*European Integration Studies, Volume 17, Number 1 (2021), pp. 167–179.*
*http://doi.org/10.46941/2021.se1.167-179*

# RESPONSIBILITY OF THE DATA CONTROLLERS IN DATA PROTECTION LAW AND THE PRACTICE OF THE AUTHORITIES IN IMPOSING ADMINISTRATIVE FINE

MÁRIO ČERTICKY*

**Abstract:** The European Union's general data protection regulation ensures a high level of protection of personal data. The data controllers, during their data processing practice, must take into account not only the provisions of the Regulation but also national regulations and evolving data protection practice. Regulatory fragmentation makes it more difficult to comply with data processing standards. The responsibility of the data controller can arise in several directions, first of all, we can separate civil and public liability. The subject of this study is the examination of administrative liability within the scope of the latter, in the framework of which it analyses the theoretical and practical issues of imposing a data protection fine. For the practice of imposing fines, the decisions taken by each European Data Protection Supervisor are presented and conclusions are drawn from them.

***Keywords:*** *data protection, GDPR, administrative fine, data protection liability, liability for data processing.*

## 1. INTRODUCTION

It's been more than two years since 25th May 2018 when the General Data Protection Regulation (hereinafter: GDPR or Regulation)[1] became applicable. Notwithstanding, data controllers, the subjects to the personal scope of the GDPR, had more than two years after its entry into force (17th May 2016) to prepare for its application. The Regulation lays down several guarantees to ensure the protection of personal data, however, the Regulation emphasizes that it respects *"all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular (…) freedom to conduct a business".*[2] Nevertheless, many data controllers see the regulation as a source of danger. It is a fact that the GDPR imposes extremely strict requirements on data controllers, but its aim is not to make the activities of data controllers impossible, but to divert the processing of personal data into a lawful channel. Of course, this places a heavy burden on data controllers, but the problem can be solved with due care and the use of people with the right expertise.

---

* Assistant Lecturer, Department of Commercial Law, Institute of Civil Law, Faculty of Law, University of Miskolc.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council 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, 4th May 2016).

2 See recital (4) of the GDPR.

The aim of the study is to briefly describe the rules on the liability of data controllers, in particular administrative liability. In addition, the study outlines the sanctions that can be applied in administrative jurisdiction, in particular the administrative fine. In the course of the investigation, I will pay particular attention to the data protection investigations carried out by the data protection supervisory authorities of the certain Member States of the European Union and to the fines imposed in that context.

In the first chapter of the study, I describe the complex world of data processing standards. In the next chapter, I outline the directions of responsibility for data processing, which can have many aspects and affect many different areas of law. From each of the lines of responsibility, I would like to analyse in detail the administrative liability, in particular the issues of the administrative fine that can be imposed in this regard. In the last chapter of the study, in the light of the most common data protection breaches, I present some of the decisions and fines imposed by the data protection supervisory authorities of the Member States of the European Union. Aim if the study is to provide a brief overview of the relevant rules of the GDPR and its practical application by supervisory authorities.

## 2. SUMMARY OF THE LEGISLATION

It is necessary to outline briefly the legislation that applies to data protection issues. The alpha and omega of data protection law is the GDPR, which must be applied directly by all data controllers from 25th May 2018. Obviously, this idea should be understood with the addition that the Regulation takes precedence over the data processing which are under the scope of it. It is noteworthy to emphasize which data processes are under the scope of the GDPR. The material scope of the Regulation initially covers the wholly or partly automated processing of personal data and the non-automated processing of personal data which are stored or are intended to be stored in a filing system.[3] This means, that the processing of personal data that are not automated and are not part of a filing system[4] are not touched by the GDPR. However, it is not a condition that the registration system is already available, it is sufficient if the register can be compiled on the basis of some organizing principle.[5] The GDPR also defines several specific data processing that are not explicitly covered by it.[6] As far as the territorial scope of the GDPR is concerned, it covers the processing of personal data in the context of the activities of an establishment[7], of a controller or a processor in the

[3] See Article 2(1) of the GDPR.

