EUROPEAN CASE LAW ON THE GDPR VIOLATION BY NATURAL PERSONS

Cornelia Beatrice Gabriela ENE-DINU[(*)]

Abstract

According to the General Data Protection Regulation (GDPR), natural persons can face significant fines if they violate data protection rules while processing personal data outside of purely personal or domestic activities. However, if the data processing is conducted purely for personal or domestic purposes, with no commercial or professional link, GDPR sanctions do not apply. The GDPR allows for hefty fines in cases of non-compliance, with penalties reaching up to 10 million euros or, in severe cases, up to 20 million euros. However, these maximum fines are generally associated with organizations rather than individuals. When determining the amount of a fine, several factors are considered, including: the seriousness of the violation, the degree of fault or negligence, the nature, duration or extent of the breach and the impact on the data subjects affected. Supervisory authorities have discretion when imposing fines and aim to ensure that penalties are proportionate to the specific circumstances of each case. As a result, while the GDPR provides for substantial fines, the actual fines imposed on individuals are generally much lower, and exorbitant fines are unlikely. While the GDPR has stringent provisions for protecting personal data and allows for significant fines in case of violations, the application of these fines to individuals is generally more measured and adjusted according to the specific context of the violation.

Keywords: *natural persons, data processing, violation, consent, case law.*

1. Introduction

Is fining natural persons for GDPR violation, a new reality? When we talk about GDPR we most often think of two things: companies and big fines. Why? Because we are already used to seeing companies all over Europe being fined and we are talking about more than 550 fines totalling more than €260,000,000.[1]

Indeed, natural persons fining for violations of the General Data Protection Regulation (GDPR) is a reality, but it is less common and less publicised than the companies fining. GDPR is about protecting personal data and applies to natural persons as well as companies and organisations. As for natural persons, they can be fined if they violate data subjects' rights[2], such as unauthorised access to personal data, unauthorised disclosure of personal data or other violations of the GDPR. However, fines for natural persons are less common and are more often applied in serious or particularly serious cases. Most of the substantial fines focus on companies and organisations because of the large amount of personal data they process and their impact

[(*)] Lecturer, PhD, Faculty of Law, "Nicolae Titulescu" University of Bucharest, Attorney-at-law – Bucharest Bar Association (e-mail: cdinu@univnt.ro).

[1] For more informations, see GDPR Enforcement Tracker Report, 4th Edition 2023, available at: https://cms.law/en/media/international/files/publications/publications/gdpr-enforcement-tracker-report-may-2023.

[2] N.-D. Ploesteanu, V. Lăcătușu, D. Farcaș, *Protecția datelor cu caracter personal și viața privată*, Universul Juridic Publishing House, Bucharest, 2018, p. 115.

on natural persons. However, it should not be ignored that natural persons can also be fined under the GDPR, especially if violations are significant or repeated.

In compliance with the provisions of art. 4 point 7 of the GDPR: "'*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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*"[3].

Under this regulation, a natural person can also be a controller if he/she becomes a data controller under the GDPR and thus the natural person is responsible for complying with the GDPR provisions regarding the personal data processing. This can occur when a natural person determines the purposes and means of processing the personal data, such as filming an event with a phone and further sharing these images on social media. In this situation, the person filming and uploading the material on social media becomes a data controller and must comply with the GDPR. This involves, among other things, informing the data subjects (e.g. the persons in the images) about the processing of their personal data[4], respecting their rights (such as the right to information and the right to data deletion) and taking appropriate security measures to protect the data. It is important that the natural person who becomes a data controller is aware of his/her responsibilities under the GDPR and ensures that the processing of personal data is lawful and observes the rights of the data subjects.

According to the GDPR, not all the activities carried out by natural persons within their personal scope are subject to the GDPR rules. If the data is processed solely for personal purposes and there is no connection with a professional or commercial activity, then the GDPR rules do not apply.

However, when a natural person uses personal data outside the personal scope, for example for socio-cultural or financial purposes, they must comply with the GDPR. Thus, if a natural person collects, stores or uses personal data for such activities, he/she must ensure that he/she respects the rights of the data subjects, and that the data processing complies with the GDPR rules.

Under these circumstances, each of us can ask the following question: can natural persons be fined for GDPR violations?

Indeed, the natural persons can be fined for violating the GDPR and this is confirmed by fines across the European Union. Thus, we have at least 18 fines applied to operators - natural persons, one of which is applied by ANSPDCP - the Romanian Supervisory Authority.

