

DOI 10.5817/MUJLT2022-2-3

DATA PROTECTION HAS ENTERED THE CHAT: ANALYSIS OF GDPR FINES¹

by

NIMRÓD MIKE*

Before the adoption of the EU-GDPR, researchers remarkably argued on law enforcement of personal data protection being „toothless” and a “paper tiger”. Almost three years after its enforcement date, the GDPR fines are increasing, and the world is beginning to witness the effect of sizeable fines awarded to organizations. This analysis aims to discover potential correlations between GDPR fines, and equally the lack of them. Such correlations might help to tap into trends that are followed by Data Protection Authorities (DPA) in their fining practices. This paper specifically describes the fines issued by the Romanian DPA, while also containing qualitative research findings extracted from discussions with interview subjects. The aim of this paper is to evaluate the possibility to construct a prediction model that is based on linear regression analysis and provide for future direction on the field of legal data analysis.

KEY WORDS

GDPR fines, data analytics, R-programming, fine calculation

1. INTRODUCTION

Data protection law has a long history in Europe, but it appears to have come to the attention of the individual from 25th of May 2018, when the EU-GDPR² (GDPR) replaced its predecessor, the Directive 95/46/EC³ (DPD). Although the DPD laid down much of the legal groundwork for EU-wide data protection, its national adaptations, legal interpretations, and

¹ The present publication is the outcome of the project „From Talent to Young Researcher project aimed at activities supporting the research career model in higher education”, identifier EFOP-3.6.3-VEKOP-16-2017-00007 co-supported by the European Union, Hungary and the European Social Fund.

* E-mail: nimrod.mike@uni-corvinus.hu, Assistant lecturer, Corvinus University of Budapest, Institute of Information Technology, Hungary.

enforcement varied across both the member states and different EU institutions⁴. With massive differences resulting between member states⁵, the academia simply called it a “paper tiger”⁶. Hence the law of the land for Europe became a regulation.

According to Blutman, a regulation has general application, is binding in his entirety and directly applicable in all European Union countries⁷. A regulation is then a stronger means to provide legislative harmonization across member states of EU. The shift from directive to regulation was necessary due to the rapidly changing environment surrounding the processing of personal data. Technological advance and massive industrial research and development are translating into newer means of processing. Many concerns were raised towards the excessive processing of personal data with the introduction of the new technologies, such as Web 2.0 services⁸, Cloud-computing⁹, Smart cards¹⁰ and others. These methods heavily rely on customer’s personal contribution since the core

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union* (L 119, 4.5.2016, p. 1–88). Available from: <https://eur-lex.europa.eu/eli/reg/2016/679> [Accessed 4 February 2021].

³ Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal of the European Union* (L281, 23/11/1995 P. 0031 – 0050). Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046> [Accessed 4 February 2021].

⁴ Ruohonen J. and Hjerpe K. (2020) The {GDPR} enforcement fines at glance, *Information Systems* 106, p.1. Available from <http://ceur-ws.org/Vol-2690/COUrT-paper1.pdf> [Accessed 5 February 2021].

⁵ Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from <https://www.jipitec.eu/issues/jipitec-8-1-2017/4533> [Accessed 10 February 2021].

⁶ Ruohonen J. and Hjerpe K. (2020) The {GDPR} enforcement fines at glance, *Information Systems* 106, p.1. Available from <http://ceur-ws.org/Vol-2690/COUrT-paper1.pdf> [Accessed 5 February 2021].

⁷ Blutman, L. (2014), *Az Európai Unió joga a gyakorlatban*, Budapest, HVG-ORAC, p.158.

⁸ Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. Web 2.0 refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information. Over time Web 2.0 has been used more as a marketing term than a computer-science-based term. Blogs, wikis, and Web services are all seen as components of Web 2.0.

⁹ Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to manage applications. In cloud computing, the word cloud (also phrased as “the cloud”) is used as a metaphor for “*the Internet*,” so the phrase *cloud computing* means “a type of Internet-based computing,” where different services – such as servers, storage, and applications – are delivered to an organization’s computers and devices through the Internet.

of the software is based on the mutual trust between the service provider and the user. As consumers were increasingly concerned about breaches of privacy, loss of trust was translated into lost opportunities and revenue for companies. Recent high profile data breaches have pushed consumers change service providers who did not adequately protect personal data. The high-profile data breaches are also the motivation behind growing monetary penalties¹¹. However, it is necessary to separate infringement cases based on the quoted articles by the DPAs as not all penalties are results of personal data breaches¹².

GDPR fines are increasing, and the world is witnessing the effect of sizeable fines awarded to organizations. Golla argues that Data Protection Authorities (DPAs) should grow teeth by issuing more significant monetary sanctions¹³. He also emphasized that there were big differences in the maximum amounts of administrative fines between the different member states in the pre-GDPR era¹⁴. While Romanian Law (maximum circa €11,000) and Slovenian Law (€12,510) allowed for relatively low fines, Spanish (€600,000) and UK Laws (£500,000) had much higher thresholds¹⁵. Indeed law enforcement of personal data protection was deemed to be „toothless“¹⁶.

This analysis aims to discover potential correlations between GDPR fines and the lack of them. The correlations might help to tap into trends that are followed by DPAs in their fining practice. This paper specifically describes the fines issued by the Romanian DPA. The main question imposed herein

¹⁰ A small electronic device about the size of a credit card that contains electronic memory and an embedded integrated circuit (IC). Smart cards containing an IC are sometimes called *Integrated Circuit Cards (ICCs)*. Smart cards are used for a variety of purposes, including storing a patient's medical records; storing digital cash; generating network IDs (similar to a token).

¹¹ At the moment of writing the highest amount has been given to Alphabet Inc. by the French DPA. Available at: <https://www.enforcementtracker.com/ETid-23> [Accessed 13 February 2021]

¹² Article 4. para (12) of GDPR provides that 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

¹³ Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from <https://www.jipitec.eu/issues/jipitec-8-1-2017/4533> [Accessed 10 February 2021].

¹⁴ Ibid.

¹⁵ Ibid.

¹⁶ Albrecht, J. P. (2016), Privacy enforcement in search of its base, In: David Wright and Paul De Hert (eds) *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer International Publishing, p. 47.

is that with the adoption of GDPR can we expect bigger fines or more frequent ones for data protection violations?

In this study both quantitative and qualitative research methods are used to answer the research question framed above. To evaluate the trends in fine setting, the workings of various DPAs are studied. Fine calculation models that have been published by the DPAs are an important part of this discovery process. Further, custom models framed by practitioners are also relatable, thus included in the analysis. The novel approach in qualitative research is the application of supervised machine-learning on a constructed dataset¹⁷. Through supervised machine learning the algorithms may discover variables¹⁸ that play a significant role in determining the administrative fine. Using the dataset, we construct three different types of trained regression algorithms (models) in R programming language. The models deployed in the analysis are based on techniques of regression tree¹⁹, random forest²⁰ and linear regression²¹.

This examination will potentially provide more transparency and offer insights on the profile of companies that are more exposed to such legal risks as receiving a fine for violating GDPR provisions. To the same extent, it may offer conclusions underlining total randomization and selective arbitration in this respect. Nonetheless, the research ideally will explain how existing guidelines on fine setting can impact the practice of DPAs.

The structure of the paper is as follows: the introduction in Section 1 serves the reader with general and wide overview about the topic itself. The introduction is followed by Section 2, where the aim is the presentation

¹⁷ The primary source for data collection is the GDPR Enforcement Tracker maintained by CMS law (www.enforcementtracker.com). The selection criteria for constructing the dataset is described in detail at Section 4.1.

¹⁸ As a key action within the dataset preparation, we develop additional attributes expressed as variables. These variables are tied to the business metrics of the companies that received an administrative fine for GDPR infringements. The variable glossary is presented in Section 4.1 and Section 4.5.1 accordingly.

¹⁹ UC Business Analytics R Programming Guide (2018) *Regression Trees*. [online]. Available from: http://uc-r.github.io/regression_trees [Accessed 5 March 2021]. Basic regression trees partition a data set into smaller groups and then fit a simple model (constant) for each subgroup.

²⁰ UC Business Analytics R Programming Guide (2018) *Random Forests*. [online]. Available from: http://uc-r.github.io/random_forests [Accessed 5 March 2021]. Random forests are responsible for building a large collection of de-correlated regression trees. Usually these have a good predictive performance.

²¹ UC Business Analytics R Programming Guide (2018) *Linear Regression*. [online]. Available from: http://uc-r.github.io/linear_regression [Accessed 5 March 2021]. Linear regression is a useful tool for predicting a quantitative response and it is a widely used statistical learning method.

of principles established by the European Data Protection Board (EDPB) in their Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679²². Section 3 provides on existing calculation models proposed by DPAs. Section 4 presents a possible new approach to predict GDPR fines supported by data analytics applying a linear regression model constructed in R programming language. Section 4 also elaborates on the case study of the administrative fines issued by the Romanian DPA. The model is presented to understand how fines are applied. Section 5 finally delivers the conclusion, limitations, and future work.

2. PRINCIPLES OF SETTINGS FINES

From a thorough reading of the EDPB Guidelines²³ four main principles can be extracted to the application of administrative fines. Table 1 summarizes the principles.

	Name	Summary
P1	Equivalent sanctions	Infringement of the Regulation should lead to the imposition of equivalent sanctions.
P2	Effective, proportionate, and dissuasive fines	As with all corrective measures chosen by the DPAs, administrative fines should be effective, proportionate, and dissuasive.
P3	Case-by-case assessment	The competent supervisory authority will make an assessment in each individual case.
P4	Active participation of DPAs	A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among DPAs.

Table 1. Principles of fines applied by DPAs

One might consider that the role of DPAs are only to issue fines, although, the powers vested in DPAs are far more reaching than the implementation of fines. The tasks of DPAs as per Art. 58 of GDPR provide a wide array

²² Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], pp. 1-17.

²³ *Op. cit.*, p.5.

of responsibilities. Figure 1 presents the typology of powers sitting with the DPAs.

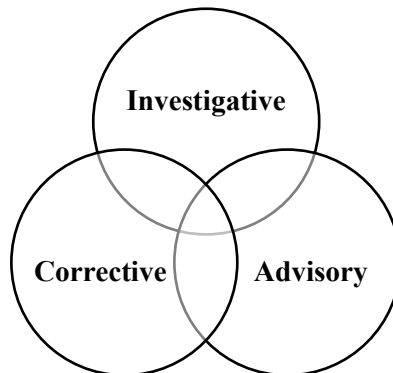


Figure 1. Powers of DPAs based on Art 58 GDPR.

Further, the EDPB Guidelines provide that the DPAs must identify the most appropriate corrective measures to address GDPR infringements. Figure 2 presents the corrective measures categories currently recognized.

