COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

DELIBERATION/2019/494

Whereas 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 (General Data Protection Regulation, hereinafter GDPR), pursuant to Article 288(2) of the Treaty on the Functioning of the European Union (TFEU), *'shall* be *binding in its entirety and directly applicable in all Member States'."*

Considering that, as the European Commission recalls in its Communication to the European Parliament and the Council of January 24, [20181], the GDPR creates a duty for Member States to *'take the necessary measures to adapt their national ¡ 9i"slaçôes",* as well as "the *possibility of further specifying the application of data protection rules in certain areas",*

Considering that, as the European Commission states in the same document, the actions of the Member States in this context are framed by "[...] *-*"9 **. of the Charter, which means that any national law aimed at specifying must meet the requirements of Article 8 of the Charter (and the re9-%--enio based on Article 8.^ of the Charter}, and [...] Article 16. Article 16(2) of the TFEU, under which national legislation may not interfere in the free movement of personal data within the EU",*

Whereas, as the European Commission states, when Member States adapt their national legislation, *'[...]* they *must take into account the fact that any national measures which result in the creation of an obstacle to the daily applicability of the Regulation and jeopardize its simultaneous and uniform application throughout the EU are contrary to the Treaties',*

Considering that the Court of Justice of the European Union (CJEU), in the *Costa/ENEL* judgment (Case No. 6/64), stated that that provision of the treaties *'[...] would be excluded from its meaning if a State could, unilaterally, annul its effects by means of a legislative act opposing the Community texts'.* And that, in the

1http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN

Variola (Case No. 34/73), the same court was also very clear in stating that "Member States have a duty not to obstruct the direct applicability inherent in the Regulations, and strict compliance with this obligation is an indispensable condition for uniform and simultaneous application of the Regulations throughout the Community";

Considering also that, as the European Commission insists, "[...] the national legislator may not copy the text of the regulation when this is not necessary in the light of the criteria laid down in the case law, nor interpret it or add additional conditions to the rules directly applicable under the regulation";

Whereas the principle of sincere cooperation, enshrined in Article 4(3) of the Treaty on European Union, implies a duty for all authorities of the Member States to take general or special measures to ensure fulfilment of the obligations imposed by Union law;

Whereas Union law presupposes that the GDPR is applied uniformly in the territory of the Member States, in order to guarantee the free movement of data, with cooperation and coherence mechanisms whose effectiveness depends on the unity of the legal regime in the context of data processing that has an impact on the territory of more than one Member State;

Considering that the national adoption of legal rules that contradict the provisions of the GDPR not only violates the principle of the primacy of Union law (CJEU judgment, Simmenthal, Proc. 106/77, § 21), but also seriously undermines the proper functioning of the coherence mechanism, putting the respective national authority at risk of violating one of the rules in antinomy;

Considering also that it follows from the principle of primacy that, in addition to national courts, administrative bodies are also obliged to disapply national rules that contradict European Union law, as the CJEU expressly ruled in the Fratelli Costanzo[2] judgment, which bound all public administration bodies to the duty to apply European Union law in full, ruling out the possibility of applying EU law.

---

[2] Judgment of June 2, 1989, Case No. 103/88, paragraphs 32-33.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

national provisions which constitute an obstacle to the full effectiveness of the rules of that law[3];

Considering also that Article 8(4) of the Constitution of the Portuguese Republic (CRP) states that the provisions of the treaties governing the European Union and the rules emanating from its institutions, in the exercise of their respective competences, shall apply in the internal order, under the terms defined by Union law, with respect for the fundamental principles of the democratic rule of law;

Considering that the CNPD drew attention to these aspects in its Opinion No. 20/2018, of May 2, 2018, which it issued on Draft Law No. 120/XIII/3.ª , which *"ensures the implementation, in the national legal order, of Regulation (EU) 2016/6/9, concerning the protection of individuals with regard to the processing of personal data and the free circulation of such data", and* listed, with reasons, the set of rules it considered likely to violate European Union law and, in particular, the GDPR^;

Considering, finally, that Law No 58/2019 of August 8 maintains some of the rules then identified as violating EU law, and that among these, there are rules whose final wording does not allow them to be saved from such a judgment through a corrective interpretation in line with EU law, as the antinomy with the rules of the GDPR and the Charter of Fundamental Rights of the European Union is insurmountable,

And without prejudice to the other comments made in the aforementioned opinion on other articles of the same draft law,

AGNPD resolves:

a. Fix o understanding that that certain rules of this law are manifestly incompatible with EU law, focusing for the time being on its

---

See also the judgment of the CJEU, *Ciola, of* April 29, 1999, Case C-224/97, paragraphs 30-32; the judgment in 1a/sy, Case C-118/00, of June 28, 2001, and the judgment in C/6, of September 9, 2003, Case C-198/01, paragraphs 48-50 and 55-56. *See* also, in national case law, the judgment of the Central Administrative Court (Norte) of July 2, 2015, Rapporteur Hélder Vieira, Case No 00462/06.2BEPRT.

