www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt: 3 Sayı:1

Geliş:03.01.2021
Kabul:07.06.2021

The Administrative Fines Regime of the General Data Protection Regulation and Its Impact*

İbrahim Barış, Sayar
Trinity College Dublin, İstanbul Barosu, İstanbul, Türkiye, sayari@tcd.ie
ORCHID: https://orchid.org// 0000-0002-4290-6463

ABSTRACT
The GDPR provides a modernised and comprehensive personal data protection regime backed by strong enforcement measures. Aiming to ensure effective protection of personal data in the European Union, the GDPR allows the national data protection authorities to impose massive administrative fines along with other corrective powers for infringements of data protection rules. While the possible maximum amount of fines implies that the EU legislator seeks for complete compliance with the Regulation, the principles and assessment criteria protect the balance and encourage the parties involved to adopt a pro-active approach and to cooperate. Therefore, the GDPR sanction regime aims at effectiveness, proportionality, and dissuasiveness. Its implementation so far demonstrates a gradual increase not only in the number of violations that have become subject to administrative fines but also in sky-high fines in specific cases. In the following years, it is expected that a high level of coherent, consistent, and effective application of the GDPR's administrative fine regime throughout the EU will progressively be reached.
Keywords: European Union, General Data Protection Regulation, Enforcement, Administrative Fines.

Genel Veri Koruma Tüzüğü İdari Para Cezaları Rejimi ve Etkililiği

ÖZ
GVKT, güçlü yaptırım olanakları ile desteklenen modern ve kapsamlı bir kişisel verilerin korunması rejimi düzenlemektedir. Avrupa Birliği'nde kişisel verilerin etkili bir şekilde korunmasını sağlamayı amaçlayan GVKT, ulusal veri koruma kurullarına, diğer düzeltici önlemler alma yetkisinin yanı sıra veri koruma kurallarının ihlali halinde önemli miktarlarda idari para cezası uygulama yetkisi vermektedir. İdari para cezalarının olası maksimum miktarı, AB yasa koyucusunun Tüzüğe tam uyum sağlanmasını amaçladığına işaret ederken, idari para cezalarına ilişkin temel ilkeler ile değerlendirme kriterleri dengeyi sağlamakta ve ilgili tarafları proaktif bir yaklaşım benimseyerek iş birliği yapmaya teşvik etmektedir. Bu nedenle GDPR yaptırım rejimi etkililiği, orantılılığı ve caydırıcılığı sağlamayı amaçlamaktadır. Şimdiye kadarki uygulama, yalnızca idari para cezalarına konu olan ihlallerin sayısında değil, aynı zamanda belirli ihlaller halinde uygulanan yüksek para cezalarında da kademeli bir artış olduğunu göstermiştir. Önümüzdeki yıllarda aşamalı olarak, GVKT'nin idari para cezalarına ilişkin kurallarının AB genelinde daha uyumlu, istikrarlı ve etkili bir şekilde uygulanacağı beklenmektedir.
Anahtar Sözcükler: Avrupa Birliği, Genel Veri Koruma Tüzüğü, Yaptırım, İdari Para Cezası.

Atıf Gösterme	Sayar, İ. B., (2021). The Administrative Fines Regime of the General Data Protection Regulation and Its Impact, *Kişisel Verileri Koruma Dergisi*. *3*(1), 1-16.

* This article is the updated version of the article that was written by the author in 'Data Protection: Law, Policy and Practice' module within Trinity College Dublin Intellectual Property & Information Technology Law LLM Programme. I would like to express my gratitude to the Jean Monnet Scholarship Programme.

INTRODUCTION

Today, we live in a data-driven digital environment in which we create a vast amount of personal information that is processed by natural persons, companies, and government agencies at any given time. The enormous volume of processed personal data brings along substantial risks of misapplication, mishandling, and misprocessing of such personal data (Murray, 2019). These risks are even more visible during the current Covid-19 pandemic (Lillington, 2020) as using so-called "tracing" and "warning" mobile applications to track millions of individuals' movements and contacts or to gather health data on the infection-related symptoms aiming to tackle the crisis is on the agenda (European Commission, April 2020; European Commission, October 2020).

The ever-increasing intrusions to our data require not only modern, harmonised and extended data protection rules but also strong protection since a law lacking effective sanctions is not a law at all (Golla, 2017). The emphasis on the need, *inter alia*, for more adequate enforcement of data protection rules (FRA, 2013) led to the adoption of the General Data Protection Regulation (GDPR) which seeks effective protection of personal data throughout the European Union (EU) and establishes equivalent and harmonised sanctions for infringements (GDPR, recital 11). In this context, GDPR equips supervisory authorities with the power to impose sky-high administrative fines, which has been inspired by the European Competition Law (Nemitz, 2020), along with a wide range of other corrective powers for infringements of the Regulation.

