Rn.18.

[35] Article 79 (4) (5) and (6) of the European Commission's proposal for a Regulation.

reference to the final version of the relevant provisions of Article 83 suggests that the intention of the EU legislator is to establish a strict liability. This view is underpinned both by the wording of article 83(2) (b) which states that «d*ue regard should be given*» and by Recital 148 of GDPR which provide for that in the imposition of administrative fines « *due regard should be given (and not necessarily) to the intentional nature of the infringement».* The introduction of strict liability for administrative sanctions does not constitute a novum in the EU legal order. It is worth noting that neither under Law 2472/1997 is the subjective liability a precondition for the imposition of fines.

In the field of administrative penalties, the principle of subjective liability is not expressly enshrined in the ECJ nor in the Charter of Fundamental Rights of the EU. In addition, the Court of Justice of the European Union has not explicitly recognized the principle of subjective liability as a general principle of European Union law. In particular the Court ruled that: « although it has not given in-depth consideration to the principle of *nulla poena sine culpa* in its case-law thus far, there are nevertheless indications that it takes it as a given that the principle holds at EU level […].I would add that the principle enjoys the status of a fundamental right which is common to the constitutional traditions of the Member States […].*Although this principle is not expressly mentioned in the Charter of Fundamental Rights of the European Union or in the ECHR […], it is the necessary precondition for the presumption of innocence. The principle of nulla poena sine culpa may therefore be considered to be contained implicitly in both Article 48(1) of the Charter and Article 6(2) ECHR, which, as has been recognized, must be taken into account in cartel proceedings[…]. Ultimately, these two provisions of the Charter and the ECHR can be regarded as the expression in procedural law of the principle of nulla poena sine culpa»*[36].

The ECJ accepts the imposition of administrative sanctions irrespective of the infringer fault, provided that it complies with the principle of proportionality[37]. In particular, «*according to the Court the imposition of a system of strict liability is not disproportionate in relation to the objectives pursued if that system is such as to encourage the persons concerned to comply with the provisions of a regulation and where the objective pursued is a matter of public interest which may justify the introduction of such a system».* In general, the characteristics of an intentional infringement contain both knowledge and willfulness of the infringement whereas ''unintentional'' indicate that there was no intention for the commitment of the infringement

[36] ECJ, C-681/1, *Schenker&Co AG and Others,* Opinion of Advocate General Kokott, (para. 41).

[37]ECJ, C-210/10, *Urban,* (par 47- 48), ECJ 2 C-497/15 and C-498/15, *Euro-Team Kft* and S*piral-GepKft.,(par.*53 et.seq), ECJ, C-210/10, *Käserei Champignon Hofmeister,* (par. 62-68), ECJ C-326/88 *Hansen,* (par. 19).

even though the controller or processor breached the imposed by the law duty of care. In the above context, given that it is stated inter alia that the intent or negligence of the infringer must be taken into account, be grounded on theory if liability of the infringer is necessary for the imposition of the fine.

However, in the case *Käserei Champignon* Hofmeister, the Court ruled that «*A penalty which is provided for by a Regulation is likely to breach the principle ΄΄nullapoena΄΄ sine culpa » only if it is of criminal nature»*[38] .

According to the case-law of the European Court of Human Rights and the Court of the European Union, the penal nature of a penalty is based on three criteria which are determined in the *case Engel.* In particular, «*the first criterion is the legal classification of the offence under national law, the second is the very nature of the offence and the third is the nature and degree of severity of the penalty that the person concerned is liable to incur»*[39]*.*

As regards the legal classification of the sanction in question, *«is not considered criminal in nature under the EU Law»* since it is characterized by GDPR as administrative penalty**[40]** .

In line with article 83, the purpose of imposing an administrative penalty, is the compliance of the infringer with the requirements of Regulation as well as the faithful observance and enforcement of personal data protection rules, not the punishment of the infringer. The preventive nature of the administrative fine follows from article 83 (1) which stipulates «*that the imposition of an administrative fine shall be dissuasive»* as well as by Recital 150 which provides for that «*the purpose of the imposition of administrative penalties is to prevent or mitigate the consequences of the infringement».* In any case, the rule of article 83 is not addressed to all citizens, but to the recipients described therein. In addition, the administrative fines of article 83, as opposed to the penalty, they do not express any social disapproval whereas they are not always on an individual nature since they are usually imposed on legal persons for acts or omission of their personnel. In conclusion, the administrative sanction does not constitute a penal sanction since it is directed to a particular circle of recipients and performs only a dissuasive function. The penal sanction extends beyond mere deterrence and includes also social disapproval. However in the light of the recent case-law in case *Ute Reindl,* the ECJ ruled that «even *if it were accepted that the sanctions of*

[38] ECJ, C-210/00,*Käserei Champignon Hofmeister, (2001),*Opinion of Advocate General Stix-Hackl (par.33-35).

[39] ECHR, *Engel and Others v. the Netherlands, (1976),* Series A No.22, (par.80-82), ECHR, S*ergey Zolotukhin v. Russia*, (2009) No.14933/03 (par. 52 and 53).

[40] ECJ, C-489/10, *Bonda,* (par.38)

article 83 of the GDPR are of penal nature-which mainly due to the amount of fine fall within the field of penal law within the meaning of ECHR- such a system (of strict liability) is not in itself disproportionate to the objectives pursued, if that system is such as to encourage the persons concerned to comply with the provisions of a regulation and where the objective pursued is a matter of public interest which may justify the introduction of such a system»[41.]

