UNIO - *EU Law Journal*. Vol. 4, No. 2, July 2018, pp 99-104.

School of Law – University of Minho

The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint

Pedro Miguel Freitas*

ABSTRACT: The aim of this paper is to analyse the punitive regime foreseen in the 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 (GDPR). The administrative fines' regime found in Article 83 of the GDPR and some of the questions it arises will be explored. We conclude that the Member States should adopt a critical stance when adapting their national legislation to the norms of the GDPR. The fundamental principles enshrined in national constitutions and supranational legal texts must be closely analysed and observed since the GDPR introduces a mandatory sanctions framework.

KEYWORDS: GDPR – sanctions – fines – sentencing – data protection.

* Professor at the School of Law of the University of Minho.

I. Introductory remarks

Though published on 4 May 2016, the 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 (GDPR), has been applicable since 25 May 2018. A deep concern about the practical consequences of its application has grown in Portugal[1], particularly as to the obligations arising from it and the consequences of its non-compliance.

II. Penalties' legal framework: a panorama

Article 84 of the GDPR is entitled *"Penalties"*, which could lead a more incautions reader to think that the penalties are to be found only in this Article. This could not be further from the truth. An understanding of what is at issue here means at least a combined reading of Articles 58, 83 and 84 of the GDPR. Let us start with Article 83 of the GDPR.

Article 83 (4), (5) and (6) lists the acts that might lead to the imposition of an administrative fine:

1. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

2. the obligations of the certification body pursuant to Articles 42 and 43;

3. the obligations of the monitoring body pursuant to Article 41(4);

4. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

5. the data subjects' rights pursuant to Articles 12 to 22;

6. the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

7. any obligations pursuant to Member State law adopted under Chapter IX;

8. non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1);

9. Non-compliance with an order by the supervisory authority as referred to in Article 58(2).

This Article does not, however, exhaust the hypotheses that generate responsibility, especially those that amount to a criminal nature intervention, legal domain that the Regulation does not deal with exhaustively. The reading of Article 84 is insufficient and it is not clear whether criminal law can be used to penalize the most serious breaches of the GDPR rules. Indeed, what is said in this Article is simply that "*Member States shall*

[1] According to Article 288 TFEU, the Regulation shall have general application and be binding in its entirety and directly applicable in all Member States. As stated by João Mota de Campos, João Luís Mota de Campos and António Pinto Pereira, *Manual de Direito Europeu* (Coimbra: Coimbra Editora, 2014), 313 and ff., a regulation has a general application because it does not specify, in the sense of individualizing, the recipients of the norms it provides. It is binding in its entirety inasmuch as it imposes compliance with all provisions, including their method of application and enforcement, on all addressees - from the European Union itself to the individual citizen. In those cases, in which the Regulation is a complete legislative act, and does not require a national rule to address matters that have been omitted, its legislative power is felt autonomously without the legislative intervention of the Member States. The national action for the implementation of the Regulation in the national legal order is not necessary. Therefore, the effect of direct applicability to the Regulations is usually pointed out. On the date of its entry into force, it shall automatically be incorporated into national law.

lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 7983, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive" (sic).[2]

This leaves some scope of action, undesirable, albeit needed to accommodate all the national legal orders' idiosyncrasies, as it may lead to discrepancies in the legal treatment of the same situations depending on the Member State concerned.

A deeper understanding of the scope of this Article is not found in other Articles of this Legislative Act, but rather in its Recitals, in particular 148 and 149. The first one, aiming at the strong enforcement of the rules of the GDPR, introduces the obligation to impose penalties including administrative fines "*for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation*". In turn, Recital 149 goes on to say that "*Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation*".

Articles 83 and 84 and Recitals 148 and 149 pave the way to the following reasoning: the response to breaches of the provisions of the GDPR is not limited to administrative fines and corrective measures, but also includes criminal sanctions. In addition, Recital 152 states that "*[w]here this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law*".

