Case No. 6275/2018 1

I. Order

OPINION No. 20/2018

The Chairman of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees

referred to the National Data Protection Commission (CNPD), for an opinion, the Proposal for a

Law No. 120/XIII/3.ª (Gov), which “Ensures the execution, in the national legal order, of the

Regulation (EU) 2016/679 on the protection of natural persons with regard to

processing of personal data and the free movement of such data'.

The request made stems from the powers conferred on the CNPD by paragraph 2 of article 22 of the

Law No. 67/98, of October 26, amended by Law No. 103/2015, of August 24 - Law of

Protection of Personal Data (hereinafter, LPDP) –, and the opinion is issued in the use of the

competence established in subparagraph a) of paragraph 1 of article 23 of the same legal instrument.

Considering the purpose of the Proposal, its assessment will be made not in relation to the

data protection law in force (the LPDP), but taking as a reference the

Regulation (EU) 2016/679 – General Regulation on Data Protection (GDPR) – and

the relevant constitutional norms.

As a preliminary note, the CNPD also underlines that the extent and density of this

opinion is due not only to the complexity of the matter but also to the fact that it does not

opportunity to comment on the draft bill of law, which

could have contributed to its final wording more in line with the GDPR and the

European Union law.

In any case, in order to facilitate the understanding of the content of the opinion and the possible

considering the adaptation of the draft law, the CNPD presents proposals

of drafting the rules of the diploma attached to this opinion.

II. Prior questions

1. Explanation of reasons and systematization

Firstly, it should be noted that the explanatory memorandum that accompanies the pleadings of the Law proposal presents some inaccuracies regarding the RGPD for which here understands to warn.

Process No. 6275/2018 1v.

Without prejudice to the considerations presented in point III.2.2., it is doubtful whether affirm that the "paradigm that underpinned the European legislator was that of the great multinationals that manage social networks or computer applications on a global scale, involving the collection and intensive use of personal data. For that reason, some of the legal solutions that were designed for this universe sometimes prove to be disproportionate or even inappropriate for the general business fabric national and for the Public Administration […]'.

In fact, what the GDPR takes as a paradigm is the technology available today for processing of personal data and, therefore, aims to reconcile the use of technological solutions in their current and future state of development, and the risks that behave, with the defense of the rights and freedoms of the people whose data are subject to treatment.

In other words, the GDPR is not only intended to regulate, or above all, to regulate processing of personal data by large companies, because these treatments do not have necessarily greater impact on the fundamental rights of citizens than those treatments carried out by small or medium-sized companies, by private non-profit entities for profit or by public entities. It is true that, considering the impact of treatments on the rights of data subjects in the Portuguese reality, so invoked in the explanatory statement, the Portuguese State and its indirect administration stand out and would therefore deserve an intense legal regime for the treatments carried out by them (it is enough think, in addition to the ministries, of bodies such as the Tax Authority and Customs, the Social Security Institute, IP, and the various Hospitals, EPEs).

Furthermore, the statement that 'the application of this regulation will result in
administrative overhead, which in many cases are not sufficiently
justified by the benefits obtained with the new personal data protection regime
in relation to the current regime" reflects a criticism of the European legislator's considerations
provided for in the GDPR and an implicit incentive for public entities to delay the
compliance with the GDPR, at least in a first phase of its application, which cannot
ceases to be of high concern to the CNPD, as an administrative authority
independent agency responsible for ensuring compliance with the legal regime for the protection of
data in the national territory.

It is also stated, on page 2 of the explanatory memorandum (4th §), that the GDPR establishes
stricter rules on the processing of special categories of personal data,
when, strictly speaking, what can be said is only that it expanded these categories (going to
cover, for example, biometric data), but not that the applicable regime is more
demanding.

As for the new features of the GDPR, it is stated on page 4 that the "role of prior control
of the supervisory authorities is deleted and replaced by records of the activities of
treatment', when strictly speaking that role is replaced by a prior duty of verification
compliance with the GDPR by those responsible and subcontractors, that the
registration is only a supplementary obligation.

Furthermore, some of the innovations introduced by the Proposal and explained in this section are
questionable compliance with the GDPR, as will be shown below.

Finally, a word for the systematization of the draft law, whose logic
in the part referring to chapters V and VI is not evident. At issue are, apparently,
matters in relation to which the European legislator recognized normative autonomy to the
Member States, but which not only contain provisions on matters excluded from that

autonomy as it is not understood the difference between special provisions and situations

specific processing of personal data. For example, provisions on

video surveillance or the processing of data on deceased persons are as special as

relating to health data. Therefore, a reformulation of this

systematization.

2. Disrespect for Union law

The CNPD cannot fail to draw attention to an unavoidable issue, which is

decisive in the appreciation of this Draft Law, since it translates into an objective violation

of Union law.

Firstly, this Proposal intends to reproduce in some articles part of the

article of the GDPR. This is, in particular, the case of article 2 (scope of application), of the

article 11 (functions of the data protection officer) or article 13 (data protection

of data protection in private entities). And this is not even about legislating on

Process No. 6275/2018 2v.

specific aspects that the Regulation refers to the scope of action of the Member State,

but only in an attempt to replicate provisions, with the aggravating factor that, in some cases,

to completely distort the content of the GDPR, grossly contradicting it.

Second, the Proposal intends to introduce into national law a rule that differs from

application of the GDPR for a time after the date prescribed in article 99 of the same

Regulation. Thus, despite the GDPR being applicable from May 25, 2018, it would be

possible, as proposed in article 61 (renewal of consent) of the Proposal,

take six months from the entry into force of national law to obtain consent

that would constitute the

foundation of

legitimacy for certain

data treatments,

therefore admitting a contrario the existence of unlawful processing during that period

of time.

However, pursuant to Article 288 of the Treaty on the Functioning of the European Union (TFEU), the

regulation is general in nature. It is mandatory in all its elements and directly

applicable in all Member States. Without prejudice to the detailed analysis carried out on the

throughout this opinion on all the rules contained in the Proposal in which the CNPD considers

there is an obvious violation of the terms of the GDPR, it is immediately noted that the legislator

Portuguese cannot extend the period of applicability of a GDPR obligation. About

this has already been ruled by the Court of Justice of the European Union (CJEU), in the Judgment

Costa/ENEL (proc. 6/64)1, in stating that this provision of the treaties would be devoid of

meaning if a State could unilaterally nullify its effects by an act

legislation enforceable against Community texts.

The Variola Judgment of the Court of Justice (case 34/73)2 also considers that the application

of a Regulation means that its entry into force and its application for or

against those who are subject to it are independent of any enforcement measure

national law (Point 10 of the Judgment).