A recent study, which was prepared by an international law firm and published at the beginning of 2020, covering the period from the entry into force of the GDPR, i.e. 25 May 2018, to 27 January 2020 has revealed that a total of 160.921 data breaches have been notified to national data protection authorities (DPAs) within the European Economic Area (EEA) and the total (reported) GDPR fines in the same period were over 114 million EUR which was relatively low considering the possibility of the imposition of fines up to 4% of the total worldwide annual turnover in case of undertakings (DLA Piper, 2020). Since the publication of this report, the numbers have gone up. Thus far, the biggest GDPR fines of 50 million EUR, 35.3 million EUR, and 27.8 million EUR have been imposed by French DPA (CNIL) against Google (CNIL, 2019), the Hamburg Commissioner for Data Protection and Freedom of Information against H&M (EDPB, October 2020) and Italian DPA against a telecommunications provider (EDPB, February 2020) respectively. On the other hand, the fines of 183.4 million GBP and 99 million GBP against British Airways and Marriott Inc. proposed by the UK Information Commissioner's Office (ICO), the finalisation of which have been delayed due to the Covid-19 (Corfield, 2020), were dramatically reduced to 20 million GBP (ICO, 16 October 2020) and 18.4 million GBP (ICO, 30 October 2020) respectively.

In this article, the notion of administrative fines under the GDPR and its impact on the implementation of data protection rules will be analysed. In the first chapter, the scope of fines will be explained following a brief overview of the legal framework and evolution of the enforcement of data protection rules in the EU. Thereon, the principles and assessment criteria for the imposition of fines will be examined. In the last chapter, the application of GDPR fines by national DPAs to date will be evaluated along with its overall impact.

AN OVERVIEW OF THE ADMINISTRATIVE FINES UNDER THE GDPR

The Legal Framework and Evolution of Data Protection Enforcement

In Europe, data protection is rooted in the European Convention on Human Rights (ECHR) (Pila and Torremans, 2018). Article 8 of the ECHR guarantees the right to respect for private and family life, home and correspondence, and an individual's right to personal data protection forms part of this right (FRA, 2018). In the context of the Council of Europe (CoE), Convention 108 is the first and, to date, only legally binding multilateral instrument on the protection of privacy and personal data (CoE Directorate, 2020). It underwent a modernisation process which was completed, although not entered into force yet, with the adoption of an amending protocol in 2018 in parallel with the reform of EU data protection rules (FRA, 2018). The Modernised Convention 108+ aims to reach an effective level of enforcement (FRA, 2018) and to this end, it requires the signatory parties to establish judicial and non-judicial sanctions for violations (Art. 12), to grant supervisory authorities with the power to impose administrative sanctions that are effective, proportionate and dissuasive (Explanatory Report to the Convention 108+, Art. 12) as well as to guarantee their independence and impartiality (Art. 15).

Under the EU law, the Charter of Fundamental Rights (Charter) which has become legally binding with the entry into force of the Lisbon Treaty not only guarantees the right to respect for private and family life but also recognizes the right to protection of personal data as a fundamental right, respectively in Articles 7 and 8. The latter is explicitly provided in Article 16 of the Treaty on the Functioning of the European Union (TFEU) which gives EU competence to legislate on data protection matters and served as a legal basis for the GDPR (FRA, 2018).

The harmonisation of the EU data protection law has been realized for the first time (Murray, 2019) with the Directive 95/46/EC that was adopted as a result of the necessity to uniform various data protection rules among the Member States to ensure a high level of protection and the free flow of personal data, which is crucial for the effective functioning of the European internal market (the

Directive 95/46/EC, recitals 3-8). However, in practice, the Directive 95/46/EC failed to provide a complete harmonisation as it was incorporated by the Member States into their national laws differently which resulted in varied rules (FRA, 2018). In terms of sanctions and particularly administrative fines, Article 24 of the Directive 95/46/EC left their regulation at the discretion of the Member States. This resulted in the existence of significant differences across the EU not only in terms of the availability of the fines but also in their maximum amounts (Golla, 2017).

The need to reform data protection rules led to the adoption of the GDPR which has been in force since 25 May 2018. The GDPR, establishing a uniform framework for data protection regime throughout the EU, not only harmonised and extended the rights of data subjects (Pila and Torremans, 2019) but also expanded and detailed the obligations of those who process and determine the processing of personal data (GDPR, recital 11). The two central changes in the GDPR are the equivalent sanctions for infringements in the Member States and the scope of their reach as the Regulation also applies to organisations operating outside of the EU (GDPR, Art. 3).

On the one hand, it was argued that the GDPR, backed by strong enforcement measures including massive fines, will bring an end to the previous lack of enforcement of data protection rules (Albrecht, 2016). On the other hand, some authors were sceptical that the GDPR will miraculously solve all the issues surrounding the enforcement of data protection rules while it will undoubtedly result in more frequent and higher fines for infringements across the Member States (Golla, 2017). It was even argued that the compliance and enforcement of the GDPR in a substantial way is almost impossible due to its very broad material and personal scope which results in the application of data protection rules to almost anyone processing practically any information at nearly any time (Purtova, 2018). It was underlined that this will lead to a more selective enforcement approach by national DPAs to cope with the increasing workload (Purtova, 2018).