The Greek Superior Administrative Court has also accepted, though not uniformly, the system of strict liability for administrative penalties[42]. Intentional breaches, due to the contempt of the infringer with regard to the provisions of law, are more severe than unintentional (breaches), therefore it is more likely to result in the application of administrative fines. The supervisory authority in order to find out intentional or negligent behavior of the offender based on objective elements of conduct of the individual case. Moreover, emerging jurisprudence and practice in the field of data protection under the Regulation should be taken into account by the supervisory authority in the assessment of the circumstances which establish an intentional nature of the breach. Circumstances indicative of intentional breaches might be unlawful processing authorized explicitly by the top management hierarchy of the controller, or in spite of advice from the data protection officer or in disregard for existing policies for instance obtaining and processing data about employees at a competitor with an intention to discredit that competitor in the market [43].

1.2.2.3 Any action taken by the controller or processor to mitigate the damage suffered by them

Article 83 (2) (c) seeks to encourage the controller or the processor to mitigate the damage caused by the infringement. The mitigation of damage does not only refer to the property damage but to the removal of any consequence of the infringement to the subject of the rights. However, after the occurrence of the breach, the responsible party should take all necessary measures in order to mitigate the consequences of the breach for the individual(s) concerned. Such responsible behaviour would be taken into account by the supervisory authority when determining the appropriate corrective measure and the amount of the sanction to be imposed in the specific case. On contradistinction, the supervisory authority will assess negatively the absence of actions aimed at mitigating the damage [44].

---

[41] ECJ, C-443/13, *Ute Reindl*, (2014), (par. 42), ECJ, C-326/88, *Hansen*, 1990, (par.19).

[42] Greek Superior Administrative Court, (ΣΤΕ), 119/2015,751/2010, 2491/2008.

[43] See Article 29 Working Party Guidelines

[44] *Nemitz* in Ehmann/Seimayr, DS-GVO, Art.83 Rn.19

Therefore, aggravating and mitigating factors are taken into account not only for the proper determination of the amount of a fine but also in the choice of appropriate corrective measures. In particular, in cases where the supervisory authority doubts about the appropriateness of an administrative fine (whether it should be imposed the fine as a standalone measure or in combination with the measures provided in article 58) aggravating and attenuating circumstances constitute a helpful tool for the supervisory authority to select the measure which is more effective, proportionate and dissuasive in the case in question [45]. The present provision requires the assessment of the degree of responsibility of the responsible persons after the occurrence of the infringement and lead to a more flexible approach for data controllers or processors who after having been informed of the infringement taken the responsibility trying to rectify the situation or limit the impact of their actions. For instance, the contact of the controller or processor with other controllers or processors who may have been involved in an extension of the processing or the timely action of the former to stop the infringement from expanding to a level which would have had more serious impact that it did, may constitute mitigating factors in favor of these persons.

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

The degree of responsibility referred in Article 83(2)(d) associated with the degree of fault in Article 83 (2)(a) but specifies the responsibility with respect to technical and organizational measures implemented by controllers/processors pursuant to article 25 and 32 of GDPR.

The Regulation has established a greater level of accountability of the data controller in comparison to the EU Data Protection Directive 95/46/EU.

The degree of responsibility of the controller or processor constitutes a decisive factor during supervisory authority's assessment regarding the application of the most appropriate corrective measure. In particular the supervisory authority shall take into account: If the controller put into effect technical measures which are consistent with the principles of data protection by design or by default (article 25), and implemented organizational measures which give effect to the principles of data protection by design and by default (article 25) at all levels of organization, whether the controller or processor adopted an appropriate level of security (article 32), and

[45] Article 29 Working Party Guidelines

should the relevant data protection routines and policies are known and applied at the appropriate level of management in the organization (article 24) [46].

Articles 25 and 32 of the GDPR require : «*the controllers take into account the 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».* The provisions introduce obligations of means rather than obligations of goals, that is, the controller should make the necessary assessments and draw the appropriate conclusions. The supervisory authority should evaluate if the controller did what it could be expected to do given the nature, the purposes or the size of the processing seen in light of the obligations imposed on them by the Regulation. The supervisory authority in its assessment should take into consideration any ''best practice'' procedures or applied methods as well as industry standards and codes of conduct in the respective field of profession. Codes of practice might be illustrative of the common practice in the field and of the level of knowledge about different means to address typical security issues associated with the processing. While best practice would be the ideal to pursue in general, the special circumstances of each individual case should be taken into consideration when the supervisory authority making the assessment of the degree of responsibility [47]. Especially for legal persons, «*each undertaking must be aware of the actions of its employees who have committed the infringement and cannot rely on malfunctioning of its internal organization»*[48] .In addition, «*the infringement can be established without demanding the identification of the persons who had acted improperly within the undertaking or who ought to have been responsible for any defective organization of the undertaking»*[49.] The diligence required in the transactions will be *determined on the basis of the size of the business, the type of economic activity and the data processing operations*[50] .