In sum, the expression "*penalties*", although absent from Article 83, includes both criminal penalties and administrative fines. It should be emphasized, however, that in the Portuguese version of the GDPR, two expressions are used interchangeably as if they were the same and may cause some confusion: "*sanções administrativas*" (administrative sanctions) and "*coimas*". This is of major importance for the Portuguese legal landscape because "*coimas*" refers to a specific legal domain different from the Administrative Law. It is akin to the German "*Ordnungswidrigkeitenrecht*" and shares many of its fundamental principles and guarantees with Criminal Law and Criminal Procedure. Different from some other European countries, *e.g.* Spain, the Portuguese legal framework attributes theoretical and practical autonomy to a legal domain coined "*Direito de Mera Ordenação Social*", in which we find the "*coimas*", one domain that is different from Administrative Law and Criminal Law, and, as the latter, has a punitive role.[3]

Putting aside the terminological confusion between administrative sanctions and "*coimas*"[4] which occurs throughout the Regulation and whose explanation can be found in the legal idiosyncrasies of the Member States – not perceiving law in a single and unanimous fashion – sometimes lending it an administrative character, other times recognizing its autonomy from other legal branches, it is apparent that the Member States, in accordance with their own legal tradition, have, at least, the possibility of

[2] In the Portuguese version of the Regulation there is a mention to Article 7983 which is obviously a typo left untouched in the Corrigendum to 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, of 23 of May 2018. The English, French, Spanish and German versions, to name a few, do not have the same problem, and simply refer to Article 83 of the GDPR.

[3] Mário Ferreira Monte, *Lineamentos de Direito das Contraordenações* (Braga: AEDUM, 2014), 49-50.

[4] See recitals no. 149, 150, 152 and Articles 58 (2)(i) and 83.

punishing infringements of the GDPR with administrative fines ("*coimas"* in the Portuguese case) or criminal penalties.

In the current moment, Portugal does not have a revised law that accommodates the changes brought by the GDPR. The law in place is Law No 67/98 of 26 October (Law on the Protection of Personal Data), as amended by the Law No 103/2015 of 24 August, which is still applicable. In the rules therein, a number of crimes are foreseen: "*non-compliance with data protection obligations*" (Article 43), "*improper access*" (Article 44), *"manipulation or destruction*" (Article 45), *"insertion of false data*" (Article 45-A), "*qualified disobedience*" (Article 46) and *"breach of confidentiality*" (Article 47). "*Coimas*" are foreseen from Articles 35 to 42.

III. Recipients of the penalties

Article 83 of the GDPR distinguishes the amount of which fine depending on whether they apply to an undertaking or not. In the case of Article 83 (4), the fine is limited to a maximum of EUR 10 000 000 or, in the case of an undertaking, 2% of its worldwide annual turnover of the preceding financial year, whichever is higher. In nos. 5 and 6 the amount of the fine is increased up to EUR 20 000 000 or, in the case of an undertaking, 4% of its worldwide annual turnover of the previous financial year, whichever is higher.

The GDPR does not give a definition of undertaking. We might resort to Article 4 (18) where the definition of enterprise is detailed as a *"natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity"*, yet this would lead us to an incoherent and illogical Article 83. If the term *"undertaking"* is to be used in the sense given in Article 4 (18), whenever we had a case of a group of undertakings – defined by Article 4 (19) as *"controlling undertaking and its controlled undertaking"* – it would not be completely covered by Article 83. Applying Article 4 of the GDPR blindly could lead to absurd results, namely that the fines applicable to enterprises are calculated either in percentage terms of their worldwide turnover - up to 2% or 4% - or taking as a maximum 10 or 20 million euros[5], depending on the criterion leading to the highest amount, while a group of undertakings might be exempt from a calculation on the basis of their worldwide turnover.