[4] The definition of the filing system is regulated in Article 4(6) of the GDPR, as follows: *"filing system means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis."*

[5] JÓRI, András: A Rendelet hatálya. In: *A GDPR magyarázata* (szerk. JÓRI András). Budapest, HVG-Orac, 2018, p. 103.

[6] See Article 2(2) and (3) of the GDPR.

[7] Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary

Union, regardless of whether the processing takes place in the Union or not.[8] Also, the GDPR has an extraterritorial scope, which means that it also covers the activities of data controllers established outside the European Union but offering their services for data subjects within the European Union.[9]

Secondly, the individual national laws laying down general rules on data protection and all sectoral legislation governing a given activity and containing a provision on data processing should apply. As regards the relationship between the GDPR and national law, the application of the Regulation takes precedence. National legislators may adopt provisions adapting or supplementing the rules of the Regulation in areas where the GDPR expressly allows it. However, a rule contrary to the provisions of the GDPR cannot be set by national legislators.

The guidelines of the European Data Protection Board help to interpret each of the rules of the GDPR. Although these guidelines are non-binding, they serve as a reference in the proceedings of the national authorities and as a basis to confirm individual decisions. These findings apply to the guidelines issued by the national authorities. This therefore means that companies need to be aware of these standards when designing their data processing practice.

In the light of the requirement in recital 10 of the GDPR, which states that the *"Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union,"* the question arise, whether any decision taken by the data protection authority of any EU Member State – of course in a similar case – can serve as a reference. If we answer this question in the affirmative, then monitoring data protection practices will become an even more difficult task. This would also mean that national authorities should take into account not only the guidelines of the European Data Protection Board but also decisions taken by other authorities when taking decisions. This would allow for a uniform data protection practice across the European Union.

However, norms that do not specifically regulate a data protection issue, but prescribe an activity or mandatory behavior that necessarily involves data processing, should not be disregarded either. In these cases, the application of the provisions from a data protection point of view is filled by the provisions of the GDPR and other legislation regarding the nature of the activity. For example, company law or contract law also contains provisions in many places that require data processing (for example register of members, reports and so one). However, these need to be implemented in practice in the light of data protection rules.

This means that all the aforementioned legal norms must be applied when ensuring the lawfulness of data processing by data controllers in their day-to-day operations, which is an extremely difficult task. Of course, it is difficult to expect a company's

with a legal personality, is not the determining factor in that respect. See recital (22) of the GDPR.

8 See Article 3(1) of the GDPR.

9 See Article 3(2) of the GDPR.

management to be a data protection expert as well, which is why it is recommended to hire a data protection expert or appoint a data protection officer.

## 3. LIABILITY FOR DATA PROCESSING AND IT'S SANCTIONS

In examining the liability related to data processing, the subject of the liability must be identified. In this context, two personal responsibilities may arise, the responsibility of the data controller and the responsibility of the data processor.[10] Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[11] So, it can be stated that there is no company who processes personal data related to their activity that does not qualify as a controller. In contrast, the person who process the personal data on behalf of the controller is considered a data processor.[12] As the data processor acts on behalf of and in accordance with the instructions of the data controller, the responsibility lies primarily with the data controller. The data controller is responsible for ensuring that the data processing complies with the requirements of the GDPR. It is important that the controller and the processor enter into a written contract in which the details of the processing are specified in accordance with Article 28(3) of the GDPR. If the data processor sets an independent purpose for data processing in addition to the instructions of the data controller, data processor shall be considered an independent data controller and therefore shall have an independent responsibility.[13]

With regard to data protection liability, it can be stated it is objective, strict liability, which can be established by any violation of data protection rules, particularly any violation of the GDPR. There may be different sanctions for violations,[14] of which the warning and the administrative fine should be highlighted. The data protection authority shall issue a warning to the controller if it finds that it is proportionate and sufficient to achieve the purpose of the sanction. If the data protection authority finds that the warning is not sufficient, it shall impose a fine.