[46] See Article 29 Working Party Guidelines

[47] See Article 29 Working Party Guidelines

[48] General Court, T-161/05, *Hoechst GmbH,* (2009), (par. 55)

[49] ECJ, C-338/00P, V*olkswagen AG*, (2003), (par. 98)

[50] BeckOKDatenSR/*Hollander*, 20. Ed.1.5.2017, DS-GVO Art.83 Rn.34

1.2.2.5 Any relevant previous infringements by the controller or processor

Article 83(2)(e) acts as an aggravating factor against the habitual infringer and highlights the pedagogical function of the fines, providing that any relevant previous infringements may be aggravating in the case of a new infringement. This criterion aims to assess the track record of the entity committing the infringement. The scope of the assessment hereto can be quite wide since any infringement of the Regulation although different in nature to the one being investigated by the supervisory authority might be *''relevant''* for the assessment as it could be indicative of a general level of insufficient knowledge or disregard for the data protection law[51].

The supervisory authority should examine whether the controller or the processor committed the same infringement earlier or in the same manner. That is the case in which the controller or processor did not respond to requests of data subjects in a timely manner on the ground of insufficient knowledge of the existing routines in the organization.

The provision may constitute a disincentive preventing controllers from cooperating with processors who have already committed a breach of legislation. However, apart from the relevance of the infringements, it also should also be taken into account the time dimension so as not counted any lapsed breaches[52].

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

Article 83(2)(f) provides that: « The degree of cooperation may be given due regard when deciding whether to impose an administrative fine and in determining the amount of fine.

The Regulation does not clarify how to take into account the efforts of the controllers or processors to remedy an infringement already established by the supervisory authority. However, when the intervention of the controller mitigates the impact of the negative consequences on the rights of individuals this could also be taken into account by the supervisory authority in the determination of the amount of fines. [53]. The supervisory authority also shall assess positively the proper response of the entity to its requests at the stage of the investigation if in the particular case the entity's cooperation result in the limitation of the negative impact on individuals' rights.

[51]See Article 29 Working Party Guidelines, p.14

[52]BeckOKDatenSR/*Hollander*, 20. Ed.1.5.2017, DS-GVO Art.83 Rn.37.

[53] See Article 29 Working Party Guideline, 14

On the contrary, the supervisory authority should not take into consideration entity's cooperation that is already required by law. For example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspections.

1.2.2.7 The categories of the personal data affected by the infringement

Another criterion to be evaluated by the supervisory authority is the categories of the personal data affected by the infringement. In particular, the supervisory authorities may examine whether the infringement concerns the processing of special categories of data as provided for in articles 9 and 10 of GDPR. It should also find out if the data is directly/ indirectly identifiable, whether the processing involves data whose dissemination could cause immediate damage or distress to the individual or if the data is directly available without technical protections or it is encrypted.

However, the fact that the infringement concerns only indirectly identifiable data or even pseudonymous/encrypted data does not in every case constitute an attenuating circumstance. For such breaches the supervisory authority may assess and other criteria for deciding on the necessity of imposing a fine [54].

1.2.2.8 The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent the controller of processor notified the infringement.

Article 33 of the GDPR, requires t*he controller to notify without undue delay the supervisory authority of personal data breaches.* The compliance of the controller with this obligation cannot be interpreted as a mitigating factor given that it constitutes a duty required by the law.

Similarly, the data controller or processor who acted carelessly without notifying or at least not notifying all of the details of the infringement either does not notify the supervisory authority may be subject to a serious penalty by the supervisory authority.

The provision in question in so far as it also concerns the processor, is incompatible with the provision of Article 33 (2) which *requires the processor to notify the controller without undue delay* and not the supervisory authority. [55]

[54] See Article 29 Working Party Guidelines, p.15

[55] *Nemitz* in Ehmann/Seimayr, DS-GVO, Art.83 Rn.25.

1.2.2.9 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.

The supervisory authority is likely to already monitor the controller/processor due to a previous infringement which has been committed by them. Therefore, the contacts of the supervisory authority which are likely to be extensive with the controller/processor should be taken into account in deciding the imposition of a fine. Contrary to the assessment in (e), this criterion seeks only to remind supervisory authority to refer to measures which have been previously imposed on the same controller or processor [56].

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

According to Article 57 (1) (a) «*The supervisory has among others the duty to monitor and enforce the application of this Regulation».* Adherence to approved codes of conduct or approved certification mechanisms may be used by the controllers or processors as a way to demonstrate compliance with the requirements of law.[57] The compliance with codes of conducts and the certification will be positively assessed by the supervisory authority since their adoption limit the likelihood of an infringement. In the event of a violation of one of the provisions of the Regulation, supervisory authority shall take into account the compliance of the controller or processor with an approved code of conduct in order to decide the necessity of imposing an effective, proportionate, dissuasive fine or other corrective measure. According to Article 40 (4): «*A code of conduct shall contain mechanisms which enable the (monitoring) body to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it ».* This arrangement gives the supervisory authority the flexibility to refrain from imposing a fine or additional measures given that the competent code community has taken the necessary action against their members thought monitoring and enforcement schemes of the code of conduct. Therefore, the monitoring body may impose sanctions for non-compliant behavior including

[56]See Article 29 Working Party Guidelines

[57]See Articles 24(3), 28(5), 32(3) of GDPR.

suspension or exclusion of the controller or processor concerned from the code community. Notwithstanding, the supervisory authority is not obliged to take into consideration previous sanctions which have been imposed by the monitoring body on the grounds that the powers of the monitoring body are «*without prejudice to the tasks and powers of the competent supervisory authority*» [58]. The failure of the controller/processor to comply with self-regulatory measures could also be indicative of their intentional or negligent behavior of non-compliance.

1.2.2.11 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.