[4] Opinion accessible at https://www.cnpd.pt/bin/decisoes/Par/40_20_2018.pdf

attention to those provisions which, due to their relevance and frequency of application, call for the formal adoption of such an understanding;

b. That, on the basis of the principle of the primacy of European Union law, and the other arguments set out below, it will disapply the following provisions of Law no. 58/2019, of August 8, in future cases that it may examine, relating to data processing and the conduct of the respective data controllers or processors[5]:

1. Article 2(1) and (2)

Article 2(1) of Law 58/2019 extends the scope of the law to all "[...] processing of personal data carried out in national territory [...], with all the exclusions provided for in Article 2 of the GDPR applying", with paragraph 2 adding that: "This law shall apply to the processing of personal data carried out outside national territory when: a) they are carried out within the scope of the activity of an establishment located in national territory; [...]".

However, even assuming that the definition of the territorial scope of application of national law follows the criteria defined in Article 3 of the GDPR, the truth is that the terms in which this definition is expressed compromise the application of procedural rules and the distribution of competence between the national supervisory authorities of the Member States, whenever cross-border processing is involved[6].

In fact, if the person responsible (or the subcontractor) has more than one establishment in the Union, Article 56(1) of the GDPR determines which national authority is competent to conduct the procedure and issue the final decision, in order to guarantee the functioning of the one-stop-shop mechanism on which the distribution of competences between the supervisory authorities of the Member States of the Union is based. E

[5] Henceforth, Law no. 58/2019.

[6] See the definition in Article 4(23) of the GDPR.

this lead supervisory authority cannot fail to take into account and therefore apply the respective national law'.

To that extent, since the lead supervisory authority corresponds, by rule, to the authority of the Member State in which the main *establishment is* located, the criterion of territorial application of Portuguese law to processing carried out on national territory, when it concerns the activity of a main establishment located in the territory of another Member State of the Union, would in principle be incompatible with the rule deriving from Article 56(1) of the GDPR. The same applies to the criterion of the application of Portuguese law to processing carried out in the context of the activity of an establishment located in Portugal when this is not the principal establishment of the person responsible.

For similar reasons, although now by reference to the territory where the representative of the person responsible is located, paragraph 2(*b)* also compromises the application of the one-stop-shop scheme provided for in Article 56 of the GDPR.

In addition, Article 3(3) of the GDPR also stipulates that it applies to the processing of personal data by controllers established outside the EU where the law of the Member State applies by virtue of public international law.

This means that the GDPR must be applied to all processing of personal data carried out in Portuguese embassies and consulates, but also in other places where, under international public law, the Portuguese state exercises its sovereignty, such as ships and aircraft.

To this extent, the delimitation of the application of the law to processing *that affects data registered in consular posts* and only concerning Portuguese citizens, contained in the

---

[7] In fact, the statement that, in relation to cross-border processing of personal data, the applicable national law is established according to the national supervisory authority competent to conduct or lead the decision-making procedure provided for in Article 60 of the GDPR, follows from logo, that such law must be applied to identify who is the national supervisory authority of the Member State where the controller or processor has its main establishment, in order to understand who can exercise, in the specific case, the powers provided for in Article 58 of the GDPR.

[8] *See the* exceptions provided for in Article 56(2) of the GDPR.

See the definition of main establishment in Article 4(f&/) of the GDPR.

Article 2(2)(c) of Law no. 58/2019 is incompatible with the GDPR, as it does not ensure the application of the GDPR under the terms and with the scope imposed by it.

Therefore, in order to ensure the full effectiveness of EU law, in particular the provisions of Article 56 and Article 3(3) of the GDPR, the CNPD will disapply Article 2(1) and (2) of Law 58/2019 in future cases that it examines, as they are incompatible with the provisions of the law and compromise the useful effect of the GDPR.

2. Article 20(1)

Article 20(1) states that "[t]he rights of information and access to personal data provided for in Articles 13 and 15 of the GDPR may not be exercised where the law imposes a duty of secrecy on the controller or processor which is enforceable against the data subject himself".

When analyzing this provision, it is important to differentiate between the rights in question.

As for the right to information, and only in the case of indirect collection of personal data, it is Article 14 of the GDPR that defines the cases in which it can be restricted, specifying, in paragraph 5(d), the legally established duty of secrecy. Thus, in this regard, as Article 14(5)(d) of the GDPR already regulates the restriction of the right to information in the face of a legal duty of secrecy, the rule in Article 20(1) adds nothing, and therefore has no independent legal relevance in relation to the provisions of the GDPR.

With regard to the right to information in the context of the collection of data directly from the data subject and also with regard to the right of access, and since Articles 13 and 15 of the GDPR do not provide for or legitimize any limitations, a restriction can only occur under the terms of Article 23 of the GDPR.