Let's review the rules for imposing an administrative fine. When imposing the fine, in particular when determining the amount of the fine, the authority shall ensure that it is effective, proportionate and dissuasive. The requirement is that it must determine in each case in light of the individual circumstances, but must endeavor to impose almost

[10] For a more detailed distinction between the controller and the processor, see the Guideline of the EDPB no. 07/2020 on the concepts of controller and processor in the GDPR. See: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf [downloaded: 5th January 2021].

[11] See Article 3(7) of the GDPR.

[12] See Article 3(8) of the GDPR.

[13] See Article 28(10) of the GDPR.

[14] These include sanctions for preventive and reparative purposes, such as instructions to remedy the infringement, to comply with the GDPR, to comply with the data subject's request, etc. See: JÓRI: op. cit. 416.

the same fine in relatively identical circumstances.[15] Article 83(2) of the GDPR sets out the circumstances to be taken into account by the authority, in particular, but not exclusively, when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine. The authority shall take into account, in particular, but not exclusively, the following circumstances: i) *"the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; ii) the intentional or negligent character of the infringement; iii) any action taken by the controller or processor to mitigate the damage suffered by data subjects; iv) any relevant previous infringements by the controller or processor; v) the categories of personal data affected by the infringement,"* etc.

It should also be emphasized that we can distinguish between two levels of violations, which affect the amount of the fine. For violations in the first category, the maximum fine may be set up to EUR 10 million or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In contrast, for the second category of infringements, the maximum fine may be set up to EUR 20 million or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The cases presented in this study are concerned infringements in the latter category. It can be concluded that, depending on the circumstances of the case, companies can expect even higher fines.

With regard to civil liability,[16] it should first be noted that Article 82 of the GDPR refers to the right to compensation. Based on this *"any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"*.[17] The GDPR regulates the liability of the data controller and the liability of the data processor separately. Accordingly, the controller is liable for any damage caused by the processing in breach of the Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.[18] If the data controller's independent liability doesn't arise, but the injuring party is the data processor, the

---

[15] See the Guidelines on the application and setting of administrative fines (wp253), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 .

[16] For a comprehensive comparison of data protection liability and civil liability, see TRULI, Emmanuela: The General Data Protection Regulation and Civil Liability. In: BAKHOUM, Mor – CONDE GALLEGO, Beatriz – MACKENRODT, Mark-Oliver – SURBLYTE-NAMAVICIENE Gintare (eds.): *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?* Springer, Berlin–Heidelberg, 2018, 303–329. https://doi.org/10.1007/978-3-662-57646-5_12; CORDEIRO, A. B. Menezes: Civil Liability for Processing of Personal Data in the GDPR. *European Data Protection Law Review (EDPL)*. 5 (4), 492–499. https://doi.org/10.21552/edpl/2019/4/7.

[17] Article 82(1) of the GDPR.

[18] Article 82(2) of the GDPR.

data controller is responsible for its conduct. As regards the exemption from the obligation to pay compensation, the GDPR contains only the following: *"a controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage."*[19] On this basis, the content of liability for damages should be determined on the basis of the liability standards established by national law.[20]

With regard to crimes related to data processing, the crime of misuse of personal data contained in § 219 of the Criminal Code[21] should be mentioned. The perpetrator of the crime can be anyone. Given that a natural person can also be considered a data controller, the crime of misuse of personal data may also arise. Under the relevant legislation,[22] the data controller may also be the subject to criminal liability.[23]

It is noteworthy to mention one of the decisions of the Hungarian Competition Authority fining Facebook for misleading the consumers.[24] The interesting thing about the case is that the decision was based on the fact that the Authority has established that personal data has value and how much we seem to use a service for free, we use our personal data to pay for it, because in this case was stated that Facebook uses our personal data to make profit.