On the other hand, with regard to the question of whether this Proposal replicates the content of the rules of the

GDPR, subjecting them to national law and, to that extent, also affecting the jurisdiction of the

European court, the Variola judgment is also very clear when it states that

1 https://institutoeuropeu.eu/images/stories/Cosa_Enel.pdf

2http://curia.europa.eu/juris/showPdf.jsf?text=&docid=88457&pageIndex=0&doclang=EN&mode=req&dir=&occ=fir

st&part=1&cid=378305

Members have a duty not to obstruct the direct applicability inherent in the regulations,

being that the strict fulfillment of this obligation is an indispensable condition for a

uniform and simultaneous application of the Regulations throughout the Community (Point 10).

Only the incorporation of elements of a regulation into national law is allowed
only to the extent necessary to maintain consistency and make national provisions
understandable, as provided for in recital 8 of the GDPR3, if they are provided for
specification of rules by the law of the Member State.

From this it can be concluded that, in the light of Union law interpreted by the Court of Justice,
the provisions of a Regulation cannot be introduced into the legal order of the
Member States through internal provisions which merely reproduce those
standards. Under the Treaties, Member States are under an obligation not to
introduce any measure that may affect the jurisdiction of the court (Point 11 of Judgment
Smallpox).

There is another Judgment of the CJEU, Commission v Italy (proc. 39/72)4, in which
relevant case law for the two types of infringement indicated above.

Thus, the Court of Justice, referring to the
setting specific deadlines by the
regulations, considered that compliance with those deadlines was essential for the
effectiveness of the measures in question, as they could only fully achieve the
their objectives if they were implemented simultaneously in all Member States, in the
established moment (…) (cf. Point 14).

On the other hand, on the mere reproduction of provisions of Community regulations in the
national legislation, the same Judgment states that this creates a misunderstanding with regard to the
legal nature of the provisions to be applied and reiterates that they are contrary to the Treaty
any implementation modalities that may impede the right effect of the regulations

3 Considering that it is based on points 26 and 27 of the Judgment of the Court of Justice of 28 March 1985,
process 272/83.

4http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30ddbf94149c102f4a878610d7c0bd468c6f.e34Kaxi
Lc3qMb40Rch0SaxyNbxz0?text=&docid=88354&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&ci

and thus jeopardize their uniform application within the Community

(cf. point 17).

With this legislative and jurisprudential framework, the national legislator is effectively

limited in its performance and must be especially careful when legislating in execution of a

Regulation, under penalty of infringing Union law. The effort to repeat the norms of the

Regulation in national law takes on even greater gravity when the text of the Proposal

clearly contradicts the content of the GDPR precepts.

On the implementation of the GDPR, the European Commission issued Guidelines in January of this

year, in a Communication to the European Parliament and the Council5, in which he argued that the

Regulation provides an opportunity to simplify the legal environment, moving

so there are fewer national rules and greater clarity for operators.

In this context, the Commission explains that any national measures that result in

create an obstacle to the direct applicability of the regulation and jeopardize its

simultaneous and uniform application throughout the EU are contrary to the Treaties.

On the other hand, the European Commission is emphatic in stating that: [R]epeting the text of the

regulations in national law is also prohibited (…) Reproduce the text of the regulation

word for word in national law aimed at specification must be something exceptional and

justified and cannot be used to add conditions or interpretations

additions to the text of the regulation.

Based on the extensive jurisprudence on this matter, cited above, the Commission

European Union reiterates that the interpretation of the regulation is up to the European courts (…) and not

to the legislators of the Member States, so the national legislator cannot copy the

GDPR text, nor interpret it or add additional conditions to the rules

directly applicable under the Regulation. If they did, operators across the

Union would again be faced with a situation of fragmentation and would not know to what rules obey.

The European Commission warns of the possibility of infringement proceedings if Member States fail to comply with these rules. Now, the text of this Law Proposal will

5http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN

unequivocally contrary to Union law, European jurisprudence and recent European Commission guidelines specifically on the GDPR.

Furthermore, in matters where the legislative competence of the Member States is not exhausted by the RGPD and, therefore, rules can be established that adapt the statute to national specificities, the Draft Law assumes a vague and open content, not thus managing to create an effectively disciplining regime for data processing.

Sometimes, limiting themselves to reproducing regulatory criteria provided for in the norm of the GDPR that grants legislative autonomy, sometimes even failing to comply with the duty to reconcile fundamental rights, imposed by the RGPD, through the provision of limits or precise material and procedural measures. And it is well known that the regulation on rights, freedoms and guarantees must, by constitutional imposition, have a higher density, not being enough with open or programmatic norms.

3. Protection of privacy

A further note to the fact that this Draft Law does not specifically provide on data relating to privacy. This option is perhaps due to the fact that the GDPR does not leave room for Member States to legislate on the data catalog specially protected personnel provided for in Article 9(1). Indeed, of these categories of personal data does not include private life, which is subject to protection reinforced in paragraph 3 of article 35 of the Constitution of the Portuguese Republic (CRP) – protection

constitutional law that is reflected in the still in force LPDP, which, in the catalog of sensitive data provided for in Article 7, includes data relating to privacy.

However, the protection of privacy and the definition of a specific protection regime reinforced are imposed not only by the Portuguese Constitution (see also paragraph 1 of article 26), but also by the European Convention on Human Rights (ECHR), in article 8, and by the Charter of Fundamental Rights of the European Union (Article 7).

It is important, in this regard, to remember that the ratio underlying this protection regime reinforced is to guarantee the dignity of the human person in the context of processing information relating to dimensions of human life whose treatment has historically generated and is likely to lead to discrimination. Hence, from the outset, the conditions for legalizing the

their treatment, listed in article 9 of the GDPR, are more restricted than those provided for in article 6 of the same diploma.

What is certain is that all these categories of personal information reveal dimensions of life private ownership of its holders, but they do not exhaust it. For this reason, even though the GDPR subjects the remaining dimensions of privacy to the data regime covered by article 6, that regime has to be interpreted in accordance with Articles 26(1) and 35(1) 3 of the CRP, and with article 8 of the ECHR and article 7 of the Charter of Fundamental Rights, always guaranteeing the result of effective protection of privacy. In fact, this is the understanding of the CJEU6.