The present provision introduces an auxiliary clause which allows the supervisory authority to take into account any other aggravating or mitigating factor resulting from the circumstances of the particular case when deciding the appropriateness of an administrative fine.

The provision itself gives example of which other elements might be taken into account when supervisory authority deciding the appropriateness of an administrative fine for breaches of the provisions mentioned in article 83 (4)-(6). In provision is expressly stated that the profit resulting from a breach may be a decisive factor for the supervisory authority as economic gain from the infringement can only be compensated though the imposition of administrative fines which are of pecuniary nature [59]. Moreover, the supervisory authority is likely to assess as a mitigating factor any legitimate doubt as to the illegality of the processing while it will obviously assess as an aggravating factor the potential active attempt of the offender to prevent the revelation of the truth.

1.3 Levels of fines

1.3.1 Level 1 infringements

GDPR by splitting up the fines in two groups indicates by definition factors regarding the different impact and importance of several potential breached obligations.

Article 83 (4) of GDPR provides for that: «*Fines of up to 10 million euros or in the case of an undertaking up to 2% of the total worldwide annual turnover of the preceding financial year*

[58] Article 41 (1)

[59] See Article 29 Working Party Guidelines

whichever is higher, shall be imposed on the controllers or processors for breaches of the provisions with regard to: the conditions applicable to child's consent in relation to information society[60], processing which not require identification[61], general obligations, obligations relating to security of personal data, data protection impact assessment and prior consultation and the data officer[62], certification and certification bodies[63]. Similarly, the same amount of fines shall be imposed on certification bodies [64] as well as on monitoring bodies for failure to comply with their obligations under the Regulation[65]. The omission of GDPR to provide for the administrative sanction of fine for infringements related to the processing of personal data concerning to criminal convictions and offences can be attributed to legislators oversight [66].

1.3.2 Level 2 infringements

More serious infringements of the GDPR are subject to administrative fines of up to 20 million euros or, in the case of undertakings, 4% of the total worldwide annual turnover of the proceeding financial year whichever is higher [67]. In particular, breaches which lead to this applicable cap are those concerning: the basic principles for processing including conditions for consent [68], data subject's rights[69], transfers of personal data to a third country or an international organization[70], obligations pursuant to Member States law adopted under Chapter IX of the GDPR and non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flow by the supervisory authority [71] or failure to access in violation of GDPR.

[60]Article 8 of GDPR

[61]Article 11 of GDPR

[62]Articles 25-39 of the GDPR

[63]Articles 42 and 43 of the GDPR

[64]Articles 42 and 43.

[65]Article 41 para 4.

[66] Rucher D./ Kugler T., *New European General Data Protection Regulation…,* ep.cit, p.186

[67]Article 83 para 5

[68]Articles 5,6,7 of the GDPR

[69]Article 12-22 of GDPR

[70]Article 44-49 of GDPR

[71]Article 85 para 2

On January 21, 2019 the French Data Protection Authority (the ΄CNIL΄΄), after collective actions filed by two non-profit associations, imposed a fine of 50 million euros on Google LLD. This is the first fine imposed by the CNIL under the GDPR and the highest fine imposed by a supervisory authority within the EU under the GDPR to date[72].

1.3.3 Level of fines in the event of infringement of several provisions of the Regulation

In some cases, the applicable cap may not always be clear, for instance, a breach of a security obligation which is subject to the lower cap may also result in breaches of the principles of integrity and confidentiality subject to the higher cap. Therefore, further guidance will be needed from data protection authorities as well as case law interpreting the GDPR.

According to article 83 (3): « *If a controller or processor intentionally or negligently for the same or linked processing operations infringe several provisions of the GDPR, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement».*

That is to say, in the event of more infringements, the authority is entitled to the imposition of an increased fine, the total amount of which may not exceed the amount determined for the heaviest infringement, and in any case, the limits laid down in Article 283 (4) and (5).

With regard to the possibility of imposing a single fine in case of more infringements, the Greek Superior Administrative Court has ruled that « *Article 21 of Law 2472/1997 does not exclude the imposition of a single fine for several violations of the legislation on the protection of personal data therefore the supervisory authorities are entitled to impose a single fine in case of different infringements of the data protection legislation»*[73]However, article 83(3) refers only to controllers and processors, leaving outside its scope the other categories of infringers without sufficient reasons. The principle «*ne bis in idem»,* as interpreted by the ECJ, must be observed in proceedings for the imposition of a fine[74]. However, pursuant to the case law of ECJ «*neither the principle of ne bis in idem nor any other principle of law obliging the supervisory authority to take account of proceedings and penalties to which an undertaking has been subject in non-Member States»*[75].

---

[72]See: European Union impose 50 million euros in https://abcdigital.ie

[73] Greek Superior Administrative Court, (ΣΤΕ), 442/2014

[74] Recital 149 states that: «*The imposition of criminal penalties for infringements of national laws and of administrative penalties should not lead to a breach of the principle of ne bis in idem as interpreted by the Court of Justice».*

[75] ECJ, C-289/04 P, *Showa Denko KK*, (2006), (par.56-57)

Hereto, the case law in relation to the corresponding provisions of the Directive 95/46/EU is expected to partially mitigate the identified ambiguity. Similar reservations have also been raised for the provisions regulating the amount of the imminent administrative fines.