The latter article allows for the possibility that Member States may "limit by legislative measure the scope of the obligations and rights provided for in Articles 12 to 22, but only provided that such limitation respects the essence of fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society" to ensure a wide range of purposes listed in paragraph 1 of the same article. However, the provisions of Article 20(1) of Law 58/2019 do not

logo specifies the purpose or purposes it aims to safeguard. Furthermore,
does not comply with any of the requirements of Article 23(2) of the GDPR.

Since it is clear that the legislative measures referred to in Article 23 of the GDPR relate to legislation that specifically regulates certain data processing (since it requires, inter alia, that explicit provisions be included regarding the purposes of the processing, the categories of personal data processed, the identification of the controllers and *the scope of the limitations imposed),* any legal limitation on the exercise of rights, in particular the exercise of a fundamental right such as the right of access, recognized independently in Article 8(2) of the Charter of Fundamental Rights and Article 35(1) of the CRP, can never result from the content of a rule such as Article 20(1) of the GDPR." of the Charter of Fundamental Rights and in Article 35(1) of the CRP, can never result from the content of a rule such as Article 20(1) of national law. Nor can the provision in
Article 20(2) of the right to request an opinion from the CNPD makes it possible to remedy non-compliance with Article 23 of the GDPR.

Therefore, in order to ensure the effectiveness of the GDPR, in particular the rights of data subjects, and in contravention of the rules of Articles 13 and 15 of the GDPR and Article 8(2) of the Charter of Fundamental Rights, without respecting the provisions of Article
23 of the same EU law, the CNPD will disapply Article 20(1) of Law 58/2019 in the specific situations it assesses.

3. Article 23D

Article 23(1) admits that the processing of personal data by public bodies may be carried out for purposes other than those which justified the collection of the data, stating that "[...] *is exceptional in nature and must be duly substantiated with a view to ensuring the pursuit of a public interest which cannot otherwise be served, in accordance with Article 6(1)(e) and (4) and Article 9(2)(p) of the GDPR".*

This legal provision is supported by various rules of the GDPR, which, however, as will be explained below, do not give the Member State the power to admit deviations from the purpose of processing in a generic and permanent manner.

In fact, the GDPR regulates the re-use of personal data for purposes other than those that justified its collection in Article 6(4), which, despite the systematic insertion of the precept, also applies to special data (because only then does the reference in point c) to such categories of data make sense). And it follows from this precept that there may be provisions of national or EU law providing for this re-use of data, but only "[...] if they constitute a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR".

However, Article 23(1) of Law 58/2019 does not specify public interest purposes that may justify such reuse, but rather extends this possibility to the pursuit of any public interest, thereby contradicting or failing to comply with the first part of Article 6(4) of the GDPR. It also fails to prove to be a necessary and proportionate measure, because this requires analysis and consideration for each new purpose (cf. recital 50, §3 of the GDPR).

Not being covered by the first part of paragraph 4 of this article, the national legal rule in question cannot, under the terms of the GDPR, attest or recognize in the abstract the non-incompatibility of the purposes (original and reuse), when the rule of Union law requires the controller, in concrete terms, to make such a weighting in the light of the criteria provided for in points a) to e) of the same paragraph 4 of article 6.

It should also be added that this rule, by admitting that personal data can be processed by public entities for any purpose other than the original one, contradicts the principle of purpose or purpose limitation, explained in Article 5(1)(b) of the GDPR - and, from the outset, enshrined in Article 8(2) of the Charter of Fundamental Rights of the European Union, as well as in Article 5(b) of the Convention.
108 of the Council of Europe - as it rules out a concrete and considered assessment of the compatibility of objectives. It should be noted that the requirement for a statement of reasons referred to in Article 23(1) of the Law is not attributed to such a judgment, but rather seems to refer to the impossibility of safeguarding the public interest in any other way.

As for the references to Article 6(1)(e) and Article 9(1)(g) of the GDPR, they can only be understood in the light of the provisions of Recital 50 of the GDPR, which reads: If the processing is necessary for the performance of a task

of public interest or in the exercise of public authority vested in the controller, Union or Member State law may determine and define the tasks and purposes for which the further processing is to be considered valid. Quite simply, a rule of EU or national law must, as can be read from it, lay down the specific tasks and purposes which the further processing is intended to pursue, which the rule in Article 1(1) of the Directive does.
23 of Law 58/2019 does not.

In short, the provisions of Article 23(1) contravene the principle of purpose, enshrined in Article 5(1)(*b) of* the GDPR, and do not comply with the requirements imposed by Article 6(4) of the GDPR on legal rules that provide for the re-use of data, which, in order to ensure the full effectiveness of the GDPR, will be disapplied by the CNPD.

Since Article 23(2) of Law No 58/2019 provides for a similar regime for the transmission of personal data between public bodies for purposes other than those determined by the collection, which corresponds to a data processing operation, the same grounds now set out lead to the same judgment of violation of the GDPR and, therefore, to the conclusion of its disapplication.