As a result, a set of data processing relating to privacy that depended, under the LPDP, on a specific legal provision or, in the absence of consent, on the recognition that its purpose corresponded to a public interest importantly, can now be carried out on the basis of one of the conditions set out in Article 6. of the GDPR. However, the assessment of the lawfulness of the processing of data relating to life private passes, in a

interpretation in accordance with constitutional norms and

mentioned above, by the concrete verification of the guarantees of effective protection

privacy and non-discrimination. In particular, treatments based on the

legitimate interest of the person in charge, the lawfulness of which depends on whether, in each case,

the rights and interests of the holders, can only be considered lawful if this is not

unnecessarily or unbearably exposed the private life of the holders or if

there is a serious risk of a discriminatory outcome for them.

III. Analysis of the draft law

In the analysis that follows, the provisions of the

Bill that translates into a direct violation of the GDPR, either by contradicting the

provided, either because they limit themselves to reproducing the rules contained therein, distorting their

value of Union law rule.

6 Cf. Schrems, Digital Rights and Tele 2 judgments, available respectively at

(http://curia.europa.eu/juris/liste.jsf?td=ALL&language=pt&jur=C,T,F&num=C-362/14)

(http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN) and

(http://curia.europa.eu/juris/liste.jsf?num=C-203/15&language=EN).

Afterwards, the regime for public entities that in the Proposal was understood to be

fix.

Thirdly, it will focus on a set of provisions on matters on which there are

duty to legislate at the national level, seeking to alert to some inconsistencies and

incompleteness. From this group, the system of administrative infractions will be highlighted, which will deserve

a more detailed analysis.

Finally, after analyzing the criminal sanctions, the other provisions of the

Proposal that focus on matters whose specific national regulation is allowed by the

GDPR

And it will close with a brief critical comment on some final provisions or

transient.

1. Norms that violate Union law

1.1 Scope of application

Let us analyze, in this regard, Article 2 of the Proposal on the scope of application of the law

national. Paragraph 1 of this article prescribes: “[The] present law applies to the treatment of

personal data carried out in the national territory, regardless of the public or

privacy of the controller or processor (…), all applicable

exclusions provided for in article 2 of the GDPR”. Paragraph 2(a) determines that: “[A]

this law applies to the processing of personal data carried out outside the territory

national law when they are carried out within the scope of the activity of an establishment located in the

National territory".

Indeed, these rules amount to a clear violation of article 3, paragraph 1, of the

GDPR, calling into question the one-stop shop mechanism that is one of the characteristics

most emblematic of this regulation.

On the one hand, according to the GDPR, the place where the data processing

actually take place, whether on national territory, in another Member State or outside the

Union, applying rather the criterion of establishment in the territory of the Union, provided that the

data processing takes place in the context of the activities of this establishment. Per

Process No. 6275/2018 5v.

on the other hand, if there is more than one establishment in the Union, the applicable law will be that of the

main establishment.

Therefore, it is not possible to apply Portuguese law to all processing of

data carried out in national territory or in the context of activities of an establishment

located in Portugal. These provisions of the Proposal unequivocally contradict what

is defined in the GDPR as to the territorial scope of application.

Likewise, subparagraph b) of paragraph 2 of article 2 of the Proposal, which intends to have
Correspondence to Article 3(2) of the GDPR, restricts its application to the allocation of
data subjects 'who reside in the national territory'. In this precept, an error persists
which is already included in the Portuguese version of the GDPR, but which limits the protection given by the
Regulation to holders residing in the territory of the Union, when in fact the application of the
GDPR extends to all holders who are in the Union. Otherwise, check out the
English version, in which the proposed Regulation was presented, discussed and approved:
«the processing of personal data of data subjects who are in the Union»7.
There is, therefore, no basis for the Draft Law to impose a restriction on the
scope of application of the GDPR, which moreover explains in its recital 14 that the protection
conferred by this Regulation should apply to natural persons,
irrespective of their nationality or place of residence, creating
consequently a differentiation of the legal regime for the protection of personal data
for holders who are in Portuguese territory but do not reside here. remember
that the Portuguese Constitution recognizes the ownership of the right to data protection to
any person, even if he is not a Portuguese citizen or resident in national territory
(cf. article 15), so we are dealing with a violation of the principle of equality in
guarantee of fundamental rights, under the terms of articles 13, 15 and 35 of the CRP. The article
8 of the Charter of Fundamental Rights of the European Union recognizes the same right to
all persons, without delimiting, according to nationality or residence, the scope of
application of the tax norm of legal protection.
7 Italics ours. See still in the French versions «qui se trouve sur le territoire de l'Union», Italian «che si trovano
nell' Unione", German "die sich in der Union befinden" and Dutch "die zich in dir Unie bevinden".

Finally, still with regard to the scope of application, subparagraph c) of paragraph 2 of article
2 of the Proposal provides that national law applies to data processing carried out outside

national territory when: "affects data subjects who, being Portuguese, reside

abroad and whose data are registered at consular posts'. Now, this contradicts

notably Article 3(3) of the GDPR, which extends its application to the person responsible for the

treatment established in a place where the law of a Member State applies by virtue of

of public international law.

Thus, the scope of application is much wider than that of consular posts,

including also Portuguese embassies, aircraft or vessels, and

covering any

kind of

processing of personal data that is carried out,

irrespective of the categories of data subjects who, naturally, may

encompass non-resident Portuguese, foreign visitors, foreign workers and

so on, something even contradictory with the limited scope of application that we criticized

above, then regarding the exclusion of non-residents.

The GDPR does not give the Member States any leeway in this matter to legislate,

the raison d'être of this article is not understood, which ends up doubly infringing the right of

Union, either by intending to replicate the rules of the regulation in national law, or by,

in doing so, entirely distort the territorial scope of application of the GDPR. It must, in this

sense, be eliminated, considering it sufficient for the purpose of delimiting the scope of

application of the Proposal the definition of its object, contained in article 1, when defining that the law

ensures the implementation, in the domestic legal order, of the GDPR.

1.2. Rules relating to the CNPD

With regard to Chapter II of the Proposal, concerning the supervisory authority in

of data protection, there are also rules that do not comply with the law

of the Union.

Thus, paragraphs 3 and 4 of article 4 (nature and independence) are limited to replicating

provisions of the GDPR, respectively provided for in paragraphs 1 and 2 of article 52 of the

Regulation, therefore, for the reasons explained above (cf. II. 2), they should be deleted.

Process No. 6275/2018 6v.

As for article 6 (attributions and powers), the provisions of subparagraphs d) and e) of paragraph 1

also repeats what is provided for in articles 41, paragraphs 3 and 5, 42, paragraph 5, 43, paragraphs 3 and 6, and

57, no. 1, points p) and q), of the GDPR. To that extent, on the grounds already stated,

these provisions must be deleted from the Proposal.