It is important to note that so far, the European case law on fining natural persons for GDPR violations is not as extensive or detailed as for companies or organisations. However, there are certain main directions in which the National Supervisory Authorities at the EU level have focused on serious violations of the GDPR and the enforcement of fines against natural persons. These main directions include:

1. Monitoring of public space and neighbours' property - if a person films or

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, published in the Official Journal L 119 of May 4, 2016.

[4] R. Ducato, *Data protection, scientific research, and the role of information*, Computer Law & Security Review, volume 37, July 2020, Southampton, United Kingdom, 2020, pp. 1-16.

monitors public space or neighbours' property without their consent or without a proper legal basis, this may be considered a serious violation of the GDPR and may attract sanctions.

2. Surreptitious filming or photography - situations where a natural person surreptitiously films or photographs other natural persons without their consent or without a proper legal basis may be considered serious violations of the GDPR and may be sanctioned accordingly.

3. Disclosure of information on the internet or to third parties - when a natural person discloses personal information of another natural persons on the internet or to third parties without their consent or without a proper legal basis, this can be considered a serious violation of the GDPR and may attract sanctions.

In all of these situations, supervisory authorities have tended to pay close attention to and closely investigate the GDPR violations in the context of public space monitoring, surreptitious filming or photography and unauthorised disclosure of personal information.

2. Criteria for assessing penalties imposed on natural persons at the level of European States - case law

Article 83 para. (2) of the GDPR provides a list of criteria that supervisory authorities should use both in assessing whether a fine should be imposed and in assessing the amount of the fine. This does not imply a new assessment of the same criteria, but an assessment which takes into account all the circumstances of each natural person case in accordance with art. 83.

The supervisory authorities should use these criteria established by the European legislator both in assessing the appropriateness of imposing a fine and in determining its amount. These criteria include, among others:

a. Nature, gravity and duration of the violation: The supervisory authorities should assess the seriousness of the violation and its duration over time.

b. Intention or negligence: It is considered whether the violation was intentional or the result of negligence.

c. Measures taken to remedy the violation: The supervisory authorities may take into account whether the person or entity concerned has taken measures to remedy the violation and to prevent reoccurrence.

d. The degree of responsibility of the concerned natural person or entity: It assesses the level of responsibility of the concerned natural person or entity for the GDPR violation.

e. Any previous history of GDPR compliance: The supervisory authorities may take into account whether the concerned person or entity has had previous violations of the GDPR.

It is important to stress out that the assessment of each natural person case must consider the specific circumstances of the violation and be carried out in accordance with the provisions of the GDPR. Thus, the supervisory authorities must apply the listed criteria appropriately and proportionately to the seriousness and circumstances of each case.

The national procedures and constitutional requirements of some countries may influence how sanctions are assessed and applied under the GDPR. In some countries, the assessment of the existence of a violation may be carried out separately from the assessment of the

sanction to be imposed[5]. This may be determined by the specific legal and constitutional procedures of the concerned country.

For example, in some countries, the process of applying sanctions for GDPR violations may involve several distinct steps, such as identifying and investigating the violation, determining guilt or liability, and then determining and applying the appropriate sanctions. In these circumstances, the content and level of detail of a draft decision issued by the supervisory authority may be influenced by these national procedures and requirements.

It is important that these decisions of the national supervisory authorities observe the principle of proportionality and fairness in the application of sanctions. The supervisory authorities must ensure that their procedures comply with the GDPR requirements and that the taken decisions are justified and in accordance with the law.

To this end, I draw attention to a first case in which the Spanish National Supervisory Authority (AEPD)[6] fined a natural person with EUR 5,300 for illegal camera surveillance. The concerned person had rented two rooms in the operator's apartment. The operator installed a video camera in the apartment and stated that it was installed solely for security purposes and also only monitored the front door area. However, it turned out that such camera was oriented in such a way that it recorded other parts of the apartment, such as the living room. The AEPD states that this constitutes an unwarranted intrusion into the privacy of the data subject without his/her consent.

In reaching this decision, the AEPD considered that, as far as consent is concerned, art. 7 of the GDPR states that "*Where the processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.*".

In compliance with the provisions of art. 4 point 11 of the GDPR, "'*consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

The AEPD also took into account the recital 32 of the GDPR, where it is regulated: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data (...)*".