In particular, with regard to the upper limit of the fines imposed on undertakings, it is argued that this is lacking predictability in so far as the fine is calculated in an abstract manner, as a percentage of the total worldwide annual turnover of the infringing undertaking. [76] However, related objections in relation to Article 23 of the Regulation 1/2003 in relation to fines for infringements of the law on cartels dismissed by the ECJ [77]. Lastly, troublesome, and in terms of the principle of specialty, is the notion of the enterprise in Article 83. The ambiguity found, beyond the theoretical debate, undermines the legal certainty, since it can catalytically affect the amount of the fines by provoking unpredictable variations.[78]

1.4 The principle of specificity and of predictability

Article 83 which provides for the general framework for the imposition of fines, referring to other provisions, raising concerns about the compatibility of the framework with the principle of specificity and the need for predictability. In line with the case law of ECJ «a *penalty, even of a non-criminal nature, cannot be imposed unless it rests on a clear and unambiguous legal basis*»[79]. Similarly, the provision in addition to the infringement, must specify the penalties provided for.

In this context, the principle of the lawfulness of offenses and penalties requires, inter alia, that Community rules are clear and precise, in particular when they impose or permit the imposition of sanctions so that interested parties are clearly aware of the rights and obligations arising from these arrangements and to take the appropriate measures [80]. This principle applies both to criminal rules and to specific administrative arrangements which impose administrative penalties or allow their enforcement. [81] The prevailing view in the theory is that the provision of Article

[76]BeckOK*DatenSR/Hollander*, 20.Ed. 1.5.2017, DS-GVO Art.83 Rn.7-7.1.

[77] ECJ, C-501/11P, *Schindler,* (2003)(par.58).

[78] Komnios K., T*he general conditions for*…, ep.cit 512

[79] ECJ, C-137/85 *Maizena GesellschaftmbH*, (1987), (par.15), ECJ, C-210/00, *Kaserei Champignon Hofmeister*, (2002), (par.52)

[80]Komnios K., T*he general conditions for*…, ep.cit 511-512.

[81] General Court, T-99/04, *AC-Treuhand AG,* (2008), (par.31).

83(5)(α) is particularly problematic, which refers to «*basic principles for processing, including conditions for consent, pursuant to Articles 5,6,7 and 9»*. In particular, the provision of Article 5, referring to the principles governing the processing of personal data, teemed with vague concepts, making it difficult for the subjects to comply with the legislative requirements and take the appropriate measures, in view of the fact that for the time being there is no *clarification of the rules of liability* by the judicial interpretation. Hereto, the case law in relation to the corresponding provisions of the Directive 95/46/EU is expected to mitigate partly the ambiguity in question. Similar concerns have also been raised for the provisions regulating the amount of the administrative fines.

In particular, with regard to the upper limit of the fines imposed on undertakings, it is argued that this is lacking predictability in so far as the fine is calculated in an abstract manner, as a percentage of the total worldwide annual turnover of the infringing undertaking.[82] However, related objections in relation to Article 23 of the Regulation 1/2003 in relation to fines for infringements of the law on cartels dismissed by the ECJ [83].

Also, controversial, and in the light of principle of specificity- is the ''notion of undertaking'' in Article 83 (4)-(6). The ambiguity found, beyond the theoretical debate, undermines the legal certainty, as it can dramatically affect the level of administrative fines causing unpredictable variations.

[82]BeckOK*DatenSR/Hollander*,20.Ed. 1.5.2017, DS-GVO Art.83 Rn.7-7.1.

[83] Cf. ECJ, decision of 18 July 2013, C-501/11P, *Schindler,* (par.58).

Chapter 2. Recipients and procedure of administrative fines

2.1.1 The recipients of fines.

The administrative fines of article 83(4) are imposed by the supervisory authorities against the controllers and processors as well as against the certification and monitoring bodies[84.] Therefore, a fine cannot by imposed neither against a processor or and any person acting under the authority of the controller or of the processor (article 29 of GDPR), nor against the controller's representatives (articles 31 and 32 of GDPR) or on a data or recipient subject since they do not have any of the above characteristics. Similarly, a fine cannot be imposed on the data protection officer (article 4(7)) so that the reference of Article 39 concerning the duties of the Data Protection Officer, in Article 38 (4) (a) which defines the obligations of the controller or the processor is likely by mistake. It should be noted that it follows from Article 21 of Law 2472/1997 that the provisions regarding the imposition of administrative fines does not apply to the processors. The arrangement will nevertheless not apply to the extent that it is contrary to the GDPR.

On the other hand, administrative fines for breaches of articles Article 83 (5) and (6) shall be imposed under the substantive law on any infringer given that the articles in question do not designate specific recipients of the fines such as article 83(4).

Regarding the orders of the supervisory authorities, although they are generally addressed the controllers and to the processors as well as to the certification bodies, on the basis of Article 83 (6), it is argued that administrative fines can also be imposed against persons who are required to comply with the specific orders[85].

In addition, contrary to the applicable Greek legislation, where pursuant to Article 21 of Law 2472/1997, the Data Protection Authority imposes the administrative sanctions of the above article without exception on the controllers or their representatives and hence on public authorities, in other EU countries, as in Germany, it is not permissible to impose a fine on public authorities.

In the context of GDPR it is up to the Member States to decide whether and to what extent fines may be imposed on public authorities.[86]

[84] Articles 43 and 41 of GDPR

[85] Article 58 (2) in conjunction with article 83 (6)

[86] Article 83(7) in conjunction with the Recital 150.