The Scope of Fines under the GDPR

The GDPR, *inter alia*, focuses on effective and equivalent sanctions for infringements of data protection rules (Golla, 2017). This is essential for an adequate and consistent level of protection of personal data across the EU (GDPR, recitals 11 and 13). In this context, the administrative fines are the strongest sanctioning mechanism directly provided by the GDPR (Golla, 2017). They are exceeding the fines provided in the (previous) Member State national laws not only in the maximum amounts but also in scope for offences subject to fines (Golla, 2017). Along with the power to impose fines, the supervisory authorities have been equipped with several other corrective powers such as issuing warnings or reprimands (GDPR, Art. 58).

The GDPR adopts a tiered approach concerning the administrative fines. Infringements provided under Articles 83(5) and (6) of the GDPR are subject to fines up to 20 million EUR or in the case of an undertaking, up to %4 of the total worldwide annual turnover of the preceding financial year, whichever is higher. The relevant infringements include violations of the basic principles for processing of personal data and the conditions for consent, the data subjects' rights including the right to be forgotten, rules regarding the transfers of personal data to non-EU countries or international organisations and failure to comply with orders of supervisory authorities. As per Article 83(3) of the GDPR, in case of infringements of several provisions by data controllers or processors intentionally or negligently for the same or linked processing operations, the total amount of the fine to be imposed is limited with this maximum amount of fine. The lower level of fines can be up to 10 million EUR or in the case of an undertaking, up to %2 of the total worldwide annual turnover, whichever is higher. The subject infringements include violations relating to the requirements for data protection by design and default, obligations to cooperate with supervisory authorities and, appoint a data protection officer as well as obligations of the certification and monitoring bodies.

Concerning the public authorities and bodies, Article 83(7) of the GDPR grants discretion to the Member States to regulate whether and to what extent fines may be imposed on them. In Ireland, the initial proposal of the Data Protection Act 2018 had exempted public authorities or bodies from fines and this has caused serious debates (McLaughlin, 2018). The final version of Article 141(4) of the Data Protection Act 2018 regulates the power of the Irish Data Protection Commission (DPC) to impose administrative fines up to 1 million EUR against data controllers or processors that are public authorities or bodies.

The legal systems of some of the Member States, such as Ireland, Denmark, or Estonia (GDPR, recital 151), do not allow for administrative fines as set out in the GDPR. In line with Article 83(9) of the GDPR, in these countries, the fine is initiated by the national DPA and imposed by competent national courts. In Ireland, as per section 143 of the Data Protection Act 2018, the Irish DPC will announce its intention to impose an administrative fine and subsequently apply to Circuit Court for the confirmation of its decision.

THE PRINCIPLES AND CRITERIA FOR THE APPLICATION OF FINES

Principles for the Imposition of Fines

Along with the level of fines, Article 83 of the GDPR lays down the criteria which national DPAs have to apply when imposing administrative fines in case of infringements of the Regulation. On 3

October 2017, the Article 29 Working Party (A29WP), which was an independent European advisory body on data protection and privacy that was set up pursuant to Article 29 of the Directive 94/46/EC and was replaced by the EDPB that was established as per Article 68 of the GDPR, has published a guideline on the application of administrative fines (A29WP, 2017). This guideline has been endorsed by the EDPB during its first plenary meeting on 25 May 2018 and now it is being called as EDPB Guideline. It guides national DPAs aiming to establish a uniform understanding and enforcement of the Regulation.

The Principle of Equivalence

The first principle underlined in the EDPB Guideline is that violations of the GDPR must lead to the imposition of equivalent or in other words, consistent sanctions. This principle not only requires the imposition of similar fines to similar cases by national DPAs of the Member States but also the application of the same level of sanctions to the same type of violations (Maxwell and Gateau, 2019). Recital 10 of the GDPR emphasizes the need for an equivalent level of data protection in the EU, consistent application of the rules, and recital 11 stresses the requirement of equivalent sanctions for violations.

The cooperation and consistency mechanisms of the GDPR are particularly important to fulfil the principle of equivalence both in national and cross-border cases since the consistency of application and enforcement of the GDPR has been particularly emphasised in the rules governing these mechanisms (GDPR, Art. 57(1)(g) and 63). While the GDPR gives national DPAs discretion in their choice of the corrective measure to be imposed and in case of a fine, the level of fine by regulating that national DPAs have the complete independence in exercising their powers (GDPR, Art. 52); EDPB Guideline emphasizes the need for continuous cooperation between national DPAs to enhance consistency on an ongoing basis (A29WP, 2017).

Effectiveness, Proportionality, and Dissuasiveness

Article 83(1) of the GDPR governs that the imposition of administrative fines should be effective, proportionate, and dissuasive. These criteria have also been mentioned in several other EU legislative instruments such as Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union (Art. 5(4)). The Modernised Convention 108+ also rules that sanctions should be effective, proportionate, and dissuasive (Explanatory Report, Art. 12). According to the EDPB Guideline, administrative fines have to appropriately correspond to the nature, significance, and consequences of the infringement and all elements of national or cross-border cases shall be assessed by national DPAs consistently and objectively (A29WP, 2017).