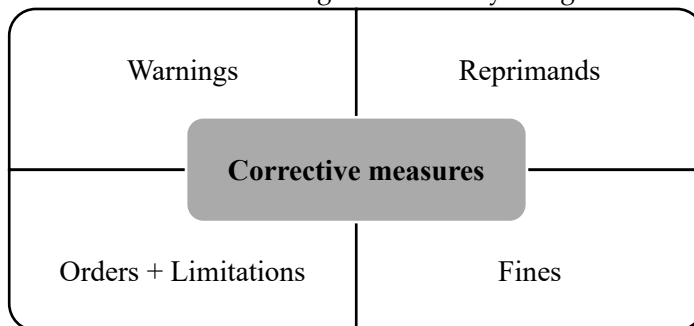


Figure 2. Categories of corrective measures

Based on Art. 58 (2) a) warnings are typically issued to a controller or processor if the intended processing operations are likely to infringe provisions of GDPR. The DPAs shall issue reprimands to a controller

or a processor where processing operations have infringed provisions of GDPR, but the infringement consists of “minor infringements”.²⁴

Orders as corrective measures can be of multiple types:

- The DPA may order the controller or processor to comply with data subject requests (DSRs) [art. 58 (2) c)];
- to bring processing operations into compliance with GDPR provisions in a specified manner and within a specified period [art. 58 (2) d)];
- to communicate a personal data breach to the data subject(s) [art. 58 (2) e)];
- to limit temporarily or permanently the processing [art. 58 (2) f)];
- to rectify, delete or restrict the processing of personal data and to notify recipients of such personal data pursuant to Art. 17 (2) and Art. 19 [art. 58 (2) g)];
- to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 [art. 58 (2) h)];
- and finally, to order the suspension of data flows to recipient in a third country or to an international organization [art. 58 (2) j)].

In addition, the DPAs can provide administrative fines, depending on the circumstances of each individual case [art. 58 (2) i)].

2.1 EQUIVALENT SANCTIONS

Recital (10) of GDPR calls for equivalent level of protection of personal data in Member States. The motivation behind enshrining that sanctions are equivalent are also further debated in Recitals (11) and (13). This provision is backed up by S. Golla²⁵. Throughout this equivalency EDPB also stresses that the GDPR calls for a greater consistency than the DPD when imposing sanctions²⁶. The principle to be followed is to prevent different corrective

²⁴ Recital 148 introduces the notion of “minor infringements”. Such infringements may constitute breaches of one or several of the Regulation’s provisions listed in article 83 (4) or (5). The assessment of the criteria in article 83 (2) may however lead the supervisory authority to believe that in the concrete circumstances of the case, the breach for example, 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. In such cases, the fine may (but not always) be replaced by a reprimand. *Op. cit.*, p. 9.

²⁵ Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from <https://www.jipitec.eu/issues/jipitec-8-1-2017/4533> [Accessed 10 February 2021].

measures being chosen by the DPAs in similar cases²⁷. C. Barrett further argues that P1 encourages DPAs to apply a consistent approach in their “use of corrective powers,” including the application of administrative fines in particular²⁸.

Practitioners denote that the principle of equivalence can also be found in the case law of the European Court of Justice (CJEU), even though its meaning is not exactly the same as that determined by the EDPB²⁹. Indeed, as the CJEU case law indicates this should mean the sanctions to violations of national law are the same as to sanctions applied by EU law³⁰. It is really important to highlight what Maxwell and Gateu are accurately pointing out on this principle: it demands the non-discrimination in the application of sanctions³¹. Non-discrimination is of utmost importance to ensure legal certainty. Regarding the scope of this paper, such obligation of non-discrimination also serves to determine why GDPR fines may be predictable.

No one would go on record saying that privacy cannot be monetized. To the same extent there is a good chance no one would dare to say that GDPR infringements cannot be translated into economic values. The mere fact that it is difficult does not mean it is impossible. S. Greengard says that it is certain, amid a litany of security breaches and breakdowns, from Equifax (2017) to Cambridge Analytica (2018), there is a growing focus on data privacy³². Frischmann in the same article further denotes that GDPR, more than anything else, represents the ongoing battle between unfettered

²⁶ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 5.

²⁷ Ibid.

²⁸ Barrett, C. (2020) Emerging Trends from the First Year of EU GDPR Enforcement, *ABA – American Bar Association Data, Spring 2020* 16 (3). Available from https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/spring/emerging-trends-the-first-year-eu-gdpr-enforcement/#25 [Accessed 25 January 2021].

²⁹ Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under the GDPR, [online]. Available from: <https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr> [Accessed 20 January 2021], p. 103.

³⁰ *Op. cit.*, p. 104.

³¹ *Op. cit.*, p. 105.

³² Greengard, S. (2018) Weighing the impact of GDPR, *Communications of the ACM* 61 (11), p. 17.

capitalism and human dignity and that the whole point of it is that it is not designed to be an efficient regulation for businesses³³.

2.2 EFFECTIVE, PROPORTIONATE, AND DISSUASIVE FINES

To best assess if a fine may fulfil the requirements of P2, a case-by-case examination is crucial. The EDPG Guidelines hint towards three possible objectives pursued by the corrective measures chosen, that is:

- re-establishing the compliance with rules,
- punish unlawful behaviour,
- or a combination of the two³⁴.

According to Maxwell – Gateu³⁵:

"Effectiveness" means that national law should not render the enforcement of EU law virtually impossible³⁶. Effectiveness also includes the principle of equivalence and non-discrimination as regards comparable violations of national law³⁷.

"Proportionality" means that sanctions should not exceed what is appropriate and necessary to attain the objective legitimately sought by the legislation, and that when there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued³⁸.

"Dissuasiveness" means that the application of the penalty must result in the party having violated the law being substantially worse off than would be the case if he complied with the law. This requires, at a minimum, that

³³ *Op cit*, p. 18.

³⁴ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 01 February 2021], p.6.

³⁵ Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under the GDPR, [online]. Available from: <https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr> [Accessed 20 January 2021], pp. 103-104.

³⁶ Judgement of Comet BV v Produktschap voor Siergewassen, Case C-45/76, ECLI:EU:C:1976:191, paragraph 16.

³⁷ *Ibid*.

³⁸ Judgement of Ute Reindle v. Bezirkshauptmannschaft Innsbruck, C- 443/13, ECLI:EU:C:2014:2370, paragraph 39.

*the penalty be sufficiently high so that the guilty party loses any benefit that arose because of its illegal behaviour*³⁹.”

According to EDPB, a more precise determination of P2, will result from the emerging practices of DPAs and CJEU case-law overtime⁴⁰. The reason behind not citing the CJEU case-law, might be that the EDPB does not wish to limit the potential of DPAs forming new trends in applications of fines. The potential to apply incentives to controllers and processors is given to the DPAs. The GDPR calls for a wide range of corrective measures, the thresholds of administrative fines being raised significantly.

The EDPB Guidelines are also putting an end to a discussion on the subject matter of what should be considered an ‘undertaking’ in the light of GDPR. Concerns were raised towards that several language versions of use an identical term for what is described as an “undertaking” in Article 83 GDPR and as an “enterprise” Article 4 (18) GDPR (English version)⁴¹. Recital (150) refers to Art. 101 and 102 TFEU⁴². The undertaking means an economic unit, which may be formed by the parent company and all involved subsidiaries (i.e. an entire corporate group will be considered an undertaking). The CJEU case law definition also confirms that the concept of an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed⁴³. In another case the definition says that an undertaking must be understood as designating an economic unit even if in law that economic unit consists of several persons, natural or legal⁴⁴.

³⁹ Judgement of LCL Le Crédit Lyonnais v. Fesih Kalhan, Case C- 565/12, ECLI:EU:C:2014:190, paragraph 51.

⁴⁰ Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 6.

⁴¹ Golla, S. (2017) Is Data Protection Law Growing Teeth? Current Lack of Sanctions in Data Protection Law and Administrative Fines under GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from <https://www.jipitec.eu/issues/jipitec-8-1-2017/4533> [Accessed 10 February 2021].

⁴² Consolidated versions of Treaty on European Union and Treaty on Functioning of European Union - Consolidated version of Treaty on Functioning of European Union - Protocols - Annexes - Declarations annexed to Final Act of Intergovernmental Conference which adopted Treaty of Lisbon, signed on 13 December 2007 - Tables of equivalences. *Official Journal of European Union* (C 326, 26/10/2012 P. 0001 – 0390). Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT> [Accessed 22 January 2021].

⁴³ Judgement of Höfner and Elser v Macrotron GmbH, Case C-41/90, ECLI:EU:C:1991:161, paragraph 21.

⁴⁴ Judgement of Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española de Petróleos SA, Case C-217/05, ECLI:EU:C:2006:784, paragraph 40.

2.3 CASE-BY-CASE ASSESSMENT

P3 is a direct consequence of the requirements set out in P2. For the corrective measures to take effect, be proportionate and dissuasive, these have to be customized based on the particularities of the case. Tailoring can be done based on aggravating and mitigation factors. The baseline is Art. 83 (2) of GDPR for such assessments. Indeed, fines are important tool that DPAs should use in appropriate circumstances, and these should not be qualified as last resort, nor to shy away from their use⁴⁵. Yet, if the fines are used too often or being excessive in their nature, it would seriously undermine their legitimacy. The DPAs are not meant to be bloodthirsty. Their powers are advisory, not only corrective. Thus, the DPAs are put to a test of conflict management.

2.4 ACTIVE PARTICIPATION OF DPAS

This last principle is just the endorsement of the consistency mechanism desired by the GDPR. With the progressive tendencies of GDPR fines, DPAs should have active information exchange hard coded in their activities. To effectively learn from each other, DPAs should participate to regular workshops⁴⁶.

Acknowledging that some national DPAs are younger than others, they might lack experience in organization and procedures. The cure to this and the application of consistency is that DPAs in a more mature state are stepping in to function as a role-model. The question arises, whether this would threaten the independency of each DPA. The answer is most probably not – DPAs should be conscious about their legal status and identify themselves as independent authorities, however teamwork should characterize their work.

The EU reform on personal data protection provides a strong template. This template needs to be applied consistently across the EU. Consequently, personal data should be exchanged freely between member states of EU. If there is one standard of protection, internal boundaries will not find their place anymore. Same applies to enforcement of GDPR infringements. The DPAs have now the mission to coordinate their activities

⁴⁵ Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 7.

⁴⁶ *Op. cit.*, p. 8.

at a previously untested level. There might be a strong opposition in the corporate arena⁴⁷, but the DPAs should stand their ground firmly. The EDPB is also entrusted with issuing binding decisions based on Art. 65 of GDPR on disputes arising between DPAs relating to the determination of the existence of an infringement⁴⁸. The first decision to be issued concerned a draft decision of the Irish DPA on Twitter International Company.

2.5 CRITERIA FRAMEWORK FOR P1-P4

The way DPA administer fines is based on the objective evaluation of the facts. The evaluation procedure consists of three basic steps presented in Figure 3.

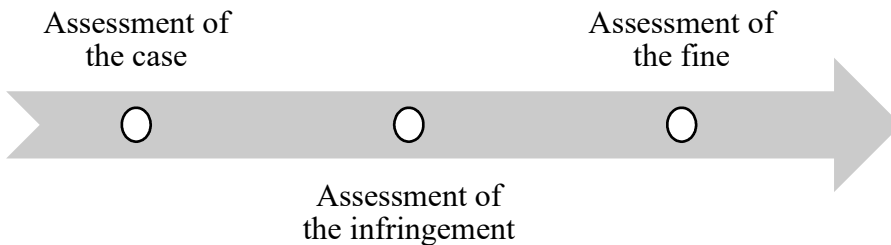


Figure 3. Evaluation procedure: three steps to determine the fines.