Still in relation to subparagraph g) of paragraph 1 of article 6, in which it is foreseen as attribution

CNPD «promote adequate and regular training actions for those in charge

of data protection', it cannot fail to emphasize that this is not a competence

of the supervisory authorities under the GDPR, and in this sense the legislator cannot

national comes to add attributions without the Regulation admitting this interference from the

Member State, which is not the case in this case.

Furthermore, pursuant to Article 38(2) of the GDPR, it is about the person responsible for

treatment and the subcontractor who is obliged to provide the person in charge of

data protection the resources necessary for the performance of its functions and the

maintenance of your knowledge. Transfer, in a way, this training burden to

the CNPD – moreover in open competition with the market – is clearly a subversion

of the rules. The GDPR only requires the supervisory authority to promote awareness

controllers and processors for their obligations under the

terms of the Regulation8, which, given the duties of the data protection officer

in the organization, already means being able to play a relevant role in the intermediation

of awareness-raising actions. This rule must therefore, because it is contrary to Union law, be

removed from the pleading.

With regard to Article 7(1) of the Proposal (prior impact assessments), in

that the CNPD is required to draw up "a list of types of data processing

whose prior impact assessment is not mandatory', it is understood that this provision

contravenes the GDPR, insofar as it requires the creation of a positive list (cf.

4 of article 35), but leaves to the discretion of the supervisory authority the possibility

to make a negative list (cf. paragraph 5 of the same article of the Regulation).

Thus, as the GDPR grants this power directly to the supervisory authority and not to the

Member State, did not give the national legislator scope to regulate this matter, so

this rule should also be deleted.

8 Cf. Article 57(1)(d) GDPR.

However, the principle underlying Article 7(2) of the Proposal to promote the realization

of impact assessments voluntarily, that is, when they do not depend on any type

of obligation, is very welcome and can be included in the law, since it does not contradict the

provided for in the GDPR. Therefore, the following wording is proposed for the article:

1 – In situations where it is not mandatory to carry out the impact assessment referred to in article 35.

GDPR, controllers and processors can carry out this prior assessment of

impact on its own initiative, albeit in the same terms as any impact assessment takes place

mandatory.

2 – The lists referred to in paragraphs 4 and 5 of article 35 of the RGPD are published on the CNPD website.

In relation to Article 8 of the Proposal (Duty to cooperate), serious reservations are raised

as to its content. First of all, in relation to paragraphs 1 and 2 of the article, as they are limited to

reproduce the content of the rules contained in article 58, paragraph 1, points a), e) and f) of the

GDPR, and the general duty of cooperation with the supervisory authority, upon request

of this, in the pursuit of its attributions is also provided for in article 31 of the

GDPR Therefore, in accordance with Union law, these two provisions

must be eliminated.

With regard to paragraph 3 of article 8, which imposes a duty of secrecy on "members of the

CNPD, as well as the technicians mandated by it», it is advisable to carefully analyze the
precept. First, this is the only rule in the entire Proposal that mentions confidentiality
professional to which anyone who works at the CNPD is subject. However, it falls short of
provided for in article 54(2) of the GDPR, as it only refers to the
context of inspection by the CNPD and not the entire activity of an inspection authority
control. Indeed, the universe of persons subject to professional secrecy must encompass
members and all personnel of the authority, as follows from the Regulation and not just the
personnel mandated for an inspection. This is, in fact, the current reality shown in the article
17 of the LPDP, which extends the duty of professional secrecy to all those who exercise functions in the
CNPD
Thus, once again, it appears that the national legislator is infringing EU law. Although
Article 54(2) of the GDPR admits some regulation by the Member State, this
cannot run counter to the scope of the European regulatory provision, that is, either
Process No. 6275/2018 7v.
regarding the universe of persons subject to secrecy, both in terms of its duration and
range, which actually happens.
Secondly, the empowerment of "trade secret" cannot be understood since it
that the GDPR already includes in the duty of secrecy of the supervisory authority's members and staff
any confidential information, and there is a set of other types of secrets legally
protected and that would be equally valuable, such as: medical secrecy, tax secrecy, secrecy
communications (in terms of traffic and location data), bank secrecy or
social security secrecy.
Finally, paragraph 4 of article 8 of the Proposal, in the form in which it is worded, constitutes a
manifest breach of the GDPR, as it automatically terminates the powers of the
supervisory authority to access personal data processed and obtain all information
relevant to the performance of their duties. As already exemplified above, there are several

types of secrecy, in different sectors of activity, and which precisely mirror the
increased protection given to especially sensitive information – which is
extremely relevant also from the point of view of the protection of personal data, being
to that extent even deserving of reinforced control.
Thus, in order to defend the rights, freedoms and guarantees of citizens, be able to verify with
effectiveness compliance with data protection rules is essential to the activity of the
CNPD Furthermore, in this new legislative framework in which the supervision model has changed to
a posteriori control. Now an open rule that establishes that the powers of
supervision of the CNPD do not prejudice the duty of secrecy is, in practice, an impediment to
carry out any type of inspection action and collect any evidence, as this
is prohibited, and those responsible for the treatments may shield themselves from not giving access to the
their information systems invoking the duty of secrecy.
In this way, it would no longer be possible, for example, for the CNPD to carry out an effective inspection
to a banking institution, the Tax Authority, the Social Security services, the
any health establishment, to a telecommunications operator.
The GDPR allows the Member State to adopt in its legal system rules that
make it possible to reconcile certain confidentiality obligations with the right to data protection
personal, if necessary and proportionate, but always within the limits of the
Regulation (cf. article 90 and recital 164 of the GDPR).

This is not the case in paragraph 4 of article 8 of the Proposal, which does not specify
measures nor is there any concrete compatibility, based on a
judgment of
proportionality, which would allow
interfere with the powers given by the GDPR to
supervisory authorities, limiting itself generically to putting a stop to the CNPD's action

upon invocation by the controller or processor of

any professional secrecy.

As there are no limitations in the Portuguese legal system to date

order to supervise the CNPD, like other public entities with

inspection powers, unless the national legislator now wants to introduce

access restrictions by the CNPD - which would have to be done in the manner provided for in the

Regulation – it is considered that article 8 should be deleted, as the wording of all

their numbers does not respect Union law.

However, as there is no other rule in this Proposal that provides for the duty of secrecy of the

members and staff of the CNPD, it is considered that article 8 can regulate this matter, in

identical to what currently exists and in line with the GDPR, suggesting the following

wording for article 8, whose title would be on professional secrecy:

1 - CNPD members and staff are bound by professional secrecy regarding personal data or

confidential information to which they have access in the performance of their duties.

2 – The obligation of secrecy remains even after the end of their duties.