## 4. PRACTICE OF IMPOSING ADMINISTRATIVE FINES

I have divided the cases in which fines have been imposed into five categories according to the nature of the violations. Thus, I have singled out the cases in which

---

19 Article 82(3) of the GDPR.

20 With regard to Hungarian law, therefore, the provisions of the Act V of 2013 on Civil Code may apply.

21 *„A person who, by violating a provision laid down in an Act or a binding legal act of the European Union on the protection or processing of personal data and for gain or causing significant harm to interests,*
*a) processes personal data in an unauthorized manner or in deviation from the purpose of processing, or*
*b) fails to take measures to safeguard such data*
*is guilty of a misdemeanour and shall be punished by imprisonment."*

22 See the Act CIV of 2001 on criminal measures applicable to a legal person.

23 See § 2 (1) of the Act CIV of 2001: *"The measures defined in the present act are applicable to legal entities in the event of committing any intentional criminal act defined in the Act C of 2012 on the Criminal Code (...) if the perpetration of such an act was aimed at or has resulted in the legal entity gaining benefit, or the criminal act was committed with the use of the legal entity and by*
*a) the legal entity's executive officer, its member, employee, officer, managing clerk entitled to represent it, its supervisory board member and/or their representatives, within the legal entity's scope of activity,*
*b) its member or employee within the legal entity's scope of activity, and it could have been prevented by the executive officer, the managing clerk or the supervisory board by fulfilling his/her/its supervisory or control obligations."*

24 See the decision of the Hungarian Competition Authority no. VJ/85/2016.

the fine was imposed for breach of the principles of the GDPR. The second category includes fines imposed for violations of the data subject's rights, while the third category includes cases of data processing without a lawful basis. In the fourth category are fines imposed in proceedings for data breaches. Finally, in the fifth category, I will mention other cases that cannot be included into those categories or they could be included into two or more mentioned categories.

The subject of the investigation were the decisions of the national authorities published by the EDPB, so I examined the decisions made not only by the Hungarian authority, but also by the authorities of almost all EU Member States.[25]

### 4.1. Violation of principles of the GDPR

Among the breaches of the data protection principles set out in the Article 5 of the GDPR should be highlighted the breach of purpose limitation,[26] the requirement of lawfulness, fairness and transparency,[27] data minimization[28] and from a data security perspective the principle of integrity and confidentiality.[29] It is noteworthy that any violation of the GDPR may result a breach of one or more principles of the GDPR, particularly the principle of lawfulness.

At the end of the 2019 the Berlin DPA imposed a fine of around 14.5 million Euros against Deutsche Wohnen for violations of the GDPR. The authority found that the company used an archive system for the storage of personal data of tenants that did not provide the possibility of removing data that was no longer required. Personal data of tenants were stored without checking whether storage was permissible or even necessary for the purpose of their original collection. This involved data on the personal and financial circumstances of tenants, such as salary statements, self-disclosure forms, extracts from employment and training contracts, tax, social security and health insurance data and bank statements.[30]

At the end of October 2020, the State Data Protection Inspectorate, which is a personal data protection supervisory authority of the Republic of Lithuania has fined

---

[25] The manuscript of the study was closed on 10 January 2021, so I examined the decisions of each Authority by this date.

[26] See Article 5(1)(b) *"personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."*

[27] See Article 5(1)(a) *"personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject."*

[28] See Article 5(1)(c) *"personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."*

[29] See Article 5(1)(f) *"personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."*

[30] See: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_hu [downloaded: 5th January 2021].

Vilnius City Municipality Administration for infringements of the principle of integrity and confidentiality. The fine (15,000 Euros) was imposed for violation of Articles 5(1)(d) and 5(1)(f) of the GDPR, i.e. a failure to implement appropriate technical and organizational measures, thus, failing to ensure the accuracy of processed personal data when processing personal data of the parents of the adopted child.[31]

### 4.2. Violation of data subject's rights

The most sensitive issues arise in the context of a breach of the data subject's rights. In the cases examined, most violations were committed in breach of the right to be informed, the right of access and the right to erasure or better known as right to be forgotten.