In the first step the facts of the case are investigated by the DPA. The aim of this step is to understand and determine more precisely what has happened. The second step leads to the assessment of whether there has been an infringement of the provisions. Any unlawful behaviour of a controller or processor is established in this step. The third step determines the level of fine. Preliminary to this, in the second step the type of corrective measure will be selected. Step three only applies if the corrective measure is an administrative fine. If warnings and reprimands are issued there is no need for the DPA to follow-up with step three. This conclusion is endorsed by the GDPR in Recital (148) and by the EDPB⁴⁹.

⁴⁷ Greengard, S. (2018) Weighing impact of GDPR, *Communications of ACM* 61 (11), p. 17.

⁴⁸ Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p.7.

Following the completion of the first two steps, the DPAs will follow-up with the third step and determine the level of fine. Step three has a high degree of complexity and subjectivity. It is the heart of both P2 and P3. Accordingly, if the factual analysis (step 1) has prompted there has been a conflict between the behaviour of controller or processor with the legislative background, and the legal analysis (step 2) provides proof of infringement deserving an administrative fine, the amount is calculated based on eleven factors. These are discussed in sections 2.5.1. – 2.5.11.

2.5.1 NATURE, GRAVITY, AND DURATION

Embracing the GDPR spirit, all the obligations incumbent on controllers and processors are categorized according to their nature in Art. 83 (4) – (6). The nature of infringement is a result of such classification. The EDPB Guidelines are pointing towards the fact that Recital (148) opens the possibility for DPAs to issue reprimands instead of fines⁵⁰. An example of this would be if the data controller is a natural person and the fine would constitute a disproportionate burden⁵¹. Here the reader may witness the evaluation procedure referenced under Figure 3. Hence, the DPAs are poised to perform case-by-case evaluations. The competent DPA during its investigation process will assess if a fine is necessary as a corrective measure. In many cases the DPAs will decide against a fine for this reason.

How gravity may be assessed is left to the discretionary power of DPAs to decide. In fact, the EDPB Guidelines provide that⁵²:

“The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement.”

Yet the duration of infringement may be illustrative of the three scenarios provided by EDP as example, it is not always obvious and easy to determine the duration of the infringement. This is especially true in cases of personal data breaches due to cybersecurity threats. The personal

⁴⁹ Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 9.

⁵⁰ Ibid.

⁵¹ Ibid.

⁵² *Op cit*, p. 10.

data breaches are one of the gravest infringements of GDPR, compared to the lack of Data Protection Officer's (DPO) contact details in the information notice. Personal data breaches are responsible for most damages suffered by data subjects and often involve the highest number of impacted data subjects. It is a top priority for organizations to evaluate and understand the source of the personal data breaches. It could be a challenge to recognize these, however there are numerous examples provided by both academia and practice. Once recognized, the root-cause for personal data breaches should be determined. There is a need to understand the causal link between a certain human error, a process, a procedure or an entire policy and the personal data breach itself. Once the root-cause analysis provides its results, competent key-personnel should conduct the treatment plan to mitigate the negative effects of personal data breaches.

Due to the argument presented above, DPAs should investigate the number of data subjects involved, the purpose of the processing and the compatible use⁵³ and if the data subjects have suffered damage⁵⁴.

2.5.2 INTENTIONAL OR NEGLIGENT CHARACTER

The EDPB Guidelines provide examples of both intentional breaches and infringements resulting from negligence⁵⁵. The GDPR highlights, and endorsed by interview subjects, that all data processing routines are following a risk-based approach. This approach requires constant evaluation, measuring, adaption and performance review. It is an infinite loop meant to be interpreted as an obligation of goal rather than an obligation of mean. Thus, neither controllers nor processors are permitted to legitimize infringements due to lack of resources or a simple failure to efficiently apply internal policies.

In practice organizations often avoid responsibilities due to the general perception that internal policies are only formal documents. Reality cannot be farther from that. The policies adopted in any organization serve

⁵³ Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, (WP 203, 00569/13/EN) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 2 February 2021].

⁵⁴ Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], pp. 9-11.

⁵⁵ *Op. cit.*, p. 12.

the purpose to lead the way or to pave the corridors of a law-abiding behaviour. Policies can often get complicated, but the solution is to enact a “policy task force”, which has its primary goal to translate it into everyday practice. Policies, i.e. documents regulating data processing activities, shall not be reactive, but proactive instead. This conclusion is supported by the idea that it is better to treat the disease not just the symptoms.

2.5.3 ACTIONS OF CONTROLLER OR PROCESSOR

There is no bulletproof system or organization. Data breaches will occur. It is not a matter of a condition, but rather of time. Controllers and processors have clear responsibilities to implement measures ensuring data security. The EDPB provides that⁵⁶:

“However, when a breach occurs and the data subject has suffered damage, the responsible party should do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned. Such responsible behaviour (or the lack of it) would be taken into account by the DPAs in their choice of corrective measure(s) as well as in the calculation of the sanction to be imposed in the specific case.”

Organizations shall find actions that are suitable to provide proof of good-faith collaboration with other entities in case of infringements. Actions include reaching out to other entities involved in the data-sharing ecosystem or even restricting and blocking access to data.

2.5.4 DEGREE OF RESPONSIBILITY

This criterion from the entire framework set by Art. 83 (2) is probably the most subjective one. Just by simply reading it from the legislative text will not shed light on its practical relevance. The reference to Art. 25 and 32 of GDPR is reiterating the above presented remark that it is about the risk-assessment. Organizations are expected to have clear methodology on how to identify and assess risks. The degree of responsibility may be measured by a verification of existing documentation that was incumbent on the controller. Further, even the documentation might not suffice, if it is not followed by implementation of measures.

The EDPB Guidelines are calling for “appropriate conclusions”⁵⁷. The DPAs will assess when the degree of responsibility has to be

⁵⁶ Ibid.

⁵⁷ *Op. cit.*, p.13.

established if the controller acted based on the appropriate conclusions. Remarkably, the words “degree of” could have been deleted from the original text due to its capability to enlarge the “grey area”. To what degree are one controller’s assessments and measures good enough, or even compliant enough, has its own relativity. If the authority is entitled to establish the degree by itself, it has huge implications. In practical terms this means that a DPA might say that a controller’s compliance efforts are not good enough and issue an administrative fine. This can lead to a depressing pressure on businesses, as budget allocations might differ from one another, as well as the place of compliance matters in the priority list.

2.5.5 PREVIOUS INFRINGEMENTS

The DPAs will keep a track record of the controller or processor committing the infringement. There is a clear intention to consider recidivism as an aggravating factor⁵⁸. According to the EDPB Guidelines, the DPAs should assess if the controller or processor has committed the same infringement before; or if the controller or processor has committed an infringement of the Regulation in the same manner⁵⁹.

Committing the same infringement should indicate a heavier corrective measure or higher fine. Controllers or processors receiving any corrective measure from a DPA should take its implementation seriously and with utmost importance. If the same incident should happen again, it would be hard to efficiently argue against the setting of an administrative fine. On the other hand, the DPAs might incur difficulty in reaching the controller or processor. Inability to cooperate is left to be a separate benchmark in this criteria framework. However, if this is the case, a question would arise as to whether insufficient cooperation would consist of a first infringement? The utility of the question comes into discussion because in such a scenario these criteria would be fulfilled in one time. However, this interpretation is *de facto* detrimentally towards the controllers and processors. It would assume a recidivism by default

⁵⁸ Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under GDPR, [online]. Available from: <https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr> [Accessed 20.01.2021], p. 108.

⁵⁹ Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 14.

in case a controller or processor is not willing to answer to notices received from DPAs. In exchange, the insufficient cooperation would definitely constitute an aggravating factor for any “first-timer” offenders.

2.5.6 COOPERATION WITH DPAS

This criterion emphasizes the procedural part of the entire investigation process around an infringement. The DPA will engage in a dialogue with the offender in order to better understand the circumstances of the situation. A high degree of cooperation would mean that throughout the entire investigation process the controller or processor is providing clear, accurate and transparent information. It does not seek to shy away from the retaliation it might face from the DPAs, nor does alter or modify results of its assessments in such a way to bend the reality in its favour. The EDPB Guidelines are claiming the cooperation obligation to be „due regard” and arguing that it does not include any cooperation that is already required by the law (e.g. allowing access to the controllers’ premises to carry out audits or inspections)⁶⁰.

2.5.7 CATEGORIES OF PERSONAL DATA AFFECTED

This criterion is related to the type of personal data that was affected by the infringement. The GDPR recognizes three major categories of personal data:

2.5.7.1 PERSONAL DATA

The DPD, the ancestor of GDPR, never intended to apply to all kinds of data. Most probably the intention was to exclude anonymized data⁶¹ from the regulation, as this could be construed as contrary to its scope, *i.e. to offer protection only for data which can be related to a person*⁶².

In 2007 the Article 29 Working Party, established under Article 20 of DPD, produced an opinion on the concept of 'personal data' to provide guidance contributing to the uniform application of data protection rules

⁶⁰ Ibid.

⁶¹ Ohm, P. (2010) Broken Promises of Privacy: Responding to Surprising Failure of Anonymization, *UCLA Law Review* Vol. 57. Available from <https://ssrn.com/abstract=1450006>. [Accessed 11 February 2021], p. 1738.

⁶² The Article 4 Par. (5) of GDPR, clarifies the aspect in question by stating that pseudonymization’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. From the wording of Recital (28) and (78) it should be concluded that pseudonymization is encouraged by the GDPR.

across the EU. There were some important points, which should be noted since it was proposed not to fall victim of 'unduly restriction' of interpretation of personal data definition. What might have been interpreted as an over-broad application of the DPD, resulting from wide interpretation of the definition, should be balanced out by using the flexibility allowed in the time actual application of the DPD's rules.

Perhaps, EU lawmakers wanted to strike a balance through the power of technology and escalating digitalization, but all that has failed earlier than everybody expected. For this reason, a new set of rules is taking place from the next year, and reform is happening at this moment in the field of data protection. *For example, in case of IP addresses*, there was a significant divergence on the level of national regulations. The Commission's Impact assessment results prove that there have been serious differences on this topic in the recent past. For instance, only a few Member States have taken a clear regulatory approach assessing the status of IP addresses. Austria considered IP addresses as being personal data in the Austrian Security Policy Act. Laws in Cyprus, Italy and Luxembourg suggested the same, but within the context of electronic communications. According to the Bulgarian and Estonian Electronic Communications Acts, only a combined set of data which includes IP addresses constituted, as a whole, personal data⁶³. Some of the Member States took the view that the processing of IP addresses does not fall within the scope of legislation implementing the Directive, as long as the addresses themselves are not linked to individuals or to PCs of individuals (e.g. Belgium, UK)⁶⁴. The national laws of Denmark, France, Germany, Hungary, Latvia, Lithuania, Netherlands, Poland, and Spain highlighted the fact that in case where re-identification of users is possible with processing data, those data shall be considered as being personal data⁶⁵. This is the case of IP addresses

⁶³ Commission Staff Working Paper of 25 January 2012, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data of. *European Commission* (SEC (2012) 73 final). Available from https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf, [Accessed 11 February 2021], p. 14.

⁶⁴ *Ibid.*

⁶⁵ *Op cit*, p.7.

too. Besides, Austria was the first to recognise dynamic IP addresses as personal data.