1.3. Rules relating to the data protection officer

Chapter III of the Proposal concerns the figure of the data protection officer (DPO).

In this matter, the GDPR leaves very little scope for Member States to legislate.

Thus, in relation to Article 9 of the Proposal (general provision), the national rule repeats the

5 of article 37 of the GDPR, regarding the professional qualifications of the person in charge of

data protection, determining in the end that it does not need certification for the

exercise of functions.

As the RGPD is silent on this, therefore not establishing any obligation to

certification, it is considered that it can be relevant and clarifying for those responsible and

subcontractors introduce this provision into national law as it does not contradict the

Regulation. However, to avoid reproducing the text of the GDPR and an erroneous

for functions referred to in article 11 of the Proposal (as will be explained below), it is suggested to

following wording for Article 9:

The data protection officer, appointed on the basis of the requirements set out in paragraph 5 of article 37 of the

GDPR, does not require professional certification to perform the functions referred to in article 39 of the

GDPR

As for article 11 of the Proposal, it is intended to establish additional functions to the

data protection officers, when this is not permitted by the Regulation,

thus constituting this article an infringement of Union law.

Furthermore, the proem of the article refers to articles 37 to 39 of the GDPR as if

these regulate the functions of the data protection officer, when only the article

39th does. In addition, paragraph a) of article 11 of the Proposal, when attributing to the EPD the

of "[to]ensure that audits are carried out, whether periodic or unscheduled" seems

contradict what is stated in Article 39(1)(b) of the GDPR, which only provides that the

data protection officer controls compliance with this regulation

(…) and with the controller's policies (…) including (…) the audits

correspondents.

For all these reasons, since the Member State is not given the possibility to legislate on

functions of the data protection officer, article 11 should be deleted from the text of the

Proposal.

Regarding article 12 (Data protection officers in public entities),

only paragraphs 1, 2 and 5 of the article are considered to comply with Union law.

As for paragraphs 3 and 4, they do not comply with the provisions of the Regulation, so they must be

deleted. Indeed, it is intended to dispose of matters that are not available

of the Member States. On the one hand, because the legislator is interfering in the designation of

data protection officers, when it is the person responsible and the subcontractor who

it is up to designate the EPD. On the other hand, because it is conditioning the distribution and sharing of EPD in public entities, without taking due account, in the specific case, of the respective organizational structures and size of the entities involved.

And even if this matter was available to the Member States, the seems to contradict the GDPR.

First of all, in paragraph 3 of article 12, the meaning of the caveat is not understood. "Regardless of who is responsible for the processing", since paragraph 1 of the Article 37 of the GDPR specifies that each controller and each subcontractor designates a EPD, so the provisions of subparagraph a) of paragraph 3 of article 12 of the Proposal raise the greatest reservations; even because, read in conjunction with the provisions of paragraph 4, at the limit it admits an EPD for the entire central administration of the State.

However, national legislation cannot exclude the obligation imposed by the GDPR, in point a) of the Article 37(1) of each public authority or body having an EPD. Do not ignores that Article 37(3) of the GDPR allows the sharing of EPDs, but there it is necessary also that the respective organizational structure and size be taken into account. And the Article 12(3) and (4) of the Proposal do not reflect this weighting. It is important to clarify that the designation of the same EPD by several public services or entities is an option that only can be followed if conditions are still assured to the person in charge of complying perform their duties efficiently, and the guarantee of the citizens' rights.

Furthermore, the provision in subparagraph d) of paragraph 3 is, in itself, contradictory to the in subparagraph a) of paragraph 1 of article 37 of the GDPR, because parishes, as persons collective bodies governed by public law, are obliged to have a data protection officer irrespective of the nature or volume of the data processed. It is true that today, with the attributions and powers of these entities, as a result of the increase in decentralization

administration, it is difficult to conceive that the volume of personal data is not

significant.

It is understandable that the Proposal wanted to safeguard the definition of the

competent to designate an EPD. However, it is doubtful whether it can be recognized that this

competence is not exclusive to the data controller, by virtue of the

GDPR, and, to that extent, not susceptible of being imputed to the highest hierarchical

an administrative organization – this is evident when laws, by legitimizing a

data processing, define who is responsible and do not make it coincide with the body of the

top of the administrative hierarchy.

Process No. 6275/2018 9v.

In this way, the CNPD understands that paragraph 3 of article 12 should be eliminated in order to

ensure compliance with the provisions of paragraph 1 of article 37 of the GDPR, which is worth

last precept as a norm attributing the competence of designation to each person responsible,

together with the laws that identify the responsibility of the treatments.

For the same reasons, Article 12(4) should be deleted, as the GDPR already

provides for the sharing of EPD by different officials.

Likewise, article 13 (Data protection officers in private entities)

is limited to reproducing, word for word, subparagraphs b) and c) of paragraph 1 of article 37 of the

GDPR, therefore, on the grounds set out above (cf. II.2), it appears to violate the right

of the Union and should therefore also be eliminated.

1.4. portability

In article 18 (Data portability and interoperability) it is intended, once again, to legislate

on matters not permitted by the European Regulation, at the same time that the

scope of the provisions of the GDPR. Paragraph 1 of the article, in the form in which it is worded, becomes

interpretive text of the Regulation, which is not admissible (cf. II.2); on the other hand, the

The content of paragraph 2 clearly contradicts what is provided for in article 20 of the GDPR.

While the Regulation provides that the data subject has the right to receive the data
personal information (…) in a structured, commonly used and machine-readable format (…), provided that
that the processing of data is obviously carried out by automated means and in the
conditions of subparagraph a) of paragraph 1 of article 20, the national legislator determines that the
data portability 'should, whenever possible, take place in an open format'.
Additionally, paragraph 3 of article 18 of the Proposal introduces a novelty in the regime of
portability, particularly for the scope of public administration, when in fact the GDPR
establishes that the data portability right does not apply to the necessary treatment
for the exercise of functions in the public interest or the exercise of public authority to
the person responsible is vested (cf. paragraph 3 of article 20). In fact, the right of portability only
is recognized by the GDPR when data processing is based on
lawfulness a contract or the consent of the data subject (cf. point a) of paragraph 1 of article
20th). These two rules combined almost entirely exclude the possibility of

exercise of the portability right within the scope of data processing by the administration
public. And even if there could be eventual situations in which this right would apply,
would have to be in the exact terms of the GDPR. Hence the entirety of article 18 of the Proposal
should also be deleted as it does not comply with Union law.
1.5. duty of secrecy
Article 20 of the Proposal (Duty of secrecy) raises a vehement criticism of the CNPD for the
flagrant violation of our Constitution and the Charter of Fundamental Rights of the Union
European Union, in addition to the manifest breach of the GDPR, by outright preventing the exercise
of the right of access.
Under the terms of the Proposal «[T]he rights of information and access to personal data
provided for in articles 13 to 15 of the GDPR cannot be exercised when the law imposes
to the controller or processor a duty of secrecy that is

enforceable against the data subject himself'.