Thus, it was assessed in the case that the respondent did not demonstrate in its submissions that the applicant has given its consent to the data processing being carried out in the manner referred to in the GDPR.

In this case, the AEPD proceeded to the individualisation of the facts and considered that the imposed fine must be effective, proportionate and dissuasive in each natural person case, in accordance with the provisions of art. 83 para. 1 of the GDPR. It was therefore considered that the penalty to be imposed should be individualised in accordance with the criteria laid down in art. 83 para. 2 of the GDPR, and with the provisions of art. 76 of the Organic Law 3/2018 on the protection of personal data and the guarantee of digital rights (LOPDGDD), in relation to art. 83 para. 2 letter (k) of the GDPR.

[5] D. F. Barbur, *Protectia datelor cu caracter personal. Ghid practic*, *2nd edition*, C.H. Beck Publishing House, Bucharest, 2022, p. 235.

[6] Resolucion de procedimiento sancionador del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes Expediente, No : EXP202300216, available: https://www.aepd.es/documento/ps-00117-2023.pdf.

The nature, seriousness and duration of the offences were taken into account as aggravating circumstances for the individualisation of the penalty [art. 83 para. 2 letter (a) of the GDPR], given that the dwelling is inviolable, and the installation of the cameras implies a significant attack on the privacy of the persons living there. To this end, the right to privacy consists in guaranteeing the free development of one's individual private life without any interference from third parties. The presence of interior cameras does not merely imply excessive control of the entry/exit of the resident and/or his/her companions, but rather data processing that is not justified in this case. Moreover, the installation of a video camera entails the unavoidable obligation to warn of its presence by means of an information device, in a sufficiently visible place, announcing the existence of the surveillance device, the identity of the person responsible for processing the data, as well as the possibility of exercising the rights provided for in art. 22 of the GDPR, obligations which the respondent has not complied with.

In the light of these aspects, the AEPD considered that the presented aspects violated the provisions of art. 6 para. 1 and art. 13 of the GDPR, a violation which entails the commission of two offences considered very serious under art. 72 para.1 of the LOPDGDD, which states that: "Based on what is laid down in art. 83 para. 5 of Regulation (EU) 2016/679, acts involving a substantial infringement of the articles mentioned therein shall be considered as very serious (...) and in particular: b) Processing of personal data without any of the conditions for lawful processing laid down in art. 6 of Regulation (EU) 2016/679. (...) h) Omission of the obligation to inform the data subject about the processing of his/her personal data in accordance with the provisions of articles 13 and 14 of Regulation (EU) 2016/679 and 12 of this Organic Law. (...)".

For all these reasons, it is considered that the appropriate sanction is an administrative fine and the obligation to uninstall any type of device inside the dwelling, stressing that the dwelling is a space reserved for the privacy of natural persons, who can carry out their personal activities there, free from any type of surveillance affecting privacy in the broadest sense.

Another case[7] involving a natural person in Austria is based on the following situation: the defendant was the mayor of a town in Austria and a sales representative of a company. In this capacity, the defendant regularly made home visits to customers in connection with the extension of the heating network and to deliver commercial offers. After a meeting on January 13, 2023, the defendant saved on his private mobile phone the name and phone number of a natural person to send him political advertisements on his behalf at a later date for the 2023 Lower Austrian state elections. At the same time, the plaintiff also saved the names and telephone numbers of six other people, whose contact details he provided to the company he worked for as a sales agent. On 25 January 2023 and 26 January 2023, the defendant sent an SMS message to three mobile phone numbers collected in the run-up to the 2023 Lower Austrian state elections. The data subjects did not consent to their personal data being stored by the defendant on his private mobile phone for the purpose of future political advertising.

[7] Data Protection Authority - Austria, File No. 2023-0.404.421, decision of 16 June 2023, available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20230616_2023_0_404_421_00/DSBT_20230616_2023_0_404_421_00.html.

The defendant subsequently deleted the contact details from his private mobile phone.

The Authority considered that the material scope of the GDPR under art. 2 of the GDPR was undoubtedly fulfilled in this case. The defendant did not object that the GDPR would not apply especially since the processing for private purposes provided for in art. 2 para. 2 letter (c) of the GDPR is not fulfilled because the processing of data by the plaintiff took place in connection with his or her professional activity, according to the recital (18) of the GDPR.