4. Article 28º , paragraph 3, point p/

Article 28(3) states that *'[w]ithout a legal provision to the contrary, the consent of the user does not constitute a legal requirement for the processing of his or her personal data. a} If the processing results in a legal or economic advantage for the user [...]'.*

Article 4(f) of the GDPR requires that consent, in order to be legally relevant and thus correspond to the lawfulness of data processing, must be free, so only when conditions guaranteeing the data subject's freedom of expression of will are met can it be considered. Certainly, as is recognized in recital 43 of the GDPR, "[...] *in specific cases where there is a manifest desire between the data subject and the data controller, consent should not be considered as a valid basis for the lawfulness of data processing".*

Despite admitting the non-equal nature of the employment relationship, it follows from the principle of the dignity of the human person that the individual needs to be recognized, even in the context of legal relationships in which, as a rule, he lacks protection in relation to the other party, the minimum of free will to enjoy his fundamental right to informational self-determination - therefore, in the jus-fundamental dimension of control of the data concerning him - recognized in article 35 of the CRP and in article 8 of the Charter of Fundamental Rights of the European Union.

It is in this same vein that the Art. 29 Working Party (WG29) and the European Data Protection Board have taken the view, while rejecting the legal relevance of workers' consent as a rule, that workers can only give their consent freely in exceptional circumstances, when the act of giving or refusing consent does not produce any negative consequences[10].

However, the provisions of Article 28(3)(a), by determining precisely the opposite solution, excessively restricts the relevance of the employee's consent, thereby eliminating any margin of free will for employees even when there are conditions for their expression without risk to their rights and interests. To that extent, this provision represents an unjustified and disproportionate restriction of the provisions of Article 6(1)(a) and Article 9(2)(a) of the GDPR. The CNPD therefore believes that this provision does not correspond to an appropriate national legislative measure that safeguards the dignity, fundamental rights and legitimate interests of the worker, and therefore does not meet the requirements of Article 9(2)(b) and Article 88(2) of the GDPR.

In short, because it represents an inappropriate, unnecessary and excessive restriction of the fundamental right to informational self-determination or data protection as a right to control one's own data, beyond what is necessary to safeguard the rights and interests of employees, Article 28(3)(a) of Law 58/2019 restricts the scope of Article 6(1)(a) and Article 9(2)(a) of the GDPR. On this basis, the CNPD, in order to ensure the

---

[10] Cf. Guidelines on consent in the GDPR, revised and approved on April 10, 2018, and taken over by the European Data Protection Board on May 25, 2018, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

full effectiveness of the GDPR, it will disapply this rule in the situations that it comes to appreciate.

5. The system of administrative offenses. Articles 37, 38 and 39.º

5.1. Article 37(1)(*a), (h) and (*A) and Article 38(1)(ô/)

Article 37(1)(*a}* stipulates that *"the following shall be regarded as very serious offenses. a} The processing of personal data in breach of the COiJSB9^ principles set out in Article fi.* of *the GDPR,".*

This provision thus seeks to rule out the possibility of penalizing negligent violations of the principles enshrined in Article 5 of the GDPR, in clear contradiction with the provisions of Article 83(5)(a) of the GDPR, which does not distinguish between the negligent or intentional nature of the conduct, and therefore does not recognize the power of the Member State legislator to define rules that reduce the list of illicit acts that can be punished.
sanction11_

Any appeal to the provisions of Article 83(2)(*b)* of the GDPR does not fit here, since that provision lays down the duty to consider the intentional or negligent nature of the unlawful conduct when deciding on the imposition of a fine or its exact amount. Therefore, since this provision is addressed to those who take such decisions, i.e. only the national supervisory authorities of each Member State and the courts, it cannot be used by the State legislator to alter the list of infringements expressly provided for in Article 83(4) and (5) of the GDPR.

Article 37(*h)*, regarding the failure to provide information under the terms imposed by Articles 13 and 14 of the GDPR, also distinguishes *relevant information* from other *information* (the omission of which would only give rise to a serious administrative offense - cf. Article 38(1)(*b)* of the Law), a distinction that is neither enshrined nor recognized in Article 83 of the GDPR.

[11] But it already allows other conducts to be added to the list of infringements provided for in Article 83(4) and

(5), as is clear from Article 84 of the GDPR.

In fact, in paragraph 5(b) of the latter article, the violation of the rights of data subjects under the terms of articles 12 to 22 is subject to the heaviest penalty, and no distinction is made, or room left to distinguish, according to the information omitted[12].

Furthermore, the violation provided for in Article 83(5)(b) of the GDPR covers all dimensions of the right to information and not just the failure to provide information. This means that misleading, erroneous, incomplete, dated or out-of-date information (in breach of Articles 12, 13 and 14) also falls within the scope of that GDPR rule, so limiting the punishable infringement only to the omission of information is incompatible with the GDPR.