In the case before the Belgian authority Google was fined, because Google refused the Belgian citizen's request applied for removal of links containing negative information about him. The Belgian DPA considers that the links should have been delisted by Google. What's more, Google lacked transparency in their delisting form, as well as in their response to the data subject. For those reasons, the Belgian DPA decided to impose a fine of EUR 600,000, which is the highest fine ever imposed by the Belgian DPA.[32]

The Hungarian Data Protection Authority fined a data controller (a banking service provider) for failing to comply with its information obligations under Articles 12 and 13 of the GDPR and, in addition, treats the personal data of many of its customers without legal basis. As a result, it imposed a fine of HUF 25 million on the data controller.[33] In another case the Hungarian DPA imposed a fine on a data controller for not allowing the data subject to exercise his or her right of access for footage taken during camera surveillance. The case find that the data controller has not put in place adequate measures to ensure that the data subject's right of access is exercised. In this context, the controller did not differentiate between the right of access to personal data and the right to copy of personal data. The authority also found a violation of the right to restrict data processing, according to which it did not comply with the data subject's request not to delete his or her personal data until his or her request has been processed. The DPA has imposed a HUF 20 million (approx. EUR 55,000) fine for violation of Articles 15 and 18 of the GDPR. [34]

### 4.3. Data processing without lawful basis

In the cases examined, most violations concerned the lawfulness of data processing, which means that data controllers did not have legal basis for data processing, so the

---

[31] See: https://edpb.europa.eu/news/national-news/2020/lithuanian-dpa-imposes-fine-improperly-processed-personal-data-parents_hu [downloaded: 5th January 2021].

[32] See: https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu600000-fine-google-belgium-not-respecting-right-be_hu [downloaded: 5th January 2021].

[33] Case no. NAIH/2019/3107/7., See: https://www.naih.hu/files/NAIH-2019-3107-hatarozat.pdf.

[34] Case no. NAIH/2020/2204/8., See: https://www.naih.hu/files/NAIH-2020-2204-8-hatarozat.pdf.

data processing was unlawful. This issue differs from the others in that, in this case, the data processing is startlingly unlawful, while in the other cases the data processing is lawful but the data controller violated other obligation of the law.

Among these cases, I would like to highlight the proceedings before the Italian authority, in which a marketing company carried out direct marketing activities between 2017 and 2019 without the consent of the data subjects, which affected millions of people. The Italian data protection authority found the violation and imposed a fine of more than EUR 27 million.[35]

In another case, the Spanish Data Protection Authority (AEPD) imposed a fine of EUR 75,000 on Vodafone Espana for processing the claimant's telephone number for marketing purposes after they had exercised their right to erasure in 2015, regardless of what was sent to the data subject as an advertising SMS. The AEPD considered that the data controller violated Article 6(1) of the GDPR, by processing the claimant's personal data without any lawful basis.[36]

I note that in the case of data processing for marketing purposes, so in both abovementioned cases, the legal basis for data processing can only be the consent [Article 6(1) of the GDPR] of the data subject.

At the end of October 2020, the Norwegian Data Protection Authority has imposed an administrative fine of more than EUR 13,000 on a data controller for performing a credit check of a sole proprietorship without having a lawful basis for the processing. The curiosity about this case is that the authority classified the sole proprietor as the data subject because credit information about a sole proprietorship is regarded as personal data, as the owner is directly identified with the enterprise, and this is directly linked to the owner's private economy. The DPA has emphasized the private character of the personal data, seeing that the data is closely linked to the private economy of the owner.[37]

The Swedish Data Protection Authority has issued an administrative fine of SEK 300,000 (approx. EUR 27,500) against a housing company for unlawful video surveillance in an apartment building in the end of the December 2020. The essence of the investigation was that the data controller observed the doors of several flats in the stairwell through camera surveillance, which the Swedish DPA considered illegal. The Authority deliberated the data controller's legitimate interest and the right to privacy of the data subject and concluded that the latter took precedence.[38]

---

35 See: https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_hu [downloaded: 5th January 2021].

36 See: https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-aepd-imposes-fine-75000-eur-vodafone_hu [downloaded: 5th January 2021].