The GDPR defines the term "processing" in art. 4 para 2 by listing a number of possible ways of using personal data: collecting, recording, organizing, arranging, storing, adapting or altering, reading, querying, using, disclosing by transmission, distribution or any other form of provision, deletion or destruction. By saving the contact details of the data entered in his private mobile phone with a view to transmitting them at a later date political advertisements, the defendant processed personal data as a responsible person within the meaning of art. 4 para 2 of the GDPR. Regarding the requirements for lawful data processing, art. 6 of the GDPR states that the processing of personal data is lawful only if at least one of the conditions listed in its content is met. In this regard, it is important that data controllers can demonstrate that the processing complies with at least one of these legal grounds in order to comply with the GDPR and ensure the lawfulness of the personal data processing.

In the present case, it was only the justification under art. 6 para. 1 letter (f) of the GDPR. There was no consent from those affected for the defendant to save the contact details on his private mobile phone. During the trial, the defendant did not invoke any other justification. Accordingly, the Authority has examined the existence of legitimate interests of the defendant or third parties within the meaning of art. 6 para. 1 letter (f) of the GDPR. Therefore, art. 6 para. 1 letter (f) of GDPR allows processing under three cumulative conditions: (i) the pursuit of a legitimate interest; (ii) the necessity of the processing; and (iii) the absence of an infringement of the rights and freedoms of others[8]. It was found that the plaintiff's interest in collecting the contact details of those affected was to "expand his circle of acquaintances" and subsequently generate more preferential votes for the state elections in Lower Austria. If it is assumed that the data processing carried out is necessary to achieve this purpose, the interests of the data subjects are overridden. Because of their relationship with the defendant, they could not reasonably expect him to provide their contact details, which they provided to him only in his capacity as an employee of a company, which he subsequently saved on his private mobile phone, and they could in no way foresee that the contact details they provided would be used by the defendant for a completely different purpose - namely to contact them for political purposes.

After having analysed the interests of the data subjects, the Authority concluded that the notion of privacy and the fundamental rights of the data subjects (the right to observe the private and family life and the right to protection of personal data) override the interests of the defendant. As a result, the legal basis invoked by him as a basis for processing personal data of data subjects is not appropriate for the specific processing. No other legal basis under art. 6 para 1 of the GDPR is possible and has not been invoked by the defendant. According to art. 5 para. 1 letter (b) of the GDPR, personal data must be collected for specified, clear

[8] ECJ Judgment of 11 December 2019, Case C-708/18, para 36 with further references.

and legitimate purposes and may not be further processed in a manner incompatible with those purposes ("purpose limitation"). This is correct, according to art. 6 para. 4 of the GDPR, when processing personal data for a purpose other than that for which they were originally collected, an assessment of the compatibility between the original purpose and the further purpose of the processing is required.

This assessment should include the following aspects: the connection between the initial and further purposes of the processing of personal data; the context in which the personal data were initially collected, including the relationship between the data subjects and the controller; the type of personal data involved in the initial and further processing; the consequences of the intended further processing for the data subjects; whether there are adequate safeguards in both the initial and intended further processing operations. This assessment must be carried out to ensure that the further processing of the data is compatible with the original purposes and that the fundamental rights and freedoms of the data subjects are respected. In the analysis carried out by the Authority, it was ruled that further processing of data is not allowed if there is no compatibility between the original and further purposes or if there is no adequate legal basis for further processing under the GDPR.

Against the background of the described facts, the Authority found that the defendant processed personal data unlawfully and without a legitimate purpose, contrary to art. 5 para. 1 letters (a) and (b) and art. 6 paras. 1 and 4 of the GDPR. This means that the objective side of the offence is fulfilled. From a subjective point of view, it is worth noting in the present case that, because of the deliberate storage of contact data for future contacts for political elections, it can be assumed that the defendant intentionally carried out the processing in question. Therefore, on the subjective side of the offence there is intent within the meaning of art. 83 para. 2 letter (b) of the GDPR.

The sentence assessment within a statutory sentencing framework is a discretionary decision that must be made in accordance with the criteria set out by the legislator. The basis for determining the penalty is the significance of the legal interest protected by the law and the intensity of the damage to this interest by the offence. Possible aggravating and mitigating circumstances must also be weighed against each other. Particular attention should be paid to the extent of the damage. In view of the nature of criminal administrative law, which under Austrian law is the legal branch of the law governing offences that violate the provisions of the GDPR, sections 32 to 35 of the Criminal Code apply *mutatis mutandis*. The defendant's income and financial circumstances and any maintenance obligations should be taken into account when setting fines. If a fine is imposed on an natural person, an alternative custodial sentence must also be imposed if it cannot be collected.