Finally, the provision for refusing to cooperate with the CNPD, in Article 37(1)(k), as a very serious offense, subject to heavier penalties, also violates the sanctioning framework contained in the GDPR, since such an offense is included in Article 83(4)(a) of the GDPR (see also Article 31 of the GDPR).

Therefore, as they contradict the exhaustive list of infringements provided for in Article 83(4) and (5) of the GDPR and the respective sanctioning framework, the CNPD will not apply Article 37(1)(a), (h) and (k) and Article 38(1)(b) of Law 58/2019 in its future decisions.

It should be noted that the CNPD recognizes the application of the remaining subparagraphs of Article 37(1) and Article 38(1), which correspond to the repetition of infringements provided for in Article 83(4) and (5) of the GDPR, insofar as they have the useful effect of allowing each of them to correspond to the limitation periods established by the national legislator in Article 40, a matter that falls within the procedural autonomy of the Member States.

5.2. Article 37(2) and Article 38(2)

[12] In fact, the reference to the delimitation of the infringement to cases of non-compliance with the communication of relevant information and the delimitation of the obligation to provide information to certain dimensions of this was included in Article 79 of the proposal for a Regulation initially presented by the European Commission on 25.01.2012 (2012/0011 COD), but was definitively eliminated in the legislative procedure, which, as a historical element of interpretation of the current EU regime, strengthens the view that the EU legislator did not want, nor does it want, the protection of rights at the sanctioning level to be limited in any way.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Article 37(2) and Article 38(2) define, for the offenses provided for in Article 83(4) and (5) of the GDPR, different sanctioning frameworks depending on the size of the companies and the collective or individual nature of the data subjects. In a regulatory framework that is intended to be uniform across Europe, the ceilings set out in Article 83(4) and (5) of the GDPR cannot be set aside by EU Member States.

It is true that the introductory wording of paragraphs 4 and 5 clearly states that the monetary amounts set out there - 10 million euros and 20 million euros or a percentage of turnover in the case of a company - are maximum limits and, therefore, it follows directly from this that the fines may not exceed them in any case.

And a careful reading of Article 83 shows that it is directly addressed to the supervisory authorities, i.*e. it* is addressed to *each national supervisory authority* (in a judgment which can obviously be reviewed by the courts) and not to the national legislator. It is enough to compare the wording of Article 83(1) with that of Article 83(1).
84: in the former, the rule is addressed to the supervisory authorities; in the latter, it is addressed to the Member States as legislators. In fact, the only provision of Article 83 addressed directly to the national legislator, paragraph 7, had to be worded differently from the other paragraphs of the article: "Member States may provide".

So much so that Article 83(9) expressly provides for the direct applicability of the article by the supervisory authorities when there is no national law[13]. And reading recitals 148 and 150 reinforces this interpretation, highlighting that the provisions of that article are intended to provide direct and binding guidance to the supervisory authorities.
This Regulation shall define the infringements and *the maximum amount and the criterion for setting the amount of the resulting fines, which shall be determined by the competent supervisory authority in* each individual case.

---

[13] Moreover, the absence of such a national law has nothing to do with the lack of national definition of limits to sanctions, but rather with the lack of regulation in certain Member States of sanctions of this type.
1^ See also the WG29 guidelines on the imposition and setting of fines for the purposes of Regulation 2016/679, where the only circumstance in which each state is allowed a free hand is the following

Therefore, the setting in abstract, in national law, of lower maximum limits than those provided for in Article 83(4) and (5) of the GDPR constitutes a violation of them. This conclusion is corroborated by the case law of the CJEU, in Commission v. Italian Republic (Case 39/72); referring to the legislation passed in the Italian Republic, the Court states that "any implementing rules which may obstruct the direct effect of Community regulations and thereby jeopardize their simultaneous and uniform application throughout the Community are contrary to the Treaty"[15] - case law reiterated in the Variola judgment (Case 34/73).

In addition, the principle of the primacy of Union law, reflected in Article 288 of the TFEU, means that regulations are binding and directly applicable in all Member States, thus ruling out any possibility of a
"State [...], unilaterally, to annul its effects by means of a legislative act that can be invoked against Community texts" (cf. the aforementioned judgment of the CJEU Costa/ENEL, Proc. no. 6/64).

Furthermore, nowhere in Article 83, or in the recitals relating to the sanctioning regime, does it make room for the autonomous consideration of the size of the company, so the criterion adopted by the national legislator, of distinguishing between small and medium-sized companies in order to reserve the maximum monetary limit of the GDPR for large companies, is in itself a violation of the GDPR.

In this regard, it is important to remember that the importance given to small and medium-sized enterprises in the GDPR is very specific, contrary to what happened in the initial proposal for regulation, because it was concluded within the EU institutions that the impact on personal data resulting from the conduct of personal data controllers (and subcontractors) does not depend on the number of employees in these organizations, but rather on the nature of the activity carried out (categories of data processed, volume of data processed, categories of data subjects being processed, etc.)[16]. To this extent, elevating the

---

the enforcement of sanctions, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

[15] Judgment Commission v. Italian Republic of February 7, 1973, Case No. 39/72, paragraph 17.