This approach was embraced by the Court of Justice of European Union, regardless if the IP data are static or dynamic⁶⁶. A dynamic IP address changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, by means of files accessible to the public, between a specific computer and the physical connection to the network used by the internet service provider. Therefore, only the internet service provider has the additional information necessary to identify the user. They identify a computer, not the person using it. True. But that is the same as a telephone; just because a call was made from a number does not tell you exactly who was talking⁶⁷. And should there be a difference between the nature of an IP address and a telephone number? Probably most of the people believe their phone number is quite personal, whereas the same level of personality and/or confidentiality shall apply to an IP address too.

In this regard, the answering to the question raised by the *Bundesgerichtshof* (Federal Court of Justice, Germany), the Court of Justice of the European Union states: 'that a dynamic IP address registered by an 'online media services provider' (that is by the operator of a website, in the present case the German Federal institutions) when its website, which is accessible to the public, is consulted, constitutes personal data with respect to the operator if it has the legal means enabling it to identify the visitor with the help of additional information which that visitor's internet service provider has⁶⁸.

Moreover, by its case-law, European Union's Court of Justice will introduce new categories, while in the fast phased modernizing society it is almost a certain fact that new types of data through which an individual could be identified will appear in a relative short period of time. Hopefully, competent bodies will decide upon this, and more than that, the informational society is ready to face technical innovations on every

⁶⁶ Judgement of Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779, paragraph 16.

⁶⁷ Hansell, S. (2008), *Europe: Your I.P. Address Is Personal.*, [blog entry], 22 January 2008, BITS. Available from: <https://bits.blogs.nytimes.com/2008/01/22/europe-your-ip-address-is-personal/> [Accessed 17 January 2021].

⁶⁸ Judgement of Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779, paragraph 49.

level. These regulations will not be adopted as slowly as it was the ongoing situation regarding the DPD.

In addition, it can be deduced, that this new tendency to sort more categories as personal data, suggests the fact that the concept cannot be treated as a strictly and promptly defined term. With the passage of time, it is very possible, if not doubtless, that the concept of personal data will be enriched with additional terms, expanding the applicability of GDPR and other acts on wider area.

Another interesting novelty is the manner in which processing can be conducted according to the GDPR, *i.e.* by structuring data. Data structuring, in essence, has to do with a system where seemingly random, unstructured data can be taken as input and a number of operations executed on it linearly or non-linearly. These operations are meant to analyse the nature of the data and its importance in the larger scheme of things. This is specifically referring to the concept of Big Data, which means extremely large data sets that may be analysed computationally in order to reveal business trends, patterns, correlations related to human behaviour through analysis of both personal and non-personal data collected from the users. As mentioned by the doctrine, the concept of Big Data, understood as a more powerful form of data mining, challenges the privacy laws in several ways, undermining the informed choice of individuals and clashing with data minimization⁶⁹. Among the advantages of Big Data and these modern ways to use some predictive and behavioural analytics, could be mentioned the possibility to prevent diseases, efficiently combat crimes and terrorism, reduce traffic jams, and enforce new technologies in order to boost medical preventions in emergency situations. Shortly, but firmly it can be applied on various fields of life.

To state the obvious, the utility of Big Data is beyond any question, but the manner in which such analytics are being conducted by enterprises, do lead to several infringements upon privacy rights of the individuals. Firstly, given the fact, that businesses are not able to exactly determine what kind of revelations will be revealed from the examination of the data sets, any kind of consent received from the customers should be considered invalid.

⁶⁹ Rubinstein, I. (2012) Big Data: The End of Privacy or a New Beginning? *NYU School of Law, Public Law Research Paper No. 12-56*. Available from <http://dx.doi.org/10.2139/ssrn.2157659> [Accessed 17 December 2020].

Users with average knowledge and limited knowledge on internet protocols and/or privacy policies could be easily tricked into giving their consent to something that they do not understand by default. Moreover, there is no incentive to learn about the procedure which stands behind their consent, which was given by them apparently with the full awareness of all the facts, i.e. an *informed consent*. Thus, when the consent is required for processing, it cannot be stated that the organization assumed an obligation of means to facilitate all possible attempt to achieve a certain result, without committing itself to the result expected. The opposite is correct. The obligation assumed by organizations in this situation shall be classed as an obligation of goal that is to achieve a specific result, *i.e.* not to collect and analyse personal data of the users without an existing prior consent. In actuality, such data sets include enormous quantity of data. In order for businesses to have access to useful material, it is a certainty, that more personal data are being processed about the individuals than it would be necessary. Thus, data minimization is also left behind in order for Big Data analytics to prevail.

2.5.7.2 SENSITIVE DATA

The special categories of personal data are listed in art. 9 (1) of GDPR. There is a general prohibition on the processing of such personal data. The GDPR and member state laws are regulating the exceptional cases when processing is permitted.

2.5.7.3 CRIMINAL DATA

According to art. 10 of GDPR, *processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.* From this provision personal data elements like criminal convictions, criminal offences, background checks can be extracted.

2.5.8 BECOMING AWARE OF THE INFRINGEMENT

The EDPB Guidelines distinguish between five different manners by which a DPA might become aware of an infringement. It can be a result

of investigation, complaints, articles in the press, anonymous tips, or notification by the data controller⁷⁰.

It is certainly noteworthy that notification is a legal obligation of controller and thus it will not translate into a mitigating factor. However, when the DPA has to assess the degree of cooperation with the controller, it will have its own weight. A good conduct by the controller in self-reporting the incident or the infringement towards the DPA can be the difference between applying a reprimand or setting an administrative fine as a corrective measure.

2.5.9 PREVIOUS ORDERS FROM AUTHORITY

In the event previous orders such as corrective measures have been issued by the DPAs with regard to the same subject matter, this criterion comes into play. It is not referring any previous infringements by the controller or processor of any type. Instead, what the DPAs should look at is whether the organization was cautious enough to implement the measures and ensure compliance with these, in case the DPA was to levy penalties of this type on them⁷¹.

2.5.10 CODES OF CONDUCT OR OTHER CERTIFICATIONS

This aspect is widely overlooked in practice. The approved codes of conduct and certification mechanisms are not used to their maximum potential. Yet, the EDPB argues that such a variable should be considered for the fine calculation. More precisely⁷²:

“Where the controller or processor has adhered to an approved code of conduct, the supervisory authority may be satisfied that the code community in charge of administering the code takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code of conduct itself. Therefore, the supervisory authority might consider that such measures are effective, proportionate, or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself. Certain forms of sanctioning non-compliant behaviour may be made through

⁷⁰ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 15.

⁷¹ Ibid.

⁷² Ibid.

the monitoring scheme, according to article 41 (2) c and 42 (4), including suspension or exclusion of the controller or processor concerned from the code community. Nevertheless, the powers of the monitoring body are without prejudice to the tasks and powers of the competent supervisory authority, which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme.”

2.5.11 OTHER FACTORS

The final stage, according to the criteria framework provided by Art. 82 (3) of GDPR, the DPAs may consider 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 infringement⁷³.

Surprisingly, this criterion is at the bottom of the framework list, but in practical terms it has strong importance level. Any organization can take profits from infringements of law. Administrative or penal fines are only issued if the offender is caught. Economic gains cannot be the result of illegitimate conduct. The application of an administrative fine by the DPAs should be logical consequence in case the organization is clearly profiting of the infringement.

3. FINE CALCULATION MODELS

A couple of DPAs already published their own guidelines on setting administrative fines. The message is clear towards controllers and processors: fines are on their way. In this section four calculation models are presented: 3.1 Dutch model; 3.2 British model; 3.3. German model; 3.4. Custom model.

3.1 DUTCH MODEL

On 14 March 2019, the Dutch DPA (*Autoriteit Persoonsgegevens*) has published its own Guidelines on Administrative Fines 2019⁷⁴. The approach implemented by the Dutch DPA is a categorization of GDPR infringements into four categories. Based on Art. 2.3 of the Dutch Guidelines, these are

⁷³ *Op cit*, p. 16.

⁷⁴ Boetebeleidsregels Autoriteit Persoonsgegevens (2019) *Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes* [online] Available from: <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan> [Accessed 14 March 2021].

presented in Table 2. Art. 2.4 further provides that the amount of the basic fine is set at the minimum of the bandwidth plus with half the bandwidth of the fine category associated with a violation.

Category	Fine bandwidth	Standard amount:
Category I.	Fine bandwidth between €0 and €200,000	Basic fine: €100,000
Category II.	Fine bandwidth between €120,000 and €500, 000	Basic fine: €310,000
Category III.	Fine bandwidth between €300,000 and €750, 000	Basic fine: €525,000
Category IV.	Fine bandwidth between €450,000 and €1,000,000	Basic fine: €725,000

Table 2. Categories of fines applied by Dutch DPA.

According to expert practitioners⁷⁵:

“Each category is linked to a specific bandwidth that the Dutch DPA considers to be “appropriate and required”. This means that the fining bandwidth is considered by the Dutch DPA to be proportional on the one hand and sufficiently dissuasive for both the offender (special prevention) and other potential offenders (general prevention) on the other. Within the chosen bandwidth the Dutch DPA has determined a standard penalty which will be the “starting point” for the calculation of the fine.

[...]

In case of a repeat offence the fine will automatically be increased with 50% unless this would be disproportionate in the circumstances of the case. Under the Guidelines there is a repeat offence “when at the time the offence was committed there were not yet five years passed since the imposition of an administrative fine by the Dutch DPA on the offender in respect of the same or a similar offence committed by the offender”. Given this

⁷⁵ Steenbruggen, W. and Van Der Eijk, B. (2019) *Dutch regulator publishes guidelines for the calculation of administrative fines under the GDPR* [online]. Available from: <https://www.twobirds.com/en/insights/2019/netherlands/dutch-regulators-publishes-guidelines-for-the-calculation-of-administrative-fines-under-the-gdpr> [Accessed 15 March 2021].

definition, other measures such as warnings, reprimands or orders under penalties will not trigger a qualification as repeat offence."

The same experts highlight two points. First they argue that the bandwidths and standard penalties are much lower than the maximum amount foreseen in the GDPR, which indicates that the Dutch DPA will normally not apply the high penalty maximums of the GDPR.⁷⁶ Second, it is further debated that there is no room for turnover based fines in normal cases when it comes to fining practices of Dutch DPA.⁷⁷ Certainly, the Dutch Guidelines are not disarming the authority from the possibility to issue even maximum amount penalties or turnover based fines, however the Dutch DPA seems to recognize the challenge to translate the turnover into fine and render the economic impact of the latter on the relevant turnover.

3.2 BRITISH MODEL

The Information Commissioner's Office in the UK (the "ICO") has published for consultation its draft statutory guidance on setting the administrative fines (hereinafter "ICO Guidelines"). The ICO also provides that the final version will be released after the UK has left the EU and due changes will be considered. This is a huge step towards transparency in regulatory actions. Just the mere fact that yet another DPA is providing its own guidance on setting of fines, paves the path towards more clarity. Although practitioners argue there is still a large amount of discretion that the regulator can apply to adjust the fine both up and downwards, meaning that the process is not as transparent as it may at first seem⁷⁸.

The ICO is applying penalty notices in case of violations. A penalty notice is a formal document issued by the ICO (under section 155 DPA 2018) when it intends to fine an organization for a breach, or breaches, of the data protection law. The penalty notice sets out the amount the ICO intends to fine an organization and the reasons for its decision⁷⁹. The aim

⁷⁶ Ibid.

⁷⁷ Ibid.