The assessment of these criteria by national DPAs must also involve the reflection of the aim pursued by the applied corrective measure. As noted in recital 148 of the GDPR, administrative fines can be imposed for violations of the Regulation in addition to, or instead of other appropriate measures. In this context, in case of a minor infringement (*according to the EDPB Guideline, these may be infringements that do not pose a considerable risk to data subjects' rights and affect the core of the obligation*), a reprimand which seeks to re-establish compliance with the GDPR rules may be implemented instead of an administrative fine (GDPR, recital 148). This is also valid concerning natural persons if it would create a disproportionate burden on them (GDPR, recital 148). If a fine to be imposed on a natural person, national DPAs have to consider both the general level of income in the relevant Member State and the economic situation of the concerning person when determining the amount of the fine (GDPR, recital 150).

However, concerning undertakings, this argument is not strongly valid (O'Dell, 2020). The notion of an undertaking has to be evaluated in accordance with Articles 101 and 102 of the TFEU (GDPR, recital 150), namely as an economic unit that may be formed by the parent company and all involved subsidiaries. EDPB Guideline also refers to the case-law of the Court of Justice of the European Union in which the notion of an undertaking has been defined as "encompasses every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed" in the context of competition law (Case C-41/90 *Klaus Höfner and Fritz Elser v Macrotron GmbH*, para 21). This broad view of the concept of undertaking leads to (the possibility of imposition of) higher amounts of fines as in the cases of British Airways and Marriot (although the amount of fines that were imposed against these companies have been significantly reduced by the ICO due to the impact of Covid-19 on the aviation and hospitality sector) and the large group of companies cannot minimise their risks by establishing specific sub-companies for personal data processing purposes (O'Dell, 2020).

Individual Assessment and Cooperation between National DPAs

Article 83(2) of the GDPR requires an assessment of all circumstances of each individual case during the evaluation of whether to impose a fine or determining its amount. The importance of administrative fines as a crucial tool to be used in appropriate cases has been emphasised in the EDPB Guideline where national DPAs are encouraged to adopt a balanced approach for the implementation of corrective measures (A29WP, 2017). The imposition of fines should not damage its effectiveness as a tool. EDPB Guideline also urged national DPAs to cooperate with each other as well as with the European Commission, which will help to achieve consistency in the implementation of administrative fines.

Assessment Criteria for the Imposition of Fines

Article 83(2) of the GDPR sets out the criteria that have to be assessed by national DPAs concerning the imposition of administrative fines. The criteria include the nature of the infringement consisting of the scope and purpose of the processing of personal data as well as the number of the data subjects and the level of their damage, whether the infringement is intentional or negligent, the existence of mitigation, the level of responsibility of data controller or processor, the existence of previous infringements, the degree of cooperation with the national DPA, the categories of personal data involved, the way that the national DPA has become aware of the infringement, the existence of previous corrective measures adopted by the national DPA on the same case, adherence to codes of conduct and certification and the existence of other aggravating or mitigation factors (See for a detailed explanation of the criteria; A29WP, 2017; Maxwell and Gateau, 2019).

The primary goal of the sanctions provided under the GDPR is to achieve effective protection of personal data across the EU rather than punishing the relevant parties for their infringement. The author of this article considers that while the sky-high amounts of administrative fines are hanging above the natural persons, companies and government agencies like the sword of Damocles aiming to ensure the complete compliance with the data protection rules; the assessment criteria of Article 83(2) of the GDPR reflects a more constructive approach of the EU legislator. Indeed, many of these criteria such as the mitigatory actions and the level of cooperation of data controllers or processors encourage the latter to adopt a pro-active approach in case of non-compliance as the more they take adequate action to compensate the offence, the less the administrative fine will be. Therefore, the assessment criteria are particularly important for the prevention of any tendency of hiding the non-compliance and data breaches in the presence of the availability of massive amounts of fines.

Policies published by national DPAs

A number of policies for the calculation of administrative fines have been published by various national DPAs while any guideline of EDPB in this context is currently unavailable. The first policy document of this kind has been published by the Dutch DPA on 14 March 2019 (Steenbruggen et al., 2019). The policy has divided infringements into four categories and assigned each category a specific bandwidth as well as a standard fine. The latter is the initial point for the calculation of the fine and the exact amount will then be determined following an assessment of all circumstances of each case. Since the bandwidths and standard fines (*the highest bandwidth is 1 million EUR and the highest standard fine is 750.000 EUR*) are lower than the maximum amounts of fines set out in the GDPR, it has been interpreted as a sign that the Dutch DPA will not impose the towering fines of the GDPR apart from exceptional cases (Steenbruggen et al., 2019). The highest amount of the GDPR fine imposed by the

Dutch DPA so far was 830.000 EUR (Bodewits and Blok, 2020). This fine was issued against the Dutch Credit Registration Bureau for the violation of Articles 12(2) and (5) of the GDPR as a result of its practice to charge fees and discourage individuals who wanted to access their data (Bodewits and Blok, 2020).