Regarding the facts of the case, the Authority took into account the following mitigating circumstances when setting the penalty: the absence of a criminal record and the active participation of the defendant in the proceedings conducted by the Authority. It was positively assessed that the defendant responded in a timely manner to the Data Protection Authority's requests in the administrative criminal proceedings, admitted to the Data Protection Authority that he sent the messages, cooperated with the Authority and confessed to the alleged offences. Moreover, by his confession, the defendant admitted the unlawful nature of his offence, which contributed to the individualisation of the sentence. Under art.

83 para. 1 of the GDPR, the supervisory authorities must also ensure that fines are effective, proportionate, and dissuasive in each individual case. In the light of the above, the fine imposed by the Authority of EUR 1,000 appears to be proportionate to the seriousness of the offence, having regard also to the limits of the penalty laid down in art. 83 para. 5 of the GDPR, in conjunction with the defendant's income and financial circumstances in accordance with the offence and guilt.

3. Conclusions

The right to privacy is a fundamental concept in the field of human rights and refers to the right of a natural person to protect his/her privacy, identity and personal space from unwanted or intrusive interference by other natural persons, organisations or government authorities. This right is recognised in numerous constitutions and international human rights documents. The data protection scope gives effect to existing national and international data protection regulations.

While the main actors in violations of personal data protection regulations are legal persons or governmental organisations, there is now a growing trend to hold natural persons also accountable for interfering in the private lives of the others. In European countries, there is a growing concern among national data protection authorities to make people more responsible for respecting the privacy and private lives of the others[9].

This trend is accentuated by technological progress, which generates increasingly dangerous social situations for the privacy of the natural person. Technological developments, particularly in communications and the internet, have made it easier for personal information and data to be accessed, stored and distributed. This has led to increased concerns about the privacy and security of the personal data. The widespread use of social media and other online platforms has increased the exposure and vulnerability of natural persons to intrusions into their privacy, such as unauthorised access to personal information or the indiscriminate sharing of images and other private data.

A growing awareness of the importance of protecting privacy and individual rights has increased pressure on institutions and natural persons to be more responsible in managing personal information and observing the privacy of the others[10]. In this context, there is a trend towards stronger regulatory and enforcement mechanisms to counter privacy violations and to establish clear responsibilities and consequences for those who commit them. The effectiveness of these mechanisms is evidenced by a growing body of case law in the area of holding natural persons liable for violations of the social values covered by personal data protection law.

References

- Barbur, Diana Flavia, *Protectia datelor cu caracter personal. Ghid practic, 2nd edition*, C.H. Beck Publishing House, Bucharest, 2022.
- Ducato, Rossana, *Data protection, scientific research, and the role of information*, in ”Computer Law & Security Review”, volume 37, July 2020, Southampton, United Kingdom, 2020.

[9] N.-D. Ploeșteanu *et alii*, *op. cit.*, p. 127.
[10] D. F. Barbur, *op. cit.*, p. 244.

- Ploesteanu, Nicolae-Dragoș, Lăcătușu, Vlad, Farcaș, Darius, *Protecția datelor cu caracter personal și viața privată*, Universul Juridic Publishing House, Bucharest, 2018.
- GDPR Enforcement Tracker Report, 4th Edition 2023, available at: https://cms.law/en/media/international/files/publications/publications/gdpr-enforcement-tracker-report-may-2023.
- 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, published in the Official Journal L No 119 of May 4, 2016.
- Data Protection Authority - Austria, File No. 2023-0.404.421, decision of 16 June 2023, available at https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20230616_2023_0_404_421_00/DSBT_20230616_2023_0_404_421_00.html.
- Resolucion de procedimiento sancionador del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes Expediente N. º: EXP202300216, available at https://www.aepd.es/documento/ps-00117-2023.pdf.
- ECJ Judgment of 11 December 2019, Case C-708/18, available at https://curia.europa.eu/juris/liste.jsf?language=en&num=C-708/18.
- The CMS Law, GDPR Enforcement Tracker, available at https://www.enforcementtracker.com/.