⁷⁸ Everett, M. (2020) *How to calculate a GDPR Fine – the proposed ICO way* [online]. Available from: <https://www.lexology.com/library/detail.aspx?g=50cca832-df9c-4d39-b771-ed4b7485e833> [Accessed 14 March 2021].

⁷⁹ Information Commissioner's Office (2020) *Statutory guidance on our regulatory action* [online]. Available from: <https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf> [Accessed 14 March 2021], p. 17.

pursued by the ICO in issuing penalty notices is in line with P2 and P3 set out in the EDPB Guidelines.

An interesting detail in the procedure provided by the ICO is the existence of a notice of intent (NOI), which advises the organization or individual that the ICO intends to serve them with a penalty⁸⁰. The NOI sets out: (a) the circumstances of the breach; (b) the ICO's investigative findings; (c) the proposed level of penalty; (d) a rationale for the basis; and (e) the amount of the penalty⁸¹. If the organization disagrees with the NOI a negotiation process can take place between the concerned parties that includes either written or oral representations.

According to the ICO⁸²:

“The maximum amount (limit) of any penalty depends on the type of breach and whether the ‘standard maximum amount’ or ‘higher maximum amount’ applies. The higher maximum amount is, in the case of an undertaking, 20 million Euros or 4% of turnover, whichever is higher, or in any other case, 20 million Euros. The standard maximum amount is, in the case of an undertaking, 10 million Euros or 2% of turnover, whichever is higher, or in any other case, 10 million Euros. Where a fine based on turnover exceeds the 10 or 20 million Euros limit, the ICO will cap the fine at the relevant limit. The ICO may impose a fine up to the relevant limit, if a fine based on turnover would not result in a proportionate fine because, for example, a company has a very low or no turnover (but has committed a serious breach of data protection law).”

The overview of the nine-step evaluation process is provided in Figure 4 below. Details on each step are included in the ICO Guidelines.

⁸⁰ *Op cit*, p. 18.

⁸¹ *Ibid*.

⁸² *Op cit*, p. 20.

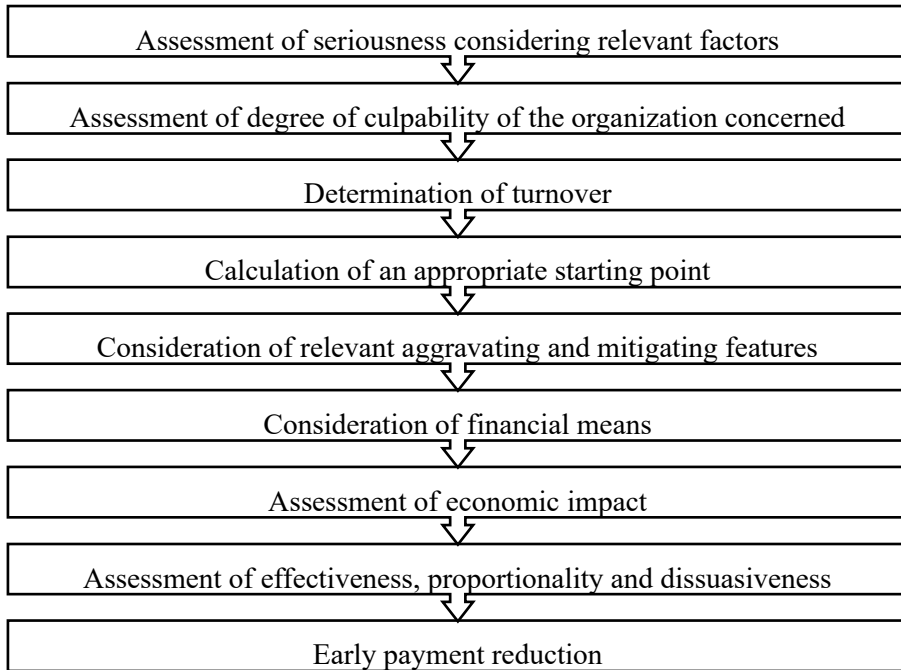


Figure 4. Nine-step evaluation process by the ICO.

Nonetheless, both the third and the last step are noteworthy points. In order to set the starting point under step three, the ICO provides a very helpful structure shown in Table 3. From the examination of this table, one may easily spot differences between the fine's bandwidths suggested by the ICO and the Dutch DPA. Also in its last step the ICO incentivizes the rapid payment of penalty notices. According to the ICO Guidelines, the ICO will reduce the monetary penalty by 20%, if they receive full payment of the monetary penalty within 28 calendar days of sending the notice⁸³. However, this early payment discount is not available if a data controller or person decides to exercise their right of appeal to the First-tier Tribunal (Information Rights)⁸⁴.

⁸³ Information Commissioner's Office (2020) *Statutory guidance on our regulatory action* [online] Available from: <https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf> [Accessed 14 March 2021], p. 24.

⁸⁴ Ibid.

Penalty starting point				
Standard Maximum Amount (SMA) (max of 2% or 10 Million Euro)				
Higher Maximum Amount (HMA) (max of 4% or 20 Million Euro)				
Seriousness:				
Degree of culpability:	Low	Medium	High	Very High
Low / No	SMA 0.125%	SMA 0.25%	SMA 0.375%	SMA 0.5%
	HMA 0.25%	HMA 0.5%	HMA 0.75%	HMA 1%
Negligent	SMA 0.25%	SMA 0.5%	SMA 0.75%	SMA 1%
	HMA 0.5%	HMA 1%	HMA 1.5%	HMA 2%
Intentional	SMA 0.375%	SMA 0.75%	SMA 1.125%	SMA 1.5%
	HMA 0.75%	HMA 1.5%	HMA 2.25%	HMA 3%

Table 3. ICO Penalty Starting Point

3.3 GERMAN MODEL

The Conference of the German Data Protection Authorities (DSK) has published its own model of calculating fines under the GDPR⁸⁵. The model is strict and can lead to very high amounts. This model heavily uses the concept of undertaking, since larger companies can receive stellar amount of fines.

The process is similar to the Dutch and British models in as much as it includes classification of infringements. It is no surprise all three models are considering such a tiering system, which has its roots in the EDPB Guidelines⁸⁶. The DSK provides a five-step procedure to calculate fines. In comparison to the Dutch and British model, this procedure focuses on the offenders not the infringement itself.

⁸⁵ Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2019) *Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen* [online]. Available from: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf [Accessed 21 March 2021].

⁸⁶ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 9.

3.3.1 CATEGORIZATION OF COMPANIES

How the DSK wishes to determine the size class of each company is based on annual threshold limits. This approach highlights the economic impact that DPAs might have. Table 4 shows the size classes.

Micro, small and medium-sized companies (SMEs)				Large companies			
A		B		C		D	
Micro companies		Small companies		Medium-sized companies		Annual turnover of more than € 50m	
Annual turnover up to € 2m		Annual turnover of more than € 2m up to € 10m		Annual turnover of more than € 10m up to € 50m			
A.I	Annual turnover up to € 700,000	B.I	Annual turnover of more than € 2m up to € 5m	C.I	Annual turnover of more than € 10m up to € 12.5m	D.I	Annual turnover of more than € 50m up to € 75m
A.II	Annual turnover of more than € 700,000 up to € 1,4m	B.II	Annual turnover of more than € 5m up to € 7.5m	C.II	Annual turnover of more than € 12.5m up to € 15m	D.II	Annual turnover of more than € 75m up to € 100m
A.II I	Annual turnover of more than € 1,4m up to € 2m	B.II I	Annual turnover of more than € 7.5m up to € 10m	C.III	Annual turnover of more than € 15m up to € 20m	D.III	Annual turnover of more than € 100m up to € 200m
				C.IV	Annual turnover of more than € 20m up to € 25m	D.IV	Annual turnover of more than € 200m up to € 300m
				C.V	Annual turnover of more than € 25m up to € 30m	D.V	Annual turnover of more than € 300m up to € 400m
				C.VI	Annual turnover of more than € 30m up to € 40m	D.VI	Annual turnover of more than € 400m up to € 500m

	C.VII	Annual turnover of more than € 49m up to € 50m	D.VI I	Annual turnover of more than € 500m
--	--------------	--	---------------	-------------------------------------

Table 4. Determination of size class.

3.3.2 AVERAGE ANNUAL TURNOVER

These are determined based on DSK guidance. Table 5 presents the thresholds of average annual turnovers.

Micro, small and medium-sized companies (SMEs)						Large companies	
A		B		C		D	
A.I	€ 350,000	B.I	€ 3.5m	C.I	€ 11.25m	D.I	€ 62.5m
A.II	€ 1,050,000	B.II	€ 6.25m	C.II	€ 13.75m	D.II	€ 87.5m
A.III	€ 1.7m	B.III	€ 8.75m	C.III	€ 17.5m	D.III	€ 150m
				C.IV	€ 22.5m	D.IV	€ 250m
				C.V	€ 27.5m	D.V	€ 350m
				C.VI	€ 35m	D.VI	€ 450m
				C.VII	€ 45m	D.VII	concrete annual turnover*

* If the annual turnover exceeds € 500m, the maximum fine of 2% or 4% of the annual turnover must be taken as the maximum limit, so that the calculation is based on the actual turnover of the respective company.

Table 5. Average annual turnover rates.

3.3.3 DAILY RATES

The daily rates are calculated using a simple mathematical calculation. The average annual turnover rates are divided by 360. Table 6 provides the overview of daily rates.

Micro, small and medium-sized companies (SMEs)						Large companies	
A		B		C		D	
A.I	€ 972	B.I	€ 9,722	C.I	€ 31,250	D.I	€ 173,611
A.II	€ 2,917	B.II	€ 17,361	C.II	€ 38,194	D.II	€ 243,056
A.III	€ 4,722	B.III	€ 24,306	C.III	€ 48,611	D.III	€ 416,667
				C.IV	€ 62,500	D.IV	€ 694,444
				C.V	€ 76,389	D.V	€ 972,222
				C.VI	€ 97,222	D.VI	€ 1.25m
				C.VII	€ 125,000	D.VII	concrete daily rate*

* If the annual turnover exceeds € 500m, the maximum fine of 2% or 4% of the annual turnover must be taken as the maximum limit, so that the calculation is based on the actual turnover of the respective company.

3.3.4 DAILY RATES MULTIPLIED BY FACTORS.

In order to receive the final amount, the daily rate has to be multiplied by a factor. This factor is based on the degree of severity of infringement and whether it is a formal or material offence. Formal infringements are listed in Art. 83 (4) of GDPR, while material offences are the ones provided by Art. 83 (5) and (6) of GDPR. The factors are displayed in Table 7.

Degree of severity of offence	Factor for formal offences	Factor for material offences
Light	1 to 2	1 to 4
Medium	2 to 4	4 to 8
Severe	4 to 6	8 to 12
Very severe	6 <	12 <

Table 7. Factors applied to daily rates.

3.3.5 FINE ADJUSTMENT

This last step pinpoints the fact that the amount calculated will be adjusted on the basis of circumstances in favour of and against the party concerned, as far as these have not yet been taken into account in the fourth step. In particular, this includes all offence-related circumstances (cf. catalogue of criteria in Art. 83 para. 2 GDPR) as well as other circumstances, such as a long proceeding or an imminent company insolvency⁸⁷.