2.1.2 The notion of ''undertaking''

Regarding the definition of the notion ''*undertaking*'' is particularly crucial since it relates to the method of calculating the administrative fines.[87]. The GDPR does not define the notion in question, however it should not be equated to the definition of an enterprise pursuant to article 4 (18) of the GDPR [88]. Recital 150 of the GDPR, defines that: «*an enterprise should rather be understood as an undertaking in accordance with Articles 102 and 102 of the TFEU, where fines are to be imposed on an undertaking»*. The TFEU does also not define the notion in question. According to the broad interpretation applied by the ECJ in antitrust cases: «a*n undertaking is every entity engaged in an economic activity, regardless of the legal status of the entity or the way in which is financed*[89]*.* Therefore, the ECJ has approved antitrust fines imposed by the Commission pursuant to article 101 of TFEU, on the parent company of a group of undertakings despite the fact that the parent company had not been involved in the infringement. The Court held that «*the mere fact that the parent company and its subsidiary, which have committed the infringement, form a single economic entity suffices to establish the parent's company liability.* [90]

Some authors in the legal literature and some data protection authorities draw for the reference in Recital 150 recital of the GDPR, to the notion of an undertaking in the antitrust context as described above that also under article 83 of the GDPR the group and not the individual legal entity is meant. The acceptance of the above assessment could lead to the following implications. First, fines against undertakings would be calculated on the basis of the turnover of the whole group of companies and not according to the turnover of the infringing legal entity. Second, the adoption of the definition of undertaking as applied by the ECJ in antitrust cases could also mean flexibility for the supervisory authority when determining the recipient(s) of an administrative fee. In the event of antitrust violations, fines can be levied a mother company for

---

[87] Rucket /Kugler., New European General Data…,ep.cit187-188.

[88] Article 4 para 18 states that: « e*nterprise means a natural or legal person engaged in an economic activity irrespective of its legal form, including partnerships or associations engaged in an economic activity».*

[89] ECJ, C-41/90-*Hofner and Elser*

[90] ECJ, C-521/09 P- *Elf Aquitaine;* ECJ, C-440/11P-*Stichting Administratie kantoor Portielje*

the breach committed by its subsidiaries under certain conditions[91]. Moreover, the antitrust definition of an undertaking enables the supervisory authority to impose fines after corporate restructurings on the legal successors of the infringing undertaking as they are generally considered to be still the same undertaking as their legal predecessor.

However, there remains a large legal uncertainty should the notion of an undertaking in GDPR can really be identical to the ECJ's interpretation in the antitrust context, on the grounds that in article 19 (4) of GDPR is expressly defined the term ''*group of undertakings*''.This differentiation in the text of the Regulation between an ''undertaking'' and a ''group of undertakings'' indicates that the legislator may not have made intentional reference to case law under which he ECJ interprets the term ''undertaking'' as including also a group of undertakings. It follows from the above that is hampered the interpretative use of Recital 150 taking also into account that pursuant to the settled case law of the ECJ «T*he preamble to a Community act has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording».*[92]

It is up to the national authorities to apply and ultimately to the ECJ to define the exact meaning of the undertaking in Article 83 of the GDPR.

The fines concern companies either established in the Union or not established in the Union *«where the processing activities are related to a) the offering of goods or services to the data subjects in Union, irrespective of whether a payment of the data subject is required or b) the monitoring of their behavior as far as their behavior takes place within the Union»*[93].

2.2 The Procedure for imposing administrative fines

2.2.1 Competent body for imposing administrative fines.

With regard to the power to impose administrative fines, article 83 does not contain a specific provision. However, given that the imposition of an administrative fine, according to Article 83 (2), falls within the corrective powers of article 58(2) (a) of GDPR, the power of the supervisory authority to impose fines is founded on article 55 of the GDPR. Therefore, and without prejudice to

[91] Cf.ECJ, decision of 29 September 2011, C-521/09 P- *Elf Aquitaine;* ECJ, decision of 11 July 2013, C-440/11P-*Stichting Administratie kantoorPortielje.*

[92] Cf. ECJ, decision of 24 November 2005, C-136/04, *DeutschesMilch-Kontor*, (parag.32)

[93] Article 3 para 2 of GDPR.

Article 83 (9), competent to levy administrative penalties are only the supervisory authorities and are not other national authorities. Each supervisory authority shall impose fines on the territory of its Member State. In particular, under Article 55 (1): *«Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State».* In case of infringements in more than one Member States, the risk of imposing multiple administrative fines is prevented by the provision of article 56 (1) which determines that: «*The supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor».* This is inferred by the exceptional provision of article 56 (2) according to which «*Each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State». Consequently,* in any other case competent to impose administrative fines is only the lead supervisory authority. Moreover, the procedure for imposing administrative fines as such is not defined by the Regulation. However, article 83 (8) provides for that « *The exercise by the supervisory authority of its power 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»*[94].

2.2.2 Administrative complaints

According to Article 77 of the Regulation: «*If a data subject feels that his rights under the GDPR have been violated, he can lodge an administrative complaint with a single supervisory authority, in particular in the Member State of his habitual residence, place of work or place of the alleged infringement».* The supervisory authority upon such complaint, which can be lodged, inter alia, by means of an electronic complaint submission form, must commence an investigation of the alleged infringement by the data controller or processor. In addition, Recital 141 stipulates that: «*The investigation by the supervisory authority should be carried out as appropriate on a case-by-case basis and subject to the judicial review* [95].