[16] This development is demonstrated by the fact that only three articles in the version of the GDPR that was finally approved refer to the size of companies: Articles 30(5), 40(1) and 42(1).

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

delimiting the sanctioning frameworks by the size of the company is incompatible with the GDPR and contrary to the underlying *rule.*

The same conclusion can be reached with regard to the differentiation of sanctions for natural persons. Once again, nowhere in Article 83 of the GDPR does it distinguish the regime according to whether the infringement is committed by a legal person or a natural person. Only in recital 150 does it state that the specific setting (by the supervisory authority) of fines for persons other than companies - which also includes legal persons of a non-business nature, whether private or public law - must take into account the general level of income in the Member State, as well as the economic situation of the person in question. Therefore, the GDPR, even in the recital, only allows the monetary ceilings to be set aside in concrete terms, in the necessarily case-by-case consideration carried out by the supervisory authority. In fact, in this recital, it is admitted that *"if the amount of the fine likely to be imposed constitutes a disproportionate -- ^9° for a natural person, it may be disproportionate for a natural person".*

areprimand instead of a fine", which clearly shows that the framework

The sanctioning authority (in the Portuguese case, the CNPD) must always comply with the provisions of Article 83(4) and (5), regardless of whether the offender is a legal person or a natural person.

The same reasoning must apply to the setting of minimum limits, since the GDPR leaves no room for the national legislator to define a sanctioning framework different from that established in Article 83(4) and (5) of the GDPR. When it states that '[a*]n infringement of the provisions to be listed shall be subject, in accordance with paragraph 2, to fines of up to ...',* the GDPR eliminates the legislative power of the Member States to define the sanctioning framework in relation to the infringements provided for in those paragraphs.

Accordingly, the CNPD will only apply Article 37(2) and Article 38(2) of Law No 58/2019 in the context of infringements not sanctioned by the GDPR, i.e. the infringements provided for in Article 37(1)(*e}* and // and Article 38(1)(*q} and* r/).

Therefore, in order to ensure the full effectiveness of the sanctioning framework established in the GDPR, in its future decisions, the CNPD will disapply Articles 37(2) and 37(2) of the GDPR.

Article 38 of Law 58/2019, as it contradicts the provisions of Article 83(4) and (5) of the GDPR, only maintaining its application in the context of infringements not sanctioned therein (therefore, those provided for in Article 37(1)(e) and (l) and Article 38(1)(q) and (r) of the national law).

5.3. Article 39(1) and (3)

Article 39(1) sets out three criteria for determining the specific measure of the fine, in addition to those laid down in Article 83(2) of the GDPR.

As mentioned, the GDPR leaves no room for Member States to define other weighting criteria in relation to the infringements provided for in Article 83(4) and (5). Only under Article 84, and therefore for infringements not sanctioned in the GDPR, will it be possible for the national legislator to add criteria, as long as they guarantee sanctions that are effective, proportionate and dissuasive. And so, as far as these are concerned, the CNPD does not question the application of Article 39(1) (i.e. the infringements provided for in Article 37(1)(e) and (l) and Article 38(1)(q) and (r) of the national law).

It is true that Article 83(2)(k) of the GDPR allows for the consideration of other aggravating or mitigating factors applicable to the factual circumstances, such as the economic benefits obtained or the losses avoided as a result of the infringement. But it seems that the choice of factors should be made only in the specific case, by the (administrative or judicial) body applying the rule in question, and no longer by the national legislator of each Member State. This is clear from the second part of the body of Article 83(2) of the GDPR, which reads: "[i]n deciding on the imposition of a fine and on the amount of the fine in each individual case, due account shall be taken of the following:[...]".

Therefore, in order to ensure the application of the provisions of Article 83(2) of the GDPR, the CNPD disapplies Article 39(1), only maintaining its application in the context of infringements not sanctioned in Article 83(4) and (5) of the GDPR, and therefore only recognizing its application to the infringements provided for in Article 83(1)(e) and (l) of the GDPR.
37 and Article 38(1)(q) and (r) of Law 58/2019.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Finally, Article 39(3) of Law no. 58/2019 provides that *'ie]xcept in the case of willful misconduct, the initiation of administrative offense proceedings depends on the CNPD's prior warning of the offender to comply with the omitted obligation or rei"niepraçâo da proi"bi"çâo violado within a reasonable period of time'.*

By imposing on the CNPD a step prior to the decision to open a sanctioning procedure, which consists of a warning to correct the unlawful conduct within a reasonable time, this rule establishes yet another special regime for unlawful conduct committed negligently by controllers, which is not compatible with the regime provided for in the GDPR.