Ziegler and Eichelmann argue that the above five steps can be summarized in a general formula⁸⁸ described as the average annual turnover divided by daily rates and then multiplied by factors, where the amount received is subject to substantial scrutiny of the competent DPA.

Hamelin and Brandt heavily debate the legal conformity of the German model. They argue that there is a dubious reference to 'group turnover'⁸⁹. As the authors provide it⁹⁰:

⁸⁷ Ziegler, S. and Eichelmann, A. R. (2019) *Five steps to calculate GDPR fines: new model adopted by German data protection authorities conference* [online]. Available from: <https://www.herbertsmithfreehills.com/latest-thinking/five-steps-to-calculate-gdpr-fines-new-model-adopted-by-german-data-protection> [Accessed 16 March 2021].

⁸⁸ Ibid.

⁸⁹ Hamelin, A. and Brandt, E. (2019) *The German model for calculating fines under GDPR: more questions than answers* [online]. Available from: <https://technologyquotient.freshfields.com/post/102fvyyu/the-german-model-for-calculating-fines-under-gdpr-more-questions-than-answers> [Accessed 16 March 2021].

⁹⁰ Ibid.

“According to Article 83 of the GDPR – the key provision on fines – the reference point for the fine is ‘the undertaking’, not ‘undertakings’ or ‘a group of undertakings. This suggests the legislator intended that a fine would apply to the particular infringing business rather than the wider group.

This makes even more sense when considering that GDPR infringements may only be committed by a data controller or processor acting as a single entity. Why then should fines be determined on the basis of the group turnover, which would include entities that are not involved in the data processing?

Furthermore, this competition law-like approach does not fit the GDPR system. Under competition law, fines are calculated based on group turnover to account for the fact that the parent company might have benefited from the infringement. This does not necessarily apply to GDPR infringements, which do not always result in commercial benefits for the controller or processor.”

Further, practicing lawyers share the concerns on legitimacy of this model. Wybitul and Crawford provide that⁹¹:

“Whether sanctions imposed under the DSK fine model properly take into account the criteria required by Article 83 GDPR or can properly ensure that fines are in fact proportionate, is questionable. The DSK model, if adopted and applied, would be ripe for challenge. It could be difficult for data protection authorities to convince courts in administrative offence proceedings that the authorities in fact have determined appropriate, lawful fines using the model.”

As a conclusion to the German model, the strong opposition is caused because such a fining model would lead to the brutal application of a stick and carrot approach. Eventually, what the German DPAs aim to achieve is to apply the possibilities offered by the GDPR. This was that personal data protection can grow not only teeth, but claws as well. It should not

⁹¹ Wybitul, T. and Crawford, G. (2019) *German Data Protection Authorities Adopt New GDPR Fine Model* [online]. Available from: <https://www.jdsupra.com/legalnews/german-data-protection-authorities-38441/> [Accessed 17 March 2021].

be a paper tiger anymore, but a reckoning force that has to be feared. The German DPAs are right about this. They should be feared because they regulate a piece of legislation that is connected to a fundamental right: the right to privacy.

In chronological order the German model was among the first to be announced. Due to its rigorous approach, it had quite a wide reach in both academia and practice. There are notable attempts to reconstruct the model and translate it into GDPR fine calculators. By way of example, Cristopher Schmidt created such calculators⁹², CMS Tax Law⁹³ and by Compliance Essentials GmbH⁹⁴. The last GDPR fine calculator manages to synthesize in the most efficient way the steps presented above.

3.4 CUSTOM MODEL

In addition to the guidelines issued by DPAs, academia has provided its own point of view in relation to the setting of administrative fines. A holistic view is applied by Maxwell and Gateu in saying that the tiering systems applied by EDPB does not provide a reliable benchmark for assessing nature and gravity⁹⁵. They recommend that a more reliable proxy would be to discover the number of data subjects affected and multiply with the level of damage suffered by each of them⁹⁶. This individual damage score may be determined – according to the authors – based on type of incidents⁹⁷. They argue that⁹⁸:

“A violation involving sensitive data, or resulting in identity theft, might correspond to a high damage score for each individual than a violation creating no damage, for example a failure to mention the duration of data retention in an information notice.

⁹² Schmidt, C. (2019) *GDPR Fine Calculator based upon the Fining Schedule of German DPAs* [software] v.2.1. Available from: <https://app.calconic.com/api/embed/calculator/5d889ed254e7dd001eadd4ed> [Accessed 20 March 2021].

⁹³ CMS Tax Law (2020) *Fine Models by DPAs – Germany* [software]. Available from: <https://www.enforcementtracker.com/?finemodel-germany> [Accessed 20 March 2021].

⁹⁴ Compliance Essentials (2020) *GDPR Fine Calculator* [software]. Available from: <https://www.dsgvo-portal.de/gdpr-fine-calculator.php> [Accessed 20 March 2021].

⁹⁵ Maxwell, W. and Gateu, C. (2019), *A point for setting administrative fines under the GDPR*, [online]. Available from: <https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr> [Accessed 20.01.2021], p. 105.

⁹⁶ Ibid.

⁹⁷ Ibid.

⁹⁸ Ibid.

(...)

For example, in the case of a data breach involving the loss of sensitive data for 100,000 data

subjects, the number of data subjects may be multiplied by a high individual damage score, for

*example 3. This would yield a nature and gravity score of $100,000 * 3 = 300,000$.*

(...)

*A purpose for data processing with a high level of utility for society, e.g. medical research, might warrant a lower multiplier than a purpose with lower societal benefits, e.g. commercial advertising. In the context of our example, let us imagine that the processing of sensitive data was done for the purpose of creating commercial profiles for advertising. This would generate a high purpose multiplier, for example 3, compared to processing for medical research, which would generate a low purpose multiplier of 1. Thus in the foregoing example, the nature and gravity score would again be multiplied by 3: $300,000 * 3 = 900,000$.*

(...)

In addition to the nature and gravity, the duration of the violation must also be taken into account. Adding duration to the formula is straightforward: It would be sufficient to add a multiplier to the equation corresponding to the number of months during which the violation occurred. In the above example, if the data vulnerability resulting in the loss of sensitive data lasted for 6 months, the resulting nature and gravity score (900,000) would be multiplied by 6, the number of months during which the violation occurred. A linear duration multiplier is routinely used in setting of competition law fines."

The custom model dives into and tries to bring parallels between data protection law and competition law. The authors are convinced that the above-mentioned variables are relatively easy to be calculated. From here it would also be straightforward to develop a scoring system or calculation starting points. This methodology can be seen in practice from the other models analysed in this chapter. They see the big challenge to set the initial monetary amount to correspond to each point in the score⁹⁹.

4. FINE PREDICTION ANALYSIS

In this sub-chapter, results of predictive analysis are presented. This research builds on regression models constructed in R programming language. The dataset is generated by the use of publicly available data on existing GDPR fines, as well as additional information, which was acquired in partnership with a private company. The analysis will also cover a country level case-study in section 4.5.

4.1 METADATA

The dataset includes 15 variables and 312 observations. Each observation is a case in which an administrative fine has been set for GDPR infringement. The variables used in this session are factor and double variables. Table 8 contains a description of each.

Name	Type	Description
Country	Factor	Represents the country in which the DPA has issued the administrative fine.
type	Factor	Represents the nature of infringement for which the fine has been issued.
industry	Factor	Represents the industry in which the controller or processor is acting.
tiertwo	Factor	Represents the delimitation based on the tiering system introduced by the GDPR. If the infringed article referenced by the DPA is mentioned in Article 83 (5) of GDPR, it will be qualified as a higher infringement, otherwise if it will remain a minor infringement for which Article 83 (4) of GDPR applies.
Fine	Double	The amount of monetary sanction given to the controller or processor

⁹⁹ *Op cit*, p. 111.

article	Double	The number of articles referenced by the DPA in the communication.
calc	Double	The number of months passed since the GDPR is applied.
calc2	Double	The number of days passed since the GDPR is applied.
turnover	Double	The amount of turnover realized by the controller or processor in 2019.
employee	Double	The number of employees of the controller or processor in 2019.
age	Double	The company seniority level that is calculated by subtracting the date of establishment from the current year.
keyarticle	Factor	It is used to verify if Article 25 or 32 is referenced by the DPA in the communication about the fine. This variable aims to verify the degree of responsibility as recommended by the EDPB Guidelines.
track	Factor	It is used to verify if the controller or processor has committed any previous infringements of GDPR. The presumption is that if an entity appears more than once in the database, the track record should be positive.
special	Factor	It is used to verify if Article 9 or 10 is referenced by the DPA in the communication of the fine. These two articles are providing for special categories of personal data.
order	Factor	It is used to verify if Article 58 is referenced by the DPA in the communication of the fine. This article provides the DPA the possibility to issue orders towards the controllers and processors. If such orders were issued and not implemented by the controllers or processors, the order variable should be positive.

Table 8. Description of variables.

4.2 REGRESSION TREE

A regression tree is generated using specific variables. The only variable that is eliminated from this analysis is the 'Country' variable due

to the massive diversity it creates in the plot. The regression tree shows that the turnover and the number of days passed since the application of GDPR are the strongest predictors that influence the amount of a GDPR fine. The type of infringement and the industry in which the controller or processor is acting will have also significant impacts. The overall regression tree is presented in Figure 5. Unfortunately, the regression tree also shows no strong correlations between the predictors.

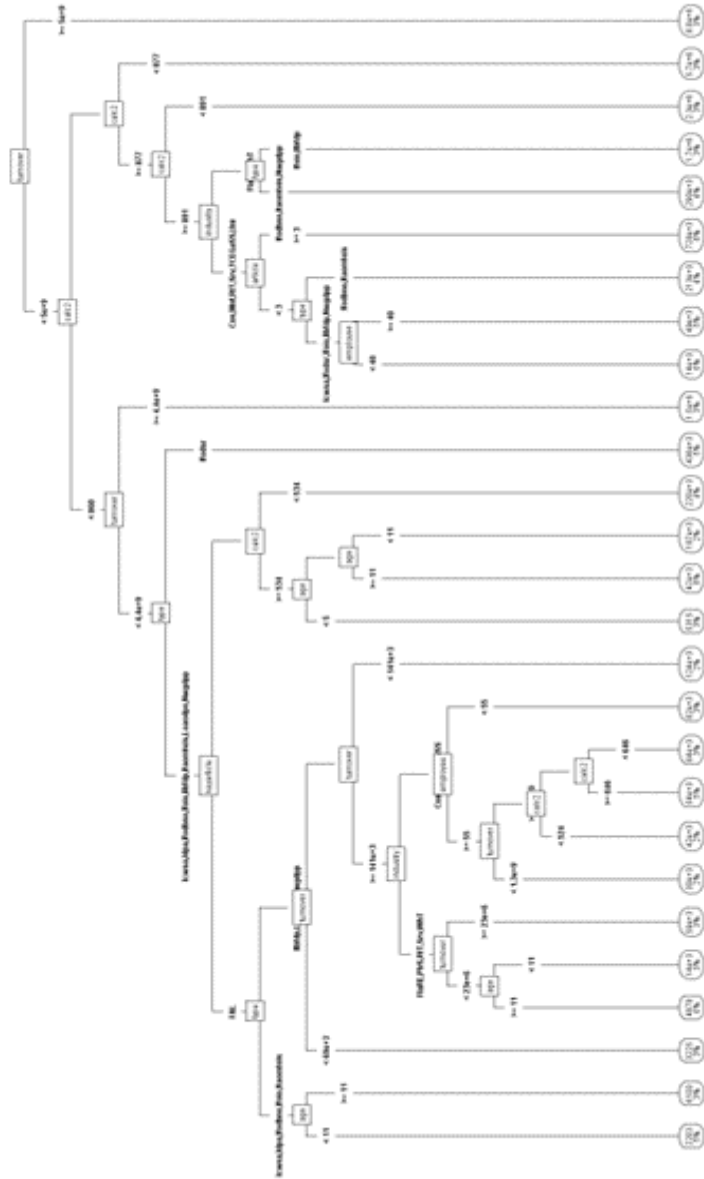


Figure 5. Regression tree of GDPR fines

4.3 RANDOM FOREST

A random forest prediction algorithm is constructed with the use of all variables. By setting the number of regression trees in this model to 1000, the error rate of the prediction model should be reduced. Figure 6 depicts the importance of variables used in this model, while Figure 7 presents the number of trees in correlation to the standard error.