Articles 13 and 14 of the GDPR regulate, respectively, what information to provide to the holder when personal data are collected directly or indirectly. In these two articles, only in the situation provided for in article 14, in which the data are not collected from the its holder but in another source, it is foreseen that the data holder may not be informed about a particular processing of data that is being carried out as a result of a legal obligation of confidentiality9 (as will be the case, in particular, of lawyers).

This obligation of secrecy will result from a specific legal provision relating to the matter in question. question and not through a generic article embedded in the national law implementing the GDPR

Article 15 of the GDPR regulates the exercise of the data subject's right of access to their data. and does not provide in the article itself any exceptional situation. Only in article 23 of the GDPR, the possibility is foreseen for Member States to be able to limit by measure legislation 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

9 Cf. Article 14(5)(d) of the GDPR.

ensure a wide range of purposes that are listed in paragraph 1 of the article. In addition Furthermore, if only for the requirements contained in paragraph 2 of article 23 of the GDPR, it is evident that the legislative measures referred to relate to legislation that regulates specifically processing of specific data, as it determines, in particular, that explicit provisions are included regarding the purposes of the treatment, the categories of personal data processed, the retention periods, the identification of those responsible by the treatments and, most importantly, within the scope of the imposed limitations.

Indeed, any limitation that is introduced by law to the exercise of rights, in

particular to the exercise of a fundamental right such as the right of access, recognized autonomously in paragraph 2 of article 8 of the Charter and in paragraph 1 of article 35 of the CRP, not may never result from the content of the rule contained in article 20 of this Proposal. nor the preliminary suppression of the exercise of a right is admissible, nor is this the legislative context adequate to regulate any type of restriction, as this can only occur in the case concrete and not in general, nor is a generic "duty of secrecy" even a purpose provided for in the GDPR.

If the objective of the national legislator is to admit limitations to the exercise of the right to information and access, a possibility that the GDPR gives to national law, will have to do so, not in the context of this Proposal, in particular in the generic terms in which it is made, but specific legislative measures in each type of case. Furthermore, the measures impose restrictions on the exercise of rights must respect the requirements of article 23. of the GDPR; otherwise, they will not constitute a legal basis for the purpose.

Even in the context of criminal investigation and prosecution of criminal offences, regulated by the Directive (EU) 2016/680, the rights of data subjects cannot be completely cancelled. Owners are always guaranteed the exercise of their right of access. At possible derogation situations must be properly specified and any partial or total refusal to provide information must be justified and documented in light of exceptions determined by law. The assessment is case by case but not arbitrary. by majority reason, article 20 of the Proposal does not provide the necessary legitimacy to do so and contradicts the provisions of article 23 of the GDPR and should therefore be deleted.

1.6. Data retention periods

As for article 21 of the Proposal (period of retention of personal data), this vigorous forecast repair by the CNPD, insofar as it is one of the principles relating to data processing.

It should be clarified from the outset that when the GDPR, like the current data protection law, is referring to conservation periods is referring to maximum conservation periods, a since the principle of limitation of retention prescribes that personal data must be kept only for as long as is necessary for the purposes for which they are treated 10.

Indeed, irrespective of the definition of a maximum retention period, the personal data must be deleted or made anonymous as soon as it is fulfilled, in the specific case, the purpose of the treatment. This means that in relation to certain data subjects, when the purpose of the treatment has already been achieved, the respective personal data to be erased, rather than continuing to be processed until it is the maximum retention period has expired.

The application of this principle is, of course, without prejudice to the need to retain data when there is a law that requires it. However, even in these circumstances, they should only be The data necessary for the fulfillment of the legal obligation will be kept and not others that are not necessary for that purpose. It will be the classic example of a treatment of customer management data, in which it is mandatory for the company to maintain customer data customer invoicing for a period of 10 years for tax purposes, hence the duty to keep other customer data (such as contacts, age, consumption details, interests and preferences) if the contractual relationship is terminated after two years old.

The wording proposed in article 21 completely distorts this basic principle of the data protection, contained in all international legal protection instruments data since 1981 with Convention 108 of the Council of Europe (Convention for the protection of individuals with regard to the automated processing of personal data guys).

10 Cf. Article 5(1)(e) of the GDPR.

Firstly, the GDPR only allows the Member State to legislate on this matter, and even
thus within the parameters defined by the Regulation, regarding data retention
for longer periods where the exclusive pursuit of marketing purposes is at stake.
public interest archive, scientific or historical research purposes or statistical purposes.
Well, that's not what happens. The Draft Law intends to regulate other aspects – in fact, of
incomprehensible way – which is in itself a violation of Union law, since the
national legislator is bound to discipline only the matters allowed by the
Union Regulation, as already explained in the light of European jurisprudence.
Thus, paragraphs 1 and 4 of article 21 subvert the principle of limiting conservation with
There are also incorrect repetitions of Union law, as explained above.
Paragraph 3 introduces an autonomous and generic purpose – to prove compliance with
obligations – which would be common to all treatments and parallel to the legitimate and
determined for each of them, to provide coverage for a retention of data for a time
almost unlimited, which is truly intolerable. On the one hand, the shelf life
of the data is always linked to the specific purpose of the treatment that formed the basis of the
its collection or further processing; on the other hand, prove compliance with
obligations is not an end in itself; Finally, this standard also intends to
cover subcontractors, when they are not available to establish
retention periods for personal data, which they process only on behalf of and on behalf of the
responsible for the treatment.
Paragraph 5 of this article provides that if there is "a data retention period imposed
By law, the right to erasure provided for in article 17 of the GDPR that has ended can only be exercised
that deadline'. This provision clearly contradicts the content of Article 17 of the
Regulation. Here it is foreseen, in particular, that the data subject has the right to
erasure of your personal data, if you object to its processing for reasons

related to your particular situation and there are no

interests

legitimate

prevailing11, or when the data is processed unlawfully.

11 Pursuant to Article 21(1) of the GDPR, the right of opposition of the holder can be exercised even when

processing of personal data, based on point e) of paragraph 1 of article 6, that is,

treatments necessary for the exercise of functions in the public interest or for the exercise of public authority to

that the person responsible is invested in. In fact, similar to what already happens in the current data protection regime.