Concerning this problematic issue, Recital 150 sought to alleviate possible hermeneutical difficulties by stating that *"[w]here administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine".*

It is essential to underline the opinion of the CJEU on the concept of an undertaking in accordance to Articles 101 and 102 TFEU. In the view of the CJEU,

[5] For José Lobo Moutinho, "Legislador português precisa-se: algumas notas sobre o regime sancionatório no Regulamento Geral sobre a Protecção de Dados [Regulamento (UE) 2016/679]", *Fórum de Protecção de Dados* 4 (2017): 50, "*the coima* ["fine"] *applicable to undertakings has as a maximum a percentage of total worldwide annual turnover of the preceding financial year*" (free translation). In our mind, such a reasoning empties of meaning the expression found at the end of Article 83(4) (5) and (6): "whichever is higher". The correct interpretation is that we are before an alternative in the case of undertakings: the fine applicable is the one which is higher, either using the criteria found in the beginning of Article 83(4) (5) and (6), or using the criteria found in the end of the said article.

"every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed…"[6] or *"an economic unit even if in law that economic unit consists of several persons, natural or legal"*.[7] It seems that the GDPR might benefit from a more precise definition of the recipients of the fines, especially concerning the sensitivity of this matter.

IV. The administrative fine's range

We have pointed out above that the upper limit of the fine applicable under Article 83 of the GDPR is EUR 10 000 000 or, in the case of an undertaking, 2% of its worldwide annual turnover of the previous financial year, depending on whichever is higher. In the most serious cases, the fine's amount shall be up to EUR 20 000 000 or, in the case of an undertaking, up to 4% of its annual worldwide turnover of the preceding financial year, whichever is higher. No minimum limit is mentioned, leaving the definition of the exact amount of the fine for the supervisory authority. To achieve this, the authority must appraise the circumstances of the individual case, having as a reference factors such as the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement or the categories of personal data affect, among other factors described in Article 83(2).

This model of determination of the administrative fine is characterized by its discretion. The supervisory authority must impose a fine within the range stated in the GDPR by measuring the aggravating or mitigation effect of certain circumstances. The GDPR introduces a high level of discretion that should have been accounted for, either by establishing more than two levels of gravity of the infringement of the GDPR and consequent administrative fines or by opting for a sentencing model that assures increased certainty to the detriment of flexibility. Implicit in the GDPR is the adoption of a sentencing guidelines model, which is highly flexible and guides by words[8], instead of a more numerical and prescriptive model commonly found in common law countries. This guidance by words is not unknown in Portugal given that Article 71 of the Portuguese Penal Code adopts it, and so it is subject to the same flaws, namely the lack of a structured approach to the task of assessment of the more just amount of fine in the individual case.

It should be noted here that, as it is constructed and proposed in the GDPR, this sentencing model raises serious doubts as to its compatibility with fundamental principles found in the constitutional texts of the Member States and in the supranational legal instruments in the field of protection of human rights, namely the principles of legality and certainty. The *"Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679"*, adopted on 3 October 2017, by Article 29 Data Protection Working Party are welcomed but not enough.[9]

V. Concluding remarks

The aim of this paper was to briefly analyse the punitive regime foreseen in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April

[6] Judgement *Höfner and Elser*, Case C-41/90, para. 21, ECLI:EU:C:1991:161.
[7] Judgement *Confederación Española de Empresarios de Estaciones de Servicio*, Case C-217/05, para. 40, ECLI:EU:C:2006:784.
[8] Julian V. Roberts, "Structured sentencing outside the United States", *Encyclopedia of criminology and criminal justice*, ed. Gerben Bruinsma and David Bloomfield (New York: Springer, 2013): 5081-82.
[9] See http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). Some important questions concerning the sanctions' regime of the GDPR are still unsolved and will undoubtedly sparkle the attention of the national lawmakers, scholars, and all stakeholders. The precise definition of the recipients of the administrative fines, the nature of the fines (quasi-criminal or administrative) and the choice of a sentencing model that is adequate for purposes of the principles of legality and certainty, are questions that must not be neglected since punitive sanctions meddle with fundamental principles and guarantees that sculpt the very foundations of a democratic State governed by the Rule of Law.