Figure 6. Importance of variables plot.

The importance of variables plot explains that 'Country' and 'turnover' are two variables with the highest impact on the predicted GDPR fine. On number of trees vs standard error plot we can see that the standard error for the formula decreases in the beginning by adding new random trees to the model, however it slowly stabilizes after 200 regression trees are added to the forest and fluctuates in an insignificant manner up until 1000 regression trees are added to the forest.

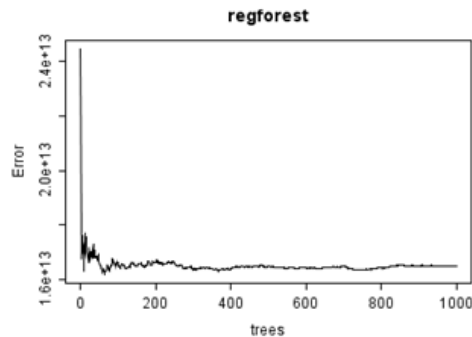


Figure 7. Number of trees vs standard error.

Further the multi-way importance plot presented in Figure 8 provides additional insights on which variables contribute the most to the accuracy of this regression model.

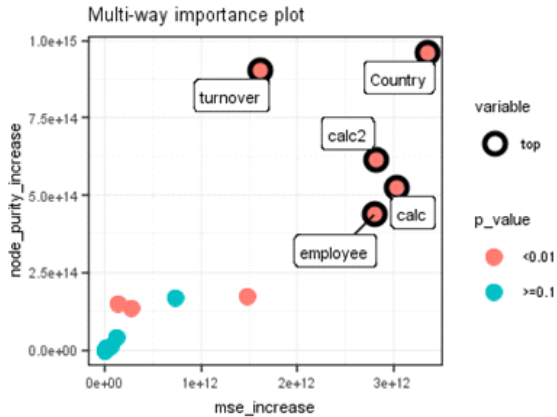


Figure 8. Multi-way importance plot.

4.4 LINEAR REGRESSION

The linear regression model provides poor results with no correlation between the predictors. The multiple R-squared is at 0.3736, the adjusted R-squared is sitting at 0.2648. This means that the variables used for this model are not the most accurate ones. After applying the backward variable selection, we arrive to at the conclusion that Country, article, turnover, age, and track variables should be used. However, the problem persists as the multiple R-squared value is still very low. The parameters after backward variable selection are:

Residual standard error: 3439000 on 288 degrees of freedom
 Multiple R-squared: 0.3473, Adjusted R-squared: 0.2952
 F-statistic: 6.663 on 23 and 288 DF, p-value: <math>< 2.2e-16</math>

Figure 9 illustrates the impact of variables in plots. Interpretation shows that in the United Kingdom (UK) the fines can be much higher compared to the others. Also, the GDPR fines tend to increase if more articles are referenced by the DPAs in their decision to issue an administrative fine. Further, whenever the turnover number is higher for a controller or processor, the amount fined will also be higher. Moreover, the seniority level of the company is not an aggravating circumstance, in terms that more recently established companies can receive higher fines. Finally, there

is a decrease in the amount if fine, in the event a company has a track record of any previous infringement. Although this might seem an unrealistic scenario, it can be applied due to the fact that the authority considers that the controller or processor was already subject to a penalty. Nonetheless, the difference between having a track record in any previous infringement seem to be negligible from the analysis.

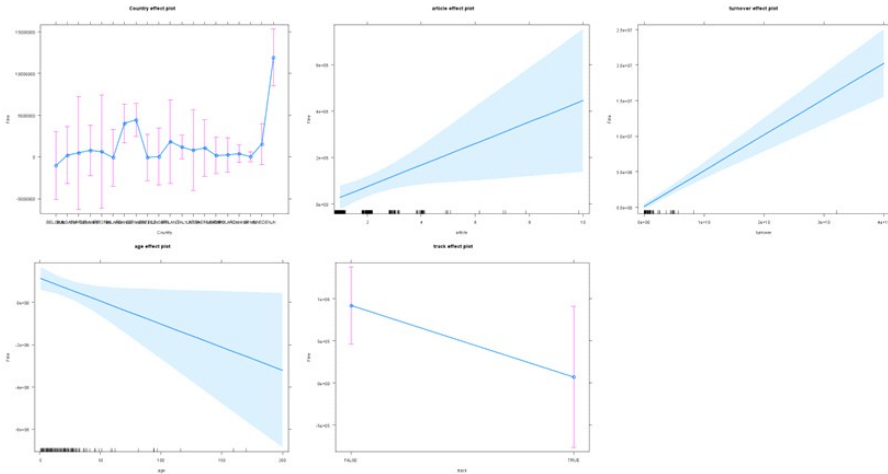


Figure 9. Impact of variables plots.

4.5 COUNTRY LEVEL ANALYSIS

The same prediction models can be performed on a different dataset. This is possible due to reporting practices of the Romanian DPA, which consistently issue a short description of the circumstances around their fining practices. By reviewing the descriptions, there is a possibility to extract new variables, which are not known of other cases. Therefore, in this sub-chapter the aim is to carry out an analysis on the Romanian cases, where a monetary sanction was applied towards a controller or processor for GDPR infringements.

4.5.1 METADATA

This dataset includes 17 variables and 40 observations. Each observation is a case officially published by the Romanian DPA. Table 9 includes a description of variables. It is worth considering that the results of the analysis will be limited to the relatively small number of observations. This will be taken into consideration throughout to process.

Name	Type	Description
months	Double	The number of months passed since the GDPR is applied.
fine	Double	The amount of monetary sanction given to the controller or processor.
type	Factor	Represents the type GDPR infringement.
controller	Factor	Represents the quality of party concerned, i.e. a controller or processor.
reference	Double	The number of articles referenced by the DPA in the communication.
ds	Double	The number of data subjects involved in the infringement.
undertaking	Factor	Represents if the party concerned is part of an undertaking or not.
private	Factor	Represents if the party concerned is an entity acting in the public or a private sector.
age	Double	The company seniority level that is calculated by subtracting the date of establishment from the current year.
turnover	Double	The amount of turnover realized by the controller or processor in 2019.
profit	Double	The amount of profit realized by the controller or processor in 2019.
cash	Double	The amount of free cash ready to be used by controller or processor.
employee	Double	The number of employees of the controller or processor in 2019.
complaint	Factor	Shows if the DPA issued the fine based on a complaint received from data subjects.
notification	Factor	Shows if the DPA issued the fine based on a notification submitted by the controller or processor.
special	Factor	Shows if Article 9 or 10 is referenced by the DPA in the communication, or there are outlier circumstances (e.g. the involved data subjects are minors).
industry	Factor	Represents the industry in which the controller or processor is acting.

Table 9. Variables of Romanian cases.

4.5.2 REGRESSION TREE

The regression tree is generated using all variables. The regression tree provides better correlation between the variables than in the previous scenario. The most important variables according to this model are the company age, the industry in which it is acting, and the number of data subjects affected by the infringement. Figure 10 provides the overview of the regression tree.

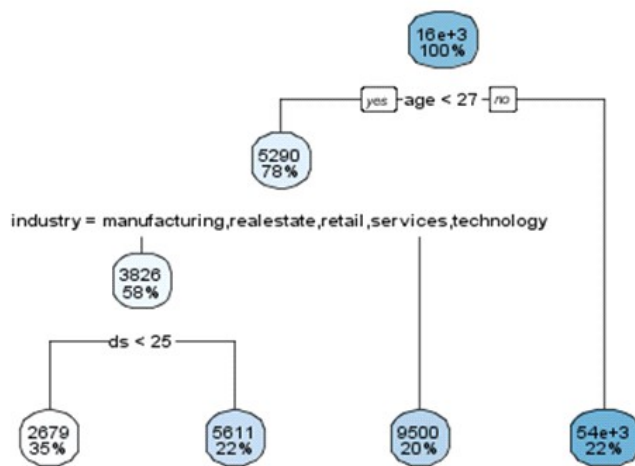


Figure 10. Regression tree of GDPR fines – Romania.

4.5.3 RANDOM FOREST

Following the example in the previous scenario, a random forest prediction algorithm is constructed with the use of all variables. The number of regression trees in this model is set to 1000 for the same reasons. Figure 12 provides the importance of variables used in this model, while Figure 11 presents the number of trees in correlation to the standard error.



Figure 11. Importance of variables plot – Romania.

We can see that in this case the variables ‘ds’ and ‘age’ are the ones with the highest impact on the predicted GDPR fine. Similarly to the previous scenario, the standard error for the formula decreases in the beginning by adding new random trees to the model, and it stabilizes after 600 regression trees are added to the forest.

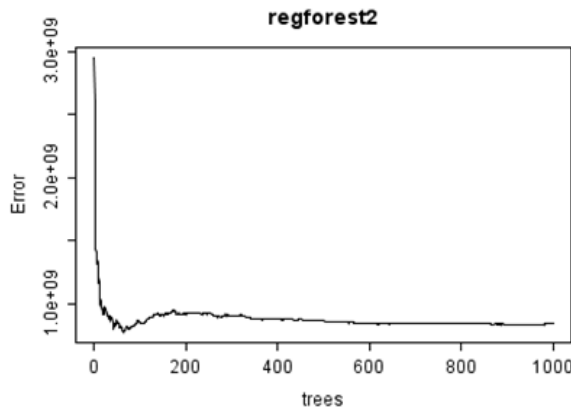


Figure 12. Number of trees vs standard error – Romania.

Also, Figure 13 gives additional insights on the multi-way importance of variables, for which the interpretation is same as in Section 4.3.

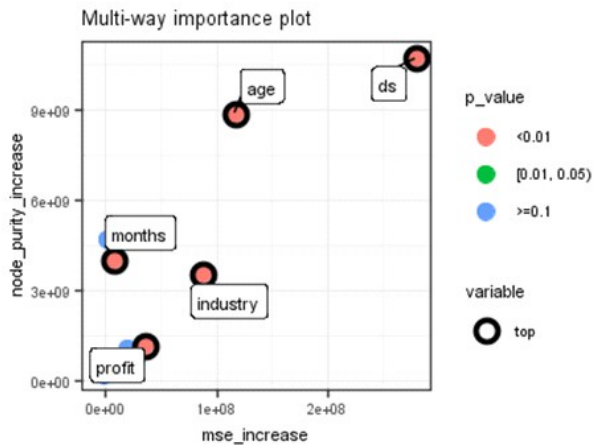


Figure 13. Multi-way importance plot – Romania.