Process No. 6275/2018 12

Thus, it is not the fact that there is a legally established data retention period,

which may prevent the data subject from exercising his right to erasure, provided that

that the legal conditions for this erasure have been met, which will have to be assessed if-

a-case. In fact, there is no relationship between the two vectors, with #5 being the opposite of

GDPR when intending to restrict the exercise of a right for a reason that cannot be met in accordance with

with the European regulation.

In this sense, paragraphs 1, 3, 4 and 5 of article 21 should be deleted from the Proposal by

be violators of Union law.

Let us now analyze the content of paragraph 2 of article 21, which deals with a matter that, indeed, is

referred to the law of the Member State. It provides that, when "it is not possible to

determine in advance the moment when [treatment] is no longer necessary, it is

lawful retention of personal data'.

In this regard, it is worth recalling recital 39 of the GDPR: personal data must

be adequate, relevant and limited to what is necessary for the purposes for which they are

treated. For this, it is necessary to ensure that the data retention period is

limited to the minimum. This close relationship between the conservation limitation principle and the

principle of data minimization, as a manifestation of the principle of

proportionality within the scope of data processing, requires that the data be

only kept for as long as they are necessary for the pursuit of the purpose set out in the

basis of your collection.

Bearing this in mind, the option expressed in this Proposal, in paragraph 2, causes the greatest perplexity.

to waive the limitation of data retention, and to waive it with such a

amplitude.

In fact, as drafted, the standard allows for unlimited storage of data.

personal data for any purpose, due to the consideration of a factor that is not

considered in the GDPR – that of the nature of the treatment – as long as it is not possible

determine in advance the moment when it is no longer needed.

Therefore, we are facing a legal provision that not only makes an exception to the rule of

limitation of data retention beyond the exceptions in the GDPR (which only

admits exceptions regarding treatments aimed at archiving purposes in the public interest,

scientific or historical research or statistical purposes), but also allows the

Process No. 6275/2018 12v.

ad eternum conservation of the same, in clear violation of the principle of proportionality,

in terms of necessity – it is recalled that the GDPR admits longer retention periods

long, but not that conservation is done without limit.

In addition, the GDPR also requires that, when there is room for data retention by

longer periods exclusively for the purposes listed in subparagraph e) of paragraph 1 of the

Article 5 of the GDPR, the data are subject to the obligation to adopt technical and

appropriate organizational arrangements to safeguard the fundamental rights of data subjects.

And as for these, paragraph 2 of article 21 is completely silent.

It is inconceivable how it is intended, in such an indeterminate way, to grant legality to treatments

of data in patent subversion of one of the basic principles of data protection. In addition

in addition, despite the fact that such different purposes are at stake, which imply needs

distinct in diverse contexts, there is not even an attempt to segregate the

specificities of each one, regulating everything en bloc as if from the same universe

treat.

In short, paragraph 2 of article 21 violates the principle of proportionality and the

expressly in subparagraph e) of paragraph 1 of article 5 and paragraph 1 of article 89 of the GDPR, being

therefore, its review is imperative.

1.7. data transfers

With regard to article 22 (Transfer of data), this rule suffers exactly

of the same vice already pointed out in other articles of this Proposal. It is intended to regulate in a

general provision, what must be precisely prescribed in the specific case.

In fact, the possibility of transferring personal data to countries

third parties or international organizations that do not have an adequate level of protection,

when the transfer is necessary for important reasons of public interest, and

this public interest is recognized by Union law or by State law.

Member to which the controller is subject12, does not constitute

in a rule that provides, in the abstract, that there is public interest whenever an entity

12 Cf. Article 49(1)(d) and Article 49(4) of the GDPR.

public in the exercise of its powers of authority transfers personal data in

fulfillment of a legal obligation without assessing the real context.

An identical derogation already exists in Directive 95/46/EC and in the LPDP, requiring its

naturally applying the assessment, in the specific case, if such transfer (as to the

controller, the purpose of the transfer, its purpose and the existence of

adequate safeguards) is legally required for the protection of a public interest

important13. Recognition of the public interest in the processing of personal data –

or a processing operation, such as a data transfer – must therefore

be legally provided for in the legislative act that provides for such treatment.

2. The exceptional regime for data processing by public entities

The Law Proposal presents a set of articles consecrating a regime differentiated for data processing in which those responsible or subcontractors are public entities. The perplexing provisions are contained in Article 23 and the Articles 44 and 54 of the Proposal.

2.1. Deviation of purpose

Starting with article 23 of the Draft Law, it appears that it admits that the processing of personal data by public entities may be carried out to purposes other than those for which the data were collected, provided that this is the pursuit of the public interest. Article 23 invokes several rules of the GDPR, the which, however, as will be shown, do not give the Member State the power to generally and permanently admit deviations from the purpose of treatments.

First of all, it is important to pay attention to the caveat contained in article 23 that the purposes must correspond to the public interest, as if this constituted a guarantee sufficient protection of the rights of citizens or a sufficient basis for an exception the principle enshrined in Article 5(1)(b) of the GDPR. Indeed, the legislator seems to forget that all purposes of data processing carried out by entities public services can only be in the public interest, because the function of public administration is

13 Cf. subparagraph c) of paragraph 1 of article 20 of the LPDP.

exclusively for the pursuit of public interests. For that reason, that caveat is, in itself superfluous. Moreover, this forecast still clashes with the fact that the public authorities can only pursue public interests that coincide with their respective legally defined attributions, and not any and all public interest.

Secondly, it should be clarified that the purpose principle, enshrined in subparagraph b)

of Article 5(1) of the GDPR, is a fundamental principle of the protection of personal data in Europe. It is, moreover, a principle that is explained in paragraph 2 of article 8 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. This means that personal data is collected for the pursuit of specific, specific purposes, which, in principle, can only be used for these purposes; the principle admits, however, the use of the data for different purposes insofar as these are not incompatible with the purpose original. What is inconsistent with the principle as it is enshrined is the determination that any and all processing of data, provided that it is carried out by public entities, may have any purpose other than the original one in view, since this determination corresponds to the negation of the principle itself.

Thus, it is clear that a rule of national law that allows the use of data personal data of citizens for any purpose in the public interest ostensibly violates the purpose principle and the provisions of Article 5(1)(b) of the GDPR.

Thirdly, the normative references contained in article 23 do not legitimize, as if stated above, as provided therein. Both subparagraph e) of paragraph 1 of article 6 and subparagraph g) of paragraph 1 of article 9 of the GDPR, are limited to recognizing the lawfulness of the processing of personal data when carried out to pursue the public interest (which must be qualified, 'important' where certain special categories of data are involved), i.e. legitimizing the collection and subsequent operations on personal data when justified for a specific public interest. Subsequent use of the same data for other purposes, even if in the public interest, is not justified by these paragraphs, nor could be, in view of the provisions of subparagraph b) of paragraph 1 of article 5 of the GDPR.