In fact, as is clear from the body of Article 83(2) of the GDPR, the EU legislator confers on the specific decision-maker, depending on the circumstances of each case, a discretionary power *to* impose fines in *addition to or instead of* the measures referred to in Article 58(2)(a)-(*h)* of the GDPR.

In fact, by stipulating that *"[fc]onced on the circumstances of each case, fines shall be imposed in addition to or instead of the measures referred to in Article 9 fi8.* Article 83(2*)* gives the national supervisory authorities the *right to impose fines in addition to or instead of the measures referred to in a^'9 fi8.*

the power to choose, on a case-by-case basis, to impose a fine only, to impose a fine and a corrective measure, or to apply one or more of the corrective measures provided for in Article 58(2) in isolation". It is this discretionary power that is indisputably granted to national supervisory authorities, with the obvious possibility of review by the courts, that the rule in Article 39(3) of Law 58/2019 is restricting, by imposing in the abstract on the CNPD the adoption of a specific corrective measure, regardless of the circumstances of each case (since it only takes into account the negligent nature of the infringement) and without allowing the immediate cumulation of the application of a sanction.

Such an imposition would deprive the Portuguese supervisory authority of the discretionary power granted to it by the GDPR, considerably removing or diminishing the useful effect of the rule that grants it. In fact, the national legislator seems to be trying to restore a provision in the first version of the proposal for a regulation drafted by the European Commission (then Article 76(3)), which was deleted at a later stage in the legislative procedure, but which nevertheless had a lesser impact on the useful effect of the rule granting the power to impose administrative sanctions, by limiting this duty.

prior warning in cases of negligent first infringement, and otherwise limited to certain categories of offenders.

In any case, the fact that this provision has been removed is a further argument in favor of the interpretation that the EU legislator has refused to limit or empty, even partially, in abstract terms, the powers to impose financial penalties for the infringements provided for in the GDPR, Therefore, a national rule that provides for such a prior procedure for any negligent infringement with the effect of delaying or making impossible the exercise of the sanctioning power recognized by the GDPR empties the useful effect of the EU rule that provides for such powers, putting in crisis the principle of the effectiveness of EU law.

With the aggravating factor that the CNPD's application of Article 39(3) of the Law would jeopardize the uniform application of the GDPR, preventing the CNPD from directly applying a sanction in the context of cross-border data processing (cf. Article 4(23) of the GDPR) in which it acts as the lead authority (cf. Article 56(1) and (2) of the GDPR). The CNPD's application of this provision, in this context, would certainly have the consequence of triggering the consistency mechanism provided for in Article 64 of the GDPR, at the end of which the CNPD would be bound to issue a decision with the content of the decision approved by the European Data Protection Board, in violation of the imposition provided for in that national rule.

What's more, the national legislator can do even less to impose on its supervisory authority the adoption of a corrective measure, determined in Article 58(2)(a) of the GDPR for cases in which a data processing operation is planned (and therefore not yet carried out) that is likely to violate the rules of the Regulation, in situations where the conditions for such a measure are not met. In other words, if the GDPR defines, in Article 58(2)(a), the preconditions for the warning decision, national law cannot impose the practice of this act when there is a situation that does not fall under these preconditions and fulfills another legal type for which the decision provided for in the GDPR is different.

With these arguments, as it is objectively incompatible with Article 83(2), as well as Article 58(2)(a) of the GDPR, thus emptying the useful effect of that rule, the CNPD will disapply Article 39(3) of Law 58/2019 in the situations on which it will rule in the future.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

6. Article 61(2)

Article 61(2) states that *"[i]f the expiry of consent is the reason for the termination of the contract to which the data subject is a party, the iralamination of the data shall take place before this occurs."*

This provision seems to have been introduced by the national legislator in an attempt to solve the problem, which has long been highlighted by the CNPD and other entities, that the contract is not an adequate basis for legitimizing the processing of special personal data, as is the case with health data [1'], so that in some sectors of activity (such as insurance) there is no legal basis for the processing of personal data necessary for the performance of contracts.

However, this provision constitutes a contradiction in terms, revealing the confusion between two autonomous grounds for legitimizing data processing, by admitting that the expiry of consent (because it does not comply with the GDPR) implies the termination of a contract, in other words, by admitting that consent to the processing of personal data is a condition for the validity of a contract to which the data subject is a party.

In fact, Article 6(1) of the GDPR distinguishes, as did Directive 95/46/EC and Law 67/98 of October 26, which transposed it, between the consent of the data subject and the contract to which the data subject is a party, providing for them as two sources of lawfulness or legitimacy for the processing of personal data. So much so that, under the terms of Article 6(1)(*b)* of the GDPR, the contract to which the data subject is a party is sufficient to justify the processing of the data necessary for its performance. Only when the controller intends to carry out other processing operations (not necessary for the performance of the contract) can it seek the consent of the data subject to legitimize these operations, under the terms of paragraph 1(a) of the same article. In this case, attention should be paid to Article 7(4), which, as highlighted in the WG29 guidelines (adopted by the European Committee) on

[1'] It should be remembered that the contract can only legitimize the processing of personal data necessary for its conclusion or execution if it does not involve the special data provided for in Article 9(1) of the GDPR, since that ground does not appear in the conditions of lawfulness provided for in Article 9(2).

consent within the meaning of the GDPR only regulates the relevance of consent for processing that is not necessary for the performance of a contract[18].