4.5.4 LINEAR REGRESSION

The linear regression model with regards to these variables provides much better results compared to the previous dataset. The first iteration gives encouraging results, which can be presented as follows:

Residual standard error: 21920 on 14 degrees of freedom
 Multiple R-squared: **0.8573**, Adjusted R-squared: **0.6024**
 F-statistic: 3.363 on 25 and 14 DF, p-value: **0.01069**

The backwards variable selection also provides guidance on eliminating at least the “months” variable, which then translate into the following results:

Residual standard error: 21180 on 15 degrees of freedom
 Multiple R-squared: **0.8572**, Adjusted R-squared: **0.6286**
 F-statistic: 3.751 on 24 and 15 DF, p-value: **0.005244**

The results of the effects of variables are then plotted to serve as basis of interpretation. Figure 14 provides the plot effects for each of the variables. It can be concluded that the number of data subjects involved in the data breaches is one of the most prominent variables. Second, if the DPA received a complaint, this would also entail a higher fine. Third, if the controller or processor is part of an undertaking is also an incentive to receive a higher fine. Forth, the existence of a notification to the DPA could translate into a higher fine.

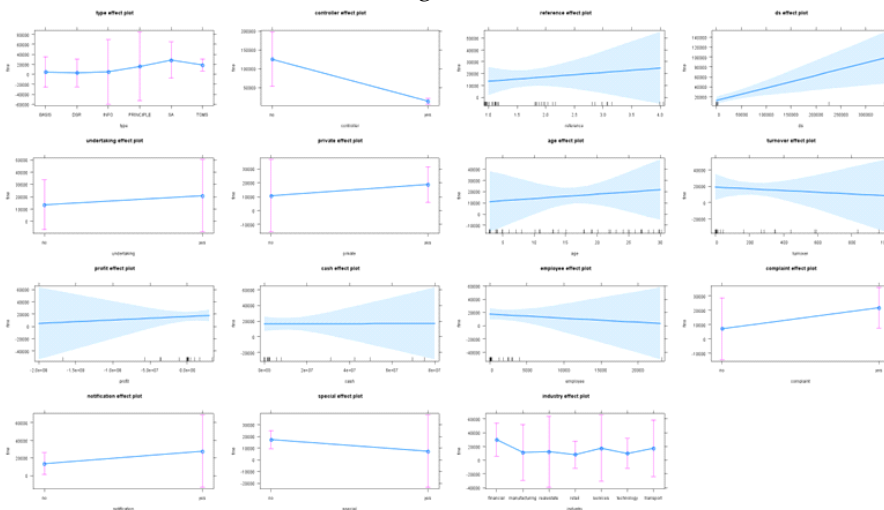


Figure 14. Impact of variables plots – Romania.

All three models are then trained with cross-validation using 15 folds with 10 repeats. The training serves the purpose to enhance the prediction accuracy. Finally the model with the most accuracy rate is selected. The regression tree as a result of cross-training got to 66%, the random forest to 69 % and the linear regression to 68 %.

The conclusion of the analysis shows that in order for these models to work more observations are needed. More observations means that more information has to be publicly available in relation to infringements. Thus, to be able to predict the amount of GDPR fines, additional information is needed for cases on the following topics as a minimum:

- a. Number of data subjects affected by the infringement;
- b. The existence of complaints submitted by data subjects;
- c. The controller or processor forming part of an undertaking;

- d. The existence of notifications submitted by the controller or processor;
- e. The category of personal data involved.

5. CONCLUSION

Predicting GDPR fines is a complex topic. This subject has recently claimed the attention of academia¹⁰⁰. Although arguably it is still an under-researched area. Thus, there is motivation to determine the best prediction models of GDPR fines. The motivation has multi-way implications.

First, the GDPR raises the fines thresholds. The competent authorities are entrusted to use powers given to them in this sense. This may not translate in eagerness to issue stellar amounts. If this would happen, certain industries or sectors would witness severe headwind. Yet, competent authorities should embrace the spirit of dissuasive administrative fines.

Second, the same authorities are lacking qualified personnel. In the event they decide to use regression analysis as a prediction model, it could lead to an enhanced internal workflow. The findings of an investigation would be added to the model, and a preliminary amount issued as administrative fine would then be auto-generated. Finally, human intervention by the competent authority may revise the level of fine. At the very least, it could speed up their entire process.

Third, fine calculation models presented in Section 3 vary on country level. There is no consistency, as DPAs are embarking on different roads. More clarity is needed on this level. Controllers and processors are not in the position to reasonably know what to expect. The calculators currently available based on the German model are just black box predictions. The values are not customized according to different characteristics of an entity.

This chapter identifies existing guidelines. It also presents the suggested calculation models. Finally it offers a different approach to calculate fines using regression analysis. Although the models did not perform on an acceptable level, the main conclusion is that this is due to lack of information on suggested variables. Nevertheless, the most optimal variables are subject to a constant evaluation procedure. Key importance

¹⁰⁰ Ruohonen J. and Hjerpe K. (2020) The {GDPR} enforcement fines at glance, *Information Systems* 106, pp. 2-9. Available from <http://ceur-ws.org/Vol-2690/COURT-paper1.pdf> [Accessed 5 February 2021].

has to be provided to the nature of personal data involved in the infringements, to the categories of data subjects affected by such infringements and not at least, whether complaints have been submitted to the competent authority in a particular case. Fulfilment of notification obligation of controllers or processors is also a decisive factor. Yet, the authority has to evaluate the economic situation of each entity that is subject to investigation. The economic situation could translate in a wide-range of variables. Only turnover-based judgments might lead to wrong decisions. The fining practices of DPAs confirm this view.

The analysis and the interviews carried out in this chapter are representing a good starting point. Nonetheless, these are limited to lack of cases available for examination. Future work indicates the need to perform the regression analysis, once a better data-set can be constructed. Additional calculation models that will be published in the future by DPAs might bring researchers one step closer to understand intentions behind the curtains. The current fining practices are still overwhelmed with high degree of discretionary subjectivity. With the value of money being quite different across Europe, this is still a problem that is desperately looking for a solution.

LIST OF REFERENCES

- [1] Albrecht, J. P. (2016), Privacy enforcement in search of its base, In: David Wright and Paul De Hert (eds) *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer International Publishing
- [2] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, (WP 203, 00569/13/EN) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 2 February 2021].
- [3] Barrett, C. (2020) Emerging Trends from the First Year of EU GDPR Enforcement, *ABA – American Bar Association Data, Spring 2020* 16 (3). Available from https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/spring/emerging-trends-the-first-year-eu-gdpr-enforcement/#25 [Accessed 25 January 2021].
- [4] Blutman, L. (2014), *Az Európai Unió joga a gyakorlatban*, Budapest, HVG-ORAC, p.158. .
- [5] Boetebeidsregels Autoriteit Persoonsgegevens (2019) *Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van*

- bestuurlijke boetes [online]. Available from: <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan> [Accessed 14 March 2021].
- [6] Commission Staff Working Paper. SEC (2012) 72 final, Brussels, 25.1.2012. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf
- [7] Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal of the European Union* (L281, 23/11/1995 P. 0031 – 0050). Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046> [Accessed 4 February 2021].
- [8] Everett, M. (2020) *How to calculate a GDPR Fine – the proposed ICO way* [online]. Available from: <https://www.lexology.com/library/detail.aspx?g=50cca832-df9c-4d39-b771-ed4b7485e833> [Accessed 14 March 2021].
- [9] Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from <https://www.jipitec.eu/issues/jipitec-8-1-2017/4533> [Accessed 10 February 2021].
- [10] Greengard, S. (2018) Weighing the impact of GDPR, *Communications of the ACM* 61 (11) .
- [11] Hamelin, A. and Brandt, E. (2019) *The German model for calculating fines under GDPR: more questions than answers* [online]. Available from: <https://technologyquotient.freshfields.com/post/102fvyu/the-german-model-for-calculating-fines-under-gdpr-more-questions-than-answers> [Accessed 16 March 2021].
- [12] Hansell, S. (2008), *Europe: Your I.P. Address Is Personal.*, [blog entry], 22 January 2008, BITS. Available from: <https://bits.blogs.nytimes.com/2008/01/22/europe-your-ip-address-is-personal/> [Accessed 17 January 2021].
- [13] Information Commissioner’s Office (2020) *Statutory guidance on our regulatory action* [online]. Available from: <https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf> [Accessed 14 March 2021]
- [14] Judgement of Comet BV v Produktschap voor Siergewassen, Case C-45/76, ECLI:EU:C:1976:191.
- [15] Judgement of Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española de Petróleos SA, Case C-217/05, ECLI:EU:C:2006:784.
- [16] Judgement of Höfner and Elsner v Macrotron GmbH, Case C-41/90, ECLI:EU:C:1991:161.

- [17] Judgement of LCL Le Crédit Lyonnais v. Fesih Kalhan, Case C- 565/12, ECLI:EU:C:2014:190.
- [18] Judgement of Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779.
- [19] Judgement of Ute Reindle v. Bezirkshauptmannschaft Innsbruck, C- 443/13, ECLI:EU:C:2014:2370.
- [20] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2019) *Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen* [online]. Available from: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf [Accessed 21 March 2021].
- [21] Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under the GDPR, [online]. Available from: <https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr> [Accessed 20.01.2021]
- [22] Ohm, P. (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review* Vol. 57. Available from <https://ssrn.com/abstract=1450006>. [Accessed 11 February 2021], p. 1738.
- [23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union* (L 119, 4.5.2016, p. 1–88). Available from: <https://eur-lex.europa.eu/eli/reg/2016/679> [Accessed 4 February 2021]
- [24] Rubinstein, I. (2012) Big Data: The End of Privacy or a New Beginning? *NYU School of Law, Public Law Research Paper No. 12-56*. Available from <http://dx.doi.org/10.2139/ssrn.2157659> [Accessed 17 December 2020].
- [25] Ruohonen J. and Hjerpe K. (2020) The {GDPR} enforcement fines at glance, *Information Systems* 106, pp. 2-9. Available from <http://ceur-ws.org/Vol-2690/COURT-paper1.pdf> [Accessed 5 February 2021].
- [26] Steenbruggen, W. and Van Der Eijk, B. (2019) *Dutch regulator publishes guidelines for the calculation of administrative fines under the GDPR* [online]. Available from: <https://www.twobirds.com/en/insights/2019/netherlands/dutch-regulators-publishes->

guidelines-for-the-calculation-of-administrative-fines-under-the-gdpr [Accessed 15 March 2021].

[27] UC Business Analytics R Programming Guide (2018), available: www.uc-r.github.io

[28] Wybitul, T. and Crawford, G. (2019) *German Data Protection Authorities Adopt New GDPR Fine Model* [online]. Available from: <https://www.jdsupra.com/legalnews/german-data-protection-authorities-38441/> [Accessed 17 March 2021].

[29] Ziegler, S. and Eichelmann, A. R. (2019) *Five steps to calculate GDPR fines: new model adopted by German data protection authorities conference* [online]. Available from: <https://www.herbertsmithfreehills.com/latest-thinking/five-steps-to-calculate-gdpr-fines-new-model-adopted-by-german-data-protection> [Accessed 16 March 2021].