A more detailed explanation requires a reference to Article 6(4) of the GDPR. Which from this rule is that personal data can be used for other purposes whenever it is possible to conclude that these are not incompatible with the purpose

origin that justified its collection, listing the criteria that the Group of

Work of Article 29 (GT29)14 had already defined in an opinion15. It so happens that in the first

part of paragraph 4 of article 6 excludes the possibility of making this judgment of not

incompatibility in relation to personal data originally processed on the basis of the

consent of

data subjects or with

basis in disposition

cool.

Precisely because in these cases, personal data can only be processed for the

purpose or purposes for which the specific consent was issued (and the

specificity of consent is essentially related to the purpose of the treatment)

or for the purpose legally foreseen when the treatment is based on a legal rule, since

it is certain that the law does not and cannot provide, in accordance with the principle of finality,

data processing without a defined purpose or for general purposes.

Now, precisely what emerges from the first part of paragraph 4 of article 6 is that the data

personal data whose treatment is based on legal provision cannot be processed for other purposes.

purposes, except for a specific legal provision to that effect, which "constitutes a

necessary and proportionate', which presupposes an analysis and consideration for each new

purpose (cf. recital 50, 2nd §). Therefore, this legal provision has, obviously, under

penalty of violation of the purpose principle, of corresponding to a legal provision that

admit the

data processing for a

purpose or

specific purposes,

determined, which is clearly not the case in Article 23 of the Draft Law.

In short, the provisions of paragraph 1 of article 23 of the Draft Law ostensibly violate the

principle of purpose, enshrined in Article 5(1)(b) of the GDPR, is not

within the scope of paragraph 4 of article 6 of the same diploma, therefore this article must

be eliminated.

2.2. No subjection to the sanctioning regime

Another solution that gives rise to the greatest reservations to the CNPD is contained in articles 44 and

54 of the Draft Law. There it is determined that the fines provided for in the GDPR and in the

14 Group made up of representatives of the data protection authorities of the European Union, provided for in

Article 29 of Directive 95/46/EC – Data Protection Directive.

15 Cf. Opinion 6/2014 on the legitimate interest of the person responsible, available at http://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2014/wp217_en.pdf .

Draft Law do not apply to public entities, invoking the provisions of paragraph 7 of the

article 83 of the RGPD, regarding the administrative offences regime.

It is true that Article 83(7) of the GDPR allows Member States to define whether

public authorities are subject to fines and to what extent (see also recital

150), so a provision such as Article 44 of the Draft Law does not violate the

GDPR literal. However, it is important to understand the ratio of paragraph 7 of article 83.

In fact, Directive 95/46/EC (cf. article 24), which the RGPD revokes, gave autonomy

Member States to define appropriate measures to ensure full

application of the regime defined therein, exemplifying with the provision for the application of sanctions.

As a result, some Member States did not provide in their legislation

sanctions for non-compliance with the personal data protection regime by

public entities. It is this reality that the GDPR takes into account, when it admits that the law

national law does not provide, or provides to a certain extent, fines for entities

public authorities (see, moreover, the reference in recital 151 of the GDPR to two

where there are no pecuniary sanctions for administrative offenses or mere
social ordering). However, the legislative option adopted in the Portuguese legal system was,
since 1991, to establish the same and exact legal regime for data protection
personal data for all data controllers, irrespective of the
private or public legal nature thereof.
In order to move away from such a legal tradition and create a differentiated regime for
public information on sanctions, it would be expected that the Draft Law would present
relevant reasons exclusive to public authorities and that, therefore, if there were no
regarding private entities. strangely,
such an option does not come specifically
based on the explanatory memorandum that accompanies the Draft Law, only if
referring generically that, given the 'paradigm underlying the legislator
European [have been] that of large multinationals that manage social networks or applications
on a global scale, involving the collection and intensive use of personal data,
[…] some of the legal solutions that were created for this universe are revealed to be
sometimes disproportionate or even inappropriate for the general fabric
national business and for the Public Administration […]", adding that "the
application of this regulation will result in high administrative burdens, which in
Process No. 6275/2018 15
many cases are not sufficiently justified by the benefits obtained with the
new personal data protection regime compared to the current regime".
Not ignoring that the RGPD also aims to safeguard the personal data of
citizens in the context of the commercial activities of multinational companies, it does not seem
accurate to say that the paradigm underlying the options poured into it are the great
multinationals. Strictly speaking, what the GDPR takes as a paradigm is the technology available
today for the processing of personal data and, therefore, seeks to regulate the

use of solutions

technologies in their current state of development and,

predictably, future.

In other words, the GDPR is not only intended to regulate, or above all, to regulate

processing of personal data by large companies, because these treatments do not have

necessarily greater impact on the fundamental rights of citizens than those

treatments carried out by public entities, which process data on a national scale and

relating to the population universe of a country, not having the citizens, in most cases,

cases, such as in relation to private entities, alternative or choice.

Nor does it intend only to sanction entities that are dedicated to making a profit

at the expense of collecting and analyzing information about people, also covering all

entities that collect and analyze information about people for purposes other than

for profit, public or private.

Thus, the GDPR regime, which was also approved by the Portuguese State within the

European institutions that intervened in the respective legislative procedure, it is intended

both for global companies that are dedicated to processing personal data and for

all those who, at a global or local level, develop activities that imply

processing of personal data, because they all have an impact on the rights

fundamentals of citizens.

From this point of view, it is important to highlight that the processing of personal data carried out

by public entities (for this purpose, it is sufficient to think about the State and the various ministries

that compose it) are just as or more intensely intrusive of the privacy and freedom of

citizens, than those carried out by private entities, and therefore as or more

potentially restrictive of citizens' fundamental rights. So the risks to the

Process No. 6275/2018 15v.

protection and security of personal data are asserted in this context with as much or more

intensity than in the scope of activities of private entities.

It is true that, from the perspective, which is the one that is of main interest here, of the protection of the fundamental rights of data subjects, the application of a sanction or, at least, the the possibility of imposing a sanction has a deterrent function of the violation or the reiteration of the violation of those rights, the exclusion of public entities from the sanctioning leaves data subjects vulnerable in relation to data processing carried out by the State and other public entities.

Even knowing that article 11 of the Penal Code excludes, as a general law, the criminal liability of public legal persons, the CNPD reiterates that the fundamental goods protected by the GDPR and the Draft