[94] Also, Recital 148 of GDPR stipulates 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»*

[95] Rucket/Kugler., *New European General Data*…, ep.cit.190.

The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period».

Moreover, according to Article 78 (1)(2):«*Each natural or legal person shall have the right to effective judicial remedy against a legally binding decision of a supervisory authority concerning them».* The supervisory authority before the imposition of the administrative fine should ensure that have been observed all the fundamental rights of the alleged infringer, that is, the right to a prior hearing and the right to judicial protection. Measures such as opinions or advice provided by the Supervisory Authority are not encompassed by these rights since they are not binding [96] .

According to article 21 para 2 of the Law 2472/1997 «The *administrative sanctions are always imposed upon prior hearing of the controller or his representative*».[97] The Greek Supreme Administrative Court held that: «*The provision of Article 21 para 2 of Law 2472/1997, interpreted in the light of Article 20 of the Constitution, has the meaning that the Authority, in exercising its aforementioned competence is required to duly observe the procedure for the hearing of the person concerned, which is also provided for in Article 6 of the Code of Administrative Procedure. That is to say, the Authority, by law, makes findings of infringements of the provisions on the lawfulness of data processing always after a lawful hearing of the person to whom the infringement is attributed».* Consequently, the supervisory authority before holding a meeting for imposing a fine is required to invite via summons the alleged infringer for presenting his arguments. Text of summons must state the reasons for which he is invited and should be served to the person concerned within a reasonable time before the hearing in order to be properly prepared. In addition, the supervisory authority, where feasible, should invite the data subject that affected by the infringement in order to expose his arguments and also for giving to the alleged infringer the right to make any rebuttal [98]. The decisions of the Authority imposing fines constitute title of execution and shall be served on the controller or his representative.

In accordance with the general principles of the Union, *«the supervisory authority is required to provide a statement of reasons in a decision imposing a fine, inter alia, for the amount of the fine imposed and the method chosen in that regard [99]. The statement of reasons must show*

---

[96] Recital 143.

[97] See Supreme Administrative Court, decision No. *96/2003.*

[98] Kanelopoulou Mpoti M., Sanctions for infringing personal data *in Kotsali Personal data, 2016, 407, Armanentos P./Sotiroupolos V. Personal Data, 2005,516-517.*

[99] Kanellopoulou-Mpoti M., S*anctions for the infringements of personal data in Kotsalis Personal data, 2016,407 where it is referred that :« The Authority's decision imposing a fine should include*

clearly and unequivocally the reasoning followed by the authority, so as to enable those concerned to know the grounds justifying the measure taken in order that they may assess whether it is appropriate to bring the matter before the Community judicature and if they do so, to enable the Court to carry out its review».

GDPR does not provide for the limitation periods within which the supervisory authorities should impose the administrative sanctions for breaches of its provisions. Therefore, the adoption of different limitation periods by the Member States hampers the desired uniform and consistent application of the rules of GDPR in the European Union[100].

2.2.3 Proceedings against the data controllers and data processors.

Additionally, data subjects entitled to brought proceedings directly against data controllers or processors for any breach of the GDPR regarding the processing of their personal data [101].

This is a major difference compared to the Directive 95/46 which provided for judicial remedy against controllers but not against processors. Proceedings shall be brought either before the courts of the Member State where the infringer is established or, unless the infringer is a public authority of a Member State acting in the exercise of its public powers, before the courts of the Member State of the data subject's residence[102]. In order to avoid contradictory judgments, GDPR states that «If related proceedings are pending before a court of another Member State, any Court seized at a later point in any time may suspend its proceedings[103].

Where proceedings are pending at first instance, the second court may also decline jurisdiction on request of a party in favor of the court first seized. This applies only if the first court has jurisdictions over the proceedings and if its law permits the consolidation of such related proceedings[104].

---

clear, detailed and thorough statement of reasons which justify not only the imposition of the fine but also the amount of the fine».

[100] Komnios K., The general conditions for…, ep.cit.513.

[101] Article 79

[102] Article 79 para 2

[103] Article 81 para 2

[104] Article 81 para 3

2.2.4 Representations of data subjects by Non-Profit Organizations.

The new legal regime introduces two provisions regarding the representation of data subjects by non-profit organizations in the course of administrative or judicial proceedings.[105]

Data subjects have the right to mandate non-profit bodies, organizations and associations to lodge administrative complaints on their behalf, to exercise the right to a judicial remedy or bring an action against data controllers and processors.[106] The NPOs may also claim damages on behalf of the data subjects should this provided for in Member State legislation.[107]

The possibility of data subjects of being represented by NPOs reinforces the rights of consumers given that individuals often do not have the resources to launch proceedings on their own. The NPOs must be properly constituted under the law of the respective Member State that is to have statutory objectives in the public interest, be active in the field of the protection of data subjects' rights and be of non-profit making character. Furthermore, GDPR includes an opening clause for collective redress according to which NPOs have independent right to lodge a complaint against an alleged breach of individual rights should this possibility provided for by Member State law. In this case the consent of the data subject does not constitute a prerequisite for the commencement of legal proceedings by the NPO. The possibility of such abstract enforcement of rights by NPOs is likely to result in an increase of proceedings against companies for alleged infringements of the GDPR.