37 See: https://edpb.europa.eu/news/national-news/2020/norwegian-dpa-fines-odin-flissenter-performing-credit-check-sole_hu [downloaded: 5th January 2021].

38 See: https://edpb.europa.eu/news/national-news/2020/300000-sek-fine-against-housing-company_hu [downloaded: 5th January 2021].

### 4.4. Responsibility for data breaches

Perhaps the biggest risk in data processing is the possibility of a personal data breach. I would like to highlight one of the newest cases from the beginning of October. The Hamburg Commissioner for Data Protection and Freedom of Information imposed a EUR 35.3 Million Fine for violations of the GDPR by H&M.[39] The company has recorded several types of data about the personal life of their employees, including personal activities, data concerning health, data about their religion and some other sensitive data, which were stored on a network drive. This drive became accessible company-wide for several hours in October 2019 due to a configuration error. So, this was a multiple violation of the GDPR, first of all it was a data processing without lawful basis and it was also a data breach and violation of the principles.

The Hungarian Data Protection Authority has imposed a HUF 7.5 million (approx. EUR 21,000) fine on a data controller providing private healthcare services for violations of Article 32(1)(b), Article 33(1), and Article 34(1), because of a data breach. Due to a data security flaw in the online system operated by the data controller, the roughly fifteen thousand personal data stored in the system, including health data, were made public and could be accessed and downloaded by anyone.[40]

In another case conducted by the Hungarian data protection authority, it imposed a fine of HUF 100 million (approx. EUR 277,000 which is the biggest fine imposed in Hungary yet) on an internet service provider because it could have accessed the databases in the content management system used by the service provider. This was because the data controller was using a system that had become obsolete for nine years and was thus extremely vulnerable. Given that the data controller also stored old data in the system that was no longer needed, also violated the principles of purpose limitation [Article 5(1)(b)] and storage limitation [Article 5(1)(e)].[41]

The Information Commissioner's Office as a British Data Protection Authority (ICO) has fined Ticketmaster UK Limited GBP 1.25 million (approx. EUR 1.3 million) for failing to keep its customers' personal data secure. The ICO found that the company failed to put appropriate security measures in place to prevent a cyber-attack on a chat-bot installed on its online payment page. The data breach, which included names, payment card numbers, expiry dates and CVV numbers, potentially affected 9.4 millions of Ticketmaster's customers across Europe including 1.5 million in the UK. Investigators found that, as a result of the breach, 60,000 payment cards belonging to Barclays Bank customers had been subjected to known

---

[39] See: https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_hu [downloaded: 5th January 2021].

[40] Case no. NAIH/2020/952/, See: https://www.naih.hu/files/NAIH-2020-952-hatarozat.pdf [downloaded: 5th January 2021].

[41] Case no. NAIH/2020/1160/10, See: https://www.naih.hu/files/NAIH-2020-1160-10-hatarozat.pdf [downloaded: 5th January 2021].

fraud. Another 6,000 cards were replaced by Monzo Bank after it suspected fraudulent use.[42]

### 4.5. Other violations of the GDPR

In other categories, I have included legal cases in which data controllers have violated their other obligations under the GDPR, such as one of the most common breaches of data security, which is not the same with data breach.