Soon after, the German Conference of Data Protection Authorities has also published a policy on 16 October 2019 which aims to provide a standardized approach for the calculation of fines to be imposed for violations in Germany (Leuthner and Schonhofen, 2019). Unlike the Dutch version, the German model not only provides a more comprehensive guide for the calculation of fines but also signals much higher fines as it places a great emphasis on the turnovers of undertakings. Accordingly, the application of this policy will likely lead to a significant rise in the amounts of fines, specifically for larger organisations facing much higher fines even for minor breaches. One of the first implementations of the German policy by the Berlin DPA has led to a 14.5 million EUR fine, imposed against a German real estate company due to over retention of personal data (Ritzer and Filkina, 2019).

On 2 October 2020, the Hamburg DPA imposed a 35.3 million EUR fine, the highest GDPR fine in Germany up to date and one of the highest GDPR fines in the EU, against H&M's Service Center due to the unlawful data collection and recordal of details about employees' private lives (EDPB, October 2020). The Hamburg DPA underlined that H&M was cooperative, provided transparent information, and put efforts to compensate those affected due to unlawful personal data collection/recordal (the Hamburg DPA, 2020). As argued by Schröder et al. (2020), since H&M's total worldwide annual turnover of the preceding financial year is massive, i.e. 21.9 billion EUR, the amount of fine could have been as high as 61 million EUR calculated according to the German policy; however, it has been cut almost in half by the Hamburg DPA due to H&M's full cooperation. Therefore, this decision is an important example demonstrating the importance of Art. 83/2(f) of the GDPR, which reads "*the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement"* shall be considered when deciding on the amount of the administrative fine.

A recent court ruling in Germany has made the German policy for the calculation of fines legally questionable. In late 2019, the German Federal DPA has issued a 9.55 million EUR fine against a German telecom company (Ritzer and Filkina, 2020). Recently, the Regional Court of Bonn overruled the German Federal DPA's decision on the ground that it was unreasonably high and drastically reduced this fine by 90% to 900.000 EUR (Tinnefeld and Hanssen, 2020). The German Court underlined that the determination of the amount of the fine mainly based on the total worldwide annual

turnover of the preceding financial year is not appropriate, in other words, the emphasis on the turnover within the Germany policy for the calculation of fines is disproportionate given that not only a minor violation by an undertaking with a high turnover may lead to disproportionately high fines but also a serious violation by an undertaking with a low turnover may lead to a disproportionately low fine (Ritzer and Filkina, 2020). Given that the Court put an emphasis on the objective factors of the violation of data protection rules and criticised the Germany policy which mainly relies on the turnover criteria, the Germany model would likely need to be modified as it does not meet the standards set out in Art. 83 of the GDPR (Ritzer and Filkina, 2020; Tinnefeld and Hanssen, 2020).

THE APPLICATION OF GDPR FINES BY NATIONAL DPAs AND ITS OVERALL IMPACT

The GDPR Fines Imposed by National DPAs Till Now

During the initial period as of the entry into force of the GDPR, the number of fines imposed for the infringements of the Regulation and their total amount was relatively low. Studies demonstrated that only 91 (reported) fines have been imposed in the EEA until 28 January 2019 (DLA Piper, 2019) meanwhile the total amount of fines have reached 56 million EUR until the first anniversary of the GDPR (IAPP, 2020), while 50 million EUR of which is the single fine imposed against Google by CNIL. Over time, the number of fines and cases that resulted in fines worth millions of EUR gradually increased. As of the end of January 2020, the total amount of fines imposed under the GDPR reached 114 million EUR with France, Germany, and Austria were the top countries that issued high value of fines (DLA Piper, 2020). In this context, an international law firm has created a GDPR Enforcement Tracker tool that includes up-to-date information on the fines imposed by national DPAs under the GDPR (See <www.enforcementtracker.com>).

The first GDPR fine was imposed in Portugal on 22 October 2018 (O'Dell, 2020). A hospital has been fined 400.000 EUR by the Portuguese DPA for three violations of the GDPR, namely violation of data minimisation, integrity and confidentiality principles provided under Articles 5(1)(c) and (f) as well as failure to ensure an adequate level of security provided under Article 32(1)(b) of the GDPR (Monteiro, 2019). The importance of the first GDPR fine is that not only the violation involves sensitive personal data but also the Portuguese DPA acted upon a newspaper article and subsequent confirmation via inspection rather than a complaint. Maltese supervisory authority is the first DPA that has issued a fine to a public body in line with Article 32 of the GDPR which sets out the rules for the security of data processing (IDPC, 2019). 5.000 EUR fine has been imposed on the Lands Authority of Malta due to the lack of adequate security measures of the online application platform on its portal.