[105] Article 80

[106] Articles 77-79

[107] Article 82

Conclusion

The GDPR constitutes a strong which legal instrument which responds to current technological innovations and to globalization. The GDPR by adopting the model of European law on free competition introduces an autonomous and effective administrative fining system in order to consolidate the uniform application of the substantive provisions of the GDPR throughout the European Union. This is an important development in the scientific field of European Data Protection law. A consistent application of the fining practice throughout the EU is ensured via the consistency mechanism. According to GDPR, administrative fines shall be effective, proportionate and dissuasive. The new legal framework provides for two levels of fines by which the more serious infringement are subject to administrative fines of up to 20 million euros or 4% of the organization's total annual global turnover. The GDPR imposes fines on both controllers and processors. In addition, accredited certification bodies which are responsible for properly assessing and certifying compliance by data controllers and processors with data protection regulation and organizational codes of conduct, may be subject to fines for breach of their obligations.

The concept of ''equivalence'' is determinant in assessing the extent of the obligations of the supervisory authorities to ensure consistency in the application of administrative fines. «*The high level of protection of natural persons and the removal of obstacles to flows of personal data within the Union can be safeguarded should the level of protection is equivalent in all Member States».*

The equivalent level of protection of personal data within the Union requires among others «e*quivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States».*

Moreover, equivalent sanction in all Member States and effective cooperation among the supervisory authorities of Member States is a way «*to prevent divergences hampering the free movement of personal data within the internal market ».*

GDPR establishes proceedings against data controllers and processors and entitle non-profit bodies to represent data subjects upon their consent in the course of administrative or judicial proceedings. In addition, includes an opening clause for collective redress that goes beyond the representation if Member States provide for NPO the right to lodge a complaint against an alleged infringement of individual rights under the GDPR.

The imposition of administrative fines does have legal implications to other powers of the supervisory authorities and the claim for damages in the sense that it does not prevent their exercise by substituting the latter.

Organizations which operate as either a data controller or processor in any Member State should be aware of the significant increase in both the amount and scope of potential fines under the new legal framework. They should also ensure that are in compliance with their obligations regarding the appropriate technical and organizational measures and that they have implemented the principles of privacy by design and privacy by default.

GDPR, through its excessive fines and the extension of the recipients of administrative sanctions, will be a decisive factor to the strict observance of legislation and thus the more effective protection of data subjects.

Bibliography

Rucker D./Kugler T., «New European General Data Protection Regulation: A Practitioner's Guide Ensuring Compliant Corporate Practice», *C.H. BECK – HART-NOMOS* (2018)

Kanelopoulou - Boti M., «Sanctions for personal data» i*n Kotsali Personal data», Nomiki Bibliothiki 2016*

Armamentos P / Sotiropoulos V., «Personal Data : Amendments to Law 2472/1997 by Law 3471 / 2006 and 3625/2007, Interpretation by article» *Sakkoulas publications, Athens-Thessaloniki (2008)*

Eugenia Alexandropoulou -Aigyptiadou., «Personal Data», *Nomiki Bibliothiki* (2016)

Komnios K.,«The general conditions for imposing fines under the GDPR: Contribution to the interpretation of article 83 of the GDPR», *ΔIME,* (2017/4)

EU Case law

ECJ C-562/12, LCL Le Credit Lyonnais (2014)

ECJ C-681/11, Schenker and Co AG (2013)

ECJ C-210/10, Urban, (2012)

ECJ C-497/15 Euro-Team Kft (2017)

ECJ C-498/15 Spiral-Gep Kft (2017)

ECJ C-210/00 Kaserei Champignon Hofmeiste (2001)

ECJ C-443/13, Ute Reindl (2014)

ECJ C-326/88, Hansen (1990)

ECJ C-338/00P, Volkswagen AG (2003)

ECJ C-289/04 P, Showa Denko KK (2006)

ECJ C-41/90 Hofner and Elser (1991)

ECJ C-97/08 P, Akzo Nobel (2009)

ECJ C-345/13, Karen Millen Fashions Ltd (2005)

ECJ C-137/85, Maizena Gesellschaft mbH (1987)

ECJ C-501/11P, Schindler (2013)

General Court T-161/05, Hoechst GmbH (2009)

General Court T-99/04, AC-Treuhand AG (2008)

ECHR, Engel and Others v. the Netherlands, (1976), Series A No.22,

ECHR, Sergey Zolotukhin v. Russia, (2009) No.14933/03

Greek Case law

Superior Administrative Court (ΣΤΕ) 1774/2016

Superior Administrative Court (ΣΤΕ) 3135/2015

Superior Administrative Court (ΣΤΕ) 1367/2008

Superior Administrative Court (ΣΤΕ) 4158/2000

Superior Administrative Court (ΣΤΕ) 1367/2008

Superior Administrative Court (ΣΤΕ) 1662/2009

Superior Administrative Court (ΣΤΕ) 96/2003

Superior Administrative Court (ΣΤΕ) 119/2015

Superior Administrative Court (ΣΤΕ) 751/2010

Superior Administrative Court (ΣΤΕ) 2491/2008

Resources

ARTICLE 29 DATA PROTECTION WORKING PARTY: Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (October 3, 2017)

Nemitz in Ehmann/Selmayr, DS-GVO

BeckOK DatenSR/*Hollander*, 20 Ed.1.5.2017, DS-GVO

Legislation Links

https://curia.europa.eu/jcms/jcms/j_6/en/

http://ec.europa.eu//justice/data-protection//index en.htm