The reason for this clear distinction in the GDPR is the requirement of freedom to give consent, imposed by Article 4(11) of the GDPR. If the consent referred to the processing of data necessary for the performance of a contract, the conditions of freedom to give consent would not be guaranteed, due to the conditioning arising from the need to provide the service which is the object of the contract.
It follows that the processing of data necessary for the performance of the contract is not, and cannot be, based on the consent of the data subject. This is also stated in the aforementioned WG29 guidelines (adopted by the European Committee) on consent:
"If the controller intends to process personal data that is actually necessary for the performance of the contract, consent is not the legal basis"[19].

In fact, this is the same reason that led the national legislator, in Article 28(3)(b), to determine that, in the context of employment contracts, the employee's consent is not relevant when the hypothesis set out in Article 6(1)(b) of the GDPR is met (i.e. the processing is necessary for the performance of the contract). What is strange is that, after clearly distinguishing, in this provision of Article 28, the two conditions for the legitimacy or lawfulness of processing in accordance with the GDPR, national law confuses them in Article 61, establishing a conditional relationship between one and the other.

Such conditionality is totally in breach of the GDPR, in particular the provisions of point 11) of Article 4 of the GDPR and in recital 42, which states that "consent should not be considered to have been freely given if the data subject does not have a genuine or free choice or is unable to refuse or withdraw consent without being adversely affected".

The CNPD therefore believes that Article 61(2) of Law 58/2019 is incompatible with Article 4(11) and Article 6(1)(a) and (b) of the GDPR, and will therefore disapply it in the situations it assesses.

---

[18] Cf. p. 9 of the document accessible at https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf

[19] Ibid.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

7. Article 62º , paragraph 2

Lastly, Article 62(2) states that *"[a]ll rules that provide for the notification of the killing of personal data to the CNPD... shall cease to apply".*
*9 ^ *FÓ date of entry into force of the GDPR'.*

However, Article 99 of the GDPR clearly states that it will enter into force on the 20th day after the date of its publication (it was published on May 4, 2016) and that it will apply from May 25, 2018. With this, the European legislator ensured a two-year transition period for Member States, administrative bodies and the various organizations that handle or process personal data to properly prepare for the new legal framework.

By making the effects of Article 62(2) retroactive to when the GDPR came into force - which, it must be stressed, is May 25, 2016 - the national legislator is determining the *retroactive application* of the GDPR, in violation of Article 99(2) of this EU law, which is not admissible under EU law.

The CJEU expressly ruled along these lines in *Commission v. Republic of Hungary* (Case No 39/72, paragraph 14), when, referring to the setting of specific deadlines by regulations, it considered that "[...] *compliance with such deadlines was essential for the effectiveness of the measures in question, since they could only fully achieve their objectives if they were implemented simultaneously in all Member States at the set time".*

In fact, such a provision would mean that the duties to notify and obtain authorization to carry out certain data processing would be retroactively extinguished with effect from May 2016; as a result, authorizations issued in the meantime, *i.e.* issued between May 25, 2016 and May 24, 2018, would lose legal relevance for the purposes of Article 60(4) of Law 58/2019, which would render much of the useful effect of the latter rule meaningless. And such a result, absurdly, cannot be the one intended by national law.

Therefore, as it is contrary to Article 99(2) of the GDPR, the CNPD will disapply Article 99(2). 62 of Law 58/2019.

CONCLUSION

On the above grounds, in order to ensure the primacy of European Union law and the full effectiveness of the GDPR, the CNPD decides to disapply the following rules of Law no. 58/2019, of August 8, in the processing of personal data that it assesses:

i. Article 2(1) and (2)
ii. Article 20(1)
iii. Article 23
iv. Article 28(3)(a)
v. Article 37 (1) (a), (h) and (k) and (2)
vi. Article 38 (1) (b) and (2)
vii. Article 39(1) and (3)
viii. Article 61(2)
ix. Article 62(2)

The CNPD clarifies that it is making this decision public in order to ensure the transparency of its future decision-making procedures and thus contribute to legal certainty and security.

It also clarifies that the non-application, in future specific cases, of the legal provisions listed above will result in the direct application of the GDPR rules that were manifestly restricted, contradicted or compromised in their useful effect[20].

Approved at the meeting of September 3, 2019

[20] For a development of the practical consequences of the disapplication by administrative bodies of national rules for violation of European Union law, see Patrícia Fragoso Martins, National Public Administrations and European Union Law - Essential Issues and Case Law, Lisbon, Universidade Católica Editora, 2018, in particular, pp. 84-85.