The first significant GDPR fine of 50 million EUR was imposed against Google LLC by CNIL on 21 January 2019 (CNIL, 2019). CNIL has found two types of breaches of the GDPR, namely lack of transparency, inadequate information, and Google's failure to obtain valid consent from data subjects concerning the ads personalization processing. When determining the amount of the fine, CNIL has considered the existence of severe violations of the fundamental principles of the GDPR, the wide extent of the processing of users' data by Google, the continuous character of the violation as well as the market share of Google's services in France. This substantial fine not only displays the significance of valid consent as a basis for lawful processing of personal data (O'Dell, 2020) but it has also been regarded as a milestone in the history of privacy and the beginning of the GDPR enforcement era implying the probable subsequent massive fines which ultimately will draw the implementation and enforcement line of the GDPR in practice (Ram and Khan, 2019).

While the 50 million EUR fine imposed against Google by CNIL on 21 January 2019 is still the biggest GDPR fine up to date, ICO announced its intention to impose 183.4 million GBP and 99 million GBP fines against British Airways (ICO, 2019) and Marriot Inc. (ICO, 2019) on 08 and 09 July 2019 respectively. Both of the proposed fines were related to cyber incidents which have been realised because of the poor level of security systems of undertakings that have affected millions of individual's data. The Marriot case is particularly important as the initial incident affected Starwood Hotels Group in 2014 which has subsequently been acquired by Marriott that failed to undertake adequate due diligence. However, Covid-19 had become a major factor in the future of both fines since both fines were significantly reduced to 20 million GBP (ICO, 16 October 2020) and 18.4 million GBP (ICO, 30 October 2020) respectively. While GDPR does not include a criterion such as the potential impact of the fine on the undertaking or the latter's ability to pay the fine when determining the amount of the fine, ICO's policy requires the consideration of mitigating factors as well as financial hardship (ICO, 2018). As predicted by Baines (2020), since the airline and hospitality industries were among the top that is affected by the crisis, it has led to a significant reduction in fines imposed against British Airways and Marriot Inc. (Baines, 2020).

From the entry into force until recently, neither Ireland nor Luxembourg DPA reported a GDPR fine despite they are the home of EU headquarters of multinational "big tech" companies such as Facebook, Google, Apple, Amazon, and PayPal. While Luxembourg DPA still did not issue a GDPR fine, Ireland's Data Protection Commission (DPC) has announced its intention to impose a 450.000 EUR fine on Twitter on 15 December 2020 for the infringement of articles 33(1) and 33(5) of the GDPR (EDPB, December 2020). The Irish DPC's Twitter decision is particularly important since it was the first decision that went through the dispute resolution process set out in Art. 65 of the GDPR (EDPB, November 2020) and the draft decision was the first one in a "big tech" case on which all

national DPAs in the EU were consulted as concerned DPAs in line with Art. 60 of the GDPR (The Irish DPC, 2020).

The Overall Impact of the GDPR Fines

The GDPR fines serve two essential functions. Firstly, they increase the incentive of data controllers or processors to act lawfully, to respect the rights of the data subjects, and to comply with the GDPR rules (Nemitz, 2020). Secondly, they play an important role in both special and general discouragement of further infringements, given that high fines draw significant public attention, especially in the case of well-known entities such as Google, Twitter, H&M, British Airways or Marriott, Inc. The implementation of fines by national DPAs will widely determine the level of fulfilment of these functions and therefore, they have to be adequately equipped concerning infrastructure, personnel, and finances.

In this context, the massive maximum amounts of administrative fines in case of non-compliance along with the extra-territorial application of the GDPR is specifically crucial for the U.S. tech companies such as Alphabet (Google parent company) or Facebook. (Houser and Voss, 2018) Indeed, while they are only faced with relatively small amounts of fines due to limitations in the national laws of the Member States before the entry into force of the GDPR, the latter can switch this practice substantially and pave the way for the imposition of fines amounted billions of EUR. As such, the regime of fines under the GDPR is a significant incentive for large-scale tech companies to comply with the rules and principles of the new data protection regime and modify their business models and practices accordingly.

Some critics argued that the two-and-a-half-year implementation of the GDPR created frustration over the unsatisfactory level of enforcement actions (Kobie, 2020), in particular by Irish and Luxembourg DPAs that oversee tech giants, and weak cooperation between national DPAs on investigations (Vinocur, 2019). The one-stop-shop regime of the GDPR has been questioned, specifically concerning Irish DPC and doubts about its willingness to rigorously apply the sanctions regime upon tech companies that have undoubtedly crucial importance for the Irish economy (Vinocur, 2019). While the Irish DPA recently announced its intention to issue a fine of 450.000 EUR on Twitter and there are ongoing investigations against other big tech companies such as Facebook/Instagram/WhatsApp, LinkedIn, Apple, Twitter (Irish DPC, 2019) Google, and Tinder (Jones, 2020), criticism as it is overwhelmed by the workload and insufficiently equipped for its task has been expressed (Scally, 2020) towards the Irish DPC which has received less than a third of the additional funding it requested for its 2020 budget (Taylor, 2019). Helen Dixon, the commissioner for the Irish DPC, underlined that while there is a high demand for quick and heavy fines on organisations for data protection

infringements, they need to observe fair procedures and build strong cases as "there would be little benefit in mass-producing decisions only to have them overturned by the courts" (Irish DPC, 2019). While the Irish DPC's budget is further increased to 19.1 million EUR for 2021; a significant increase in its workload can also be expected in the new year (the Irish DPC, October 2020).