In one case, the German authority imposed a fine of almost EUR 10 million on a telephone company, which did not provide sufficient technical and organizational measures to prevent unauthorized persons from being able to obtain customer information via the customer hotline service. In this context, the DPA also emphasized that the appointment of a data protection officer would also be such a measure, an obligation which the controller also failed to fulfill, despite the fact that it would have been mandatory under Article 37 of the GDPR.[43]

As a matter of data security measures, the Hungarian Data Protection Authority explained in one of its decisions related to paper files management that the data controller did not take the necessary organizational measures regarding the destruction of records containing personal data, thus violating the requirement of Article 32(1) of the GDPR. The Hungarian DPA imposed a fine of HUF 500,000 (approx. EUR 1,400).[44] It should be noted that this fine was not a high amount, but given the gravity of the infringement, it is certainly an indication to data controllers that they should also place great emphasis on the security of paper-based personal data.

## 5. SUMMARY AND CONSEQUENCES

In fact, full compliance with data protection rules is very difficult, but not impracticable. To do this, companies may seek the help of an expert, or employ a person or team who or which deals with data protection compliance in day to day work. Overall, companies need to place a strong emphasis on compliance with data protection rules, as they can also expect large fines for breaches or for violations. Due to the difficulty of complying with data protection rules, companies need to be prepared for possible fines and therefore need to shape their management. Imposing an administrative fine is therefore a constant risk for companies, so they need to put a lot of emphasis on risk management. They can use several options to do this, such as setting up a fund to cover the amount of the fine. It should be noted that insurance products specifically designed to cover such losses have already appeared on the insurance market. Finally, the most effective way to avoid fines is to fully comply with data protection rules.

---

[42] See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/ [downloaded: 5th January 2021].

[43] See: https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_hu

[44] Case no. NAIH/2020/1137, See: https://www.naih.hu/files/NAIH-2020-1137-hatarozat.pdf.

**LIST OF LITERATURE**

[1] CORDEIRO, A. B. Menezes: Civil Liability for Processing of Personal Data in the GDPR. *European Data Protection Law Review (EDPL)*, 5 (4), 492–499, https://doi.org/10.21552/edpl/2019/4/7.

[2] JÓRI András: A Rendelet hatálya. In: *A GDPR magyarázata* (szerk. JÓRI András). Budapest, HVG-Orac, 2018.

[3] European Data Protection Board: *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. See: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf [downloaded: 5th January 2021].

[4] TRULI, Emmanuela: The General Data Protection Regulation and Civil Liability. In: BAKHOUM, Mor – CONDE GALLEGO, Beatriz – MACKENRODT, Mark-Oliver – SURBLYTE-NAMAVICIENE Gintare (eds.): *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?* Berlin–Heidelberg, Springer, 2018, 303–329. https://doi.org/10.1007/978-3-662-57646-5_12.

[5] Article 29 Workig Party: *Guidelines on the application and setting of administrative fines (wp253).* See: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 [downloaded: 5th January 2021].

[6] https://edpb.europa.eu/news/national-news/2021/polish-dpa-id-finance-poland-checking-potential-system-vulnerabilities_hu [downloaded: 5th January 2021].

[7] https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_hu [downloaded: 5th January 2021].

[8] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/ [downloaded: 5th January 2021].

[9] https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_hu [downloaded: 5th January 2021].

[10] https://edpb.europa.eu/news/national-news/2020/300000-sek-fine-against-housing-company_hu [downloaded: 5th January 2021].

[11] https://edpb.europa.eu/news/national-news/2020/norwegian-dpa-fines-odin-flissenter-performing-credit-check-sole_hu [downloaded: 5th January 2021].

[12] https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-aepd-imposes-fine-75000-eur-vodafone_hu [downloaded: 5th January 2021].

[13] https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_hu [downloaded: 5th January 2021].

[14] https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu 600000-fine-google-belgium-not-respecting-right-be_hu [downloaded: 5th January 2021].

[15] https://edpb.europa.eu/news/national-news/2020/lithuanian-dpa-imposes-fine-improperly-processed-personal-data-parents_hu [downloaded: 5th January 2021].

[16] https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_hu [downloaded: 5th January 2021].