The sanction regime of the GDPR is inspired by the European Competition Law and therefore, the national DPAs must take advantage of the extensive experience of the EU competition authorities. As emphasised by Helen Dixon, while EU competition investigations take several years to complete (Irish DPC, 2019), they ultimately lead to the imposition of billion EUR fines (European Commission, 2019; Google has also been fined by the European Commission 2.42 billion EUR and 4.34 billion EUR in 2017 and 2018 respectively). Soon, similar high fines, specifically on "big tech" companies, can be expected for serious breaches of the GDPR, particularly from the Irish DPC, based on strong cases (O'Dell, 2020).

CONCLUSION

"Houston, we have had a problem". The famous quotation may be used to depict the era before the GDPR when (*de facto* unharmonized) data protection rules across the EU could not be efficiently implemented and protected through fierce sanctions, in particular administrative fines. The GDPR, which has also served as a model for various countries across the globe, has been adopted to create comprehensive and modernised rules which will redress the challenges of the digital age. Therefore, the GDPR consists of one of the most comprehensive collections of data protection rules backed by substantial enforcement measures.

On the one hand, the sanction regime of the GDPR and particularly administrative fines are high enough to convey the message that the desire of the EU legislator is the complete and coherent implementation of data protection rules, non-compliance with which may have serious consequences. Thus, they are adequate to expect that data controllers or processors abstain from any infringement and put their utmost effort to ensure compliance. On the other hand, the principles and assessment criteria of the fines are crucial to protect the balance and to encourage relevant parties for a pro-active approach and cooperation.

Nevertheless, the two-and-a-half-year implementation of the GDPR has shown that the intended (high) level of protection and effective enforcement has not been reached yet in practice. The administrative fines mechanism is particularly important to effectively protect the fundamental right of data protection and without the efficient implementation of this strong tool by national DPAs, the GDPR

will be mighty only on paper. As the current digital world is constantly changing, it is understandable to expect quick actions to ensure that data protection rules are adequately respected. However, since the decisions of national DPAs are subject to judicial review, it is also important to build strong cases that will result in favor of authorities at the litigation stage and not to sacrifice the quality for the sake of expediency. The Regional Court of Bonn's decision reducing the fine imposed by German Federal DPA's by 90% and establishing the Germany policy for the calculation of fines does not meet the standards set out in Art. 83 of the GDPR is a good example to this critical point.

In subsequent years, it can be expected that the physical, personal and economical capacity of national DPAs across the EU, as well as the level of cooperation between them, will continue to increase, new EDPB guidelines, particularly on the calculation of the fines will be published, a more frequent and higher level of fines will be imposed in case of infringements following the completion of pending investigations carried out by national DPAs and consequently, a high level of coherent, consistent and effective application of the GDPR's sanctions regime will be progressively reached.

BIBLIOGRAPHY

**The last access to all given internet sources is 02 January 2021.*

Albrecht J P, (2016). 'How the GDPR Will Change the World' 2(3) EDPLR.

Article 29 Working Party, (2017) 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679' (WP 253)

Baines J, (2020). 'Covid-19 and ICO's proposed fines for BA and Marriott' (Mishcon de Reya) <www.mishcon.com>.

Bodewits J and Blok B, (2020). 'Dutch DPA Issues Record Fine for Violating GDPR Data Subject Rights' (Lexology) <www.lexology.com>.

Case C-41/90 *Kalus Höfner and Fritz Elser v Macrotron GmbH* [1991] ECR I-01979.

Charter of Fundamental Rights of the European Union [2012] OJ C 326.

CNIL, (2019). 'The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC' <www.cnil.fr>.

Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C 326.

Corfield G, (2020). 'British Airways and Marriott UK data protection fines deferred again as coronavirus shutdown hits business' *The Register* <www.theregister.co.uk>.

Council of Europe Directorate General Human Rights and Rule of Law, (2020). 'Data Protection Convention 108' <www.youtube.com>.

Council of Europe, (1950). Convention for the Protection of Human Rights and Fundamental Freedoms (as amended) ETS 5.

Council of Europe, (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108.

Council of Europe, (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No. 223.

Data Protection Act 2018 of Ireland.

Data Protection Commission, 'Annual Report' [2019].

Directive 95/46/EC 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 [1995] OJ L 281.

DLA Piper, (2020). 'GDPR data breach survey: January 2020' 4 <www.dlapiper.com>.

- 'Over 59.000 personal data breaches reported across Europe since introduction of GDPR, according to DLA Piper survey' (6 February 2019) <www.dlapiper.com>.

EU Agency for Fundamental Rights, (2013). *Access to data protection remedies in EU Member.*

European Commission, (2020). 'Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures'

- 'Coronavirus: EU interoperability gateway for contact tracing and warning apps – Questions and Answers' (19 October 2020).
- 'Commission fines Google €1.49 billion for abusive practices in online advertising' (20 March 2019).

European Data Protection Board, (2020). 'Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre'

- 'Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR' (09 November 2020).
- 'Irish Data Protection Commission announces decision in Twitter inquiry' (15 December 2020).
- 'Marketing: The Italian SA Fines TIM EUR 27.8 Million' (1 February 2020).

Golla S J, (2017). 'Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR' 8(1) JIPITEC.

Hamburg DPA, (2020). '35.3 million euros fine for data protection violations in the H&M service center' <datenschutz-hamburg.de>.

- *Handbook on European data protection law* [2018].

Horgan-Jones J, (2020). 'Data commissioner starts investigations into Google and Tinder' *The Irish Times* <www.irishtimes.com/>.

Houser K A and Voss W G, (2018). 'GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy' 25(1) RJLT.

Information Commissioner's Office, (2019). 'Intention to fine British Airways £183.39m under GDPR for data breach'

- 'Intention to fine Marriott International, Inc. £99 million under GDPR for data breach' (09 July 2019).
- 'ICO fines British Airways £20m for data breach affecting more than 400.000 customers' (16 October 2020).
- 'ICO fines Marriott International Inc £18.4 million for failing to keep customers' personal data secure' (30 October 2020).

Information Commissioner's Office, 'Regulatory Action Policy' [2018].

International Association of Privacy Professionals, 'GDPR One Year Anniversary – Infographic' <iapp.org>.

Ireland Data Protection Commission, (2020). 'Data Protection Commission statement on funding in 2021 Budget' <www.dataprotection.ie>.

Kobie N, (2020). 'Germany says GDPR could collapse as Ireland dallies on big fines' (Wired) <www.wired.co.uk>.

Leuthner C and Schonhofen S, (2019). 'Calculation of Administrative Fines under GDPR – Standardized Concept Published in Germany' (Mondaq)

Lillington K, (2020) 'Coronavirus: Contact tracing app raises privacy concerns' *The Irish Times* <www.irishtimes.com>.

Maxwell W and Gateau C, (2019). 'A point for setting administrative fines under the GDPR' 16 RJSP.

McLaughlin S, (2018) 'Ireland: A Brief Overview of the Implementation of the GDPR' 4(2) EDPL.

Monteiro A M, (2019). 'First GDPR fine in Portugal issued against hospital for three violations' (IAPP) <iapp.org>.

Murray A, *Information Technology Law* (4th edn, Oxford University Press 2019).

Nemitz P, 'Fines under the GDPR' [2017] CPDP Conference Book.

O'Dell E, (2020). 'Data Protection Remedies, Fines & Damages' (Trinity College Dublin 2019-2020 Data Protection: Law, Policy and Practice)

Office of the Information and Data Protection Commissioner, (2019) 'Lands Authority Personal Data Breach' <idpc.org.mt>.

Pila J and Torremans P, (2019). *European Intellectual Property Law* (2nd edn, Oxford University Press)

Purtova N, (2018). 'The law of everything. Broad concept of personal data and future of EU data protection law' 10(1) LIT.

Ram A and Khan M, (2019). 'France fines Google €50m in test for EU's new data laws' (Financial Times) <www.ft.com>.

Regulation 2016/679 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 [2016] OJ L 119.

Ritzer C and Filkina N, 'First multi-million GDPR fine in Germany: €14.5 million for not having a proper data retention schedule in place' (the Data Protection Report, 12 November 2019) <www.dataprotectionreport.com>.

- 'German Court cuts multimillion GDPR fine by 90%' (the Data Protection Report, 17 November 2020) <www.dataprotectionreport.com>.

Scally D, 'German regulatory says Irish data protection commission is being overwhelmed' *The Irish Times* (3 February 2020) <www.irishtimes.com>.

Schröder et al., 'Have EU Employees? Beware: H&M Slapped with Massive GDPR Fine for Wrongful Processing of Employee Data, Despite Cooperation' (Orrick, 1 October 2020) <blogs.orrick.com>.

Steenbruggen W and others, 'Dutch regulator publishes guidelines for the calculation of administrative fines under the GDPR' (Bird & Bird, April 2019) <www.twobirds.com>.

Taylor C, 'Data Protection Commission disappointed at budget allocation' *The Irish Times* (9 October 2019) <www.irishtimes.com>.

Tinnefeld C and Hanssen H, 'German Court Drastically Reduces GDPR Fine' (Lexology, 17 November 2020) <www.lexology.com>.

Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306.

Vinocur N, (2019). 'One country blocks the world on data privacy' (Politico) <www.politico.eu>.

- 'We have a huge problem: European regulator despairs over lack of enforcement' (Politico) <www.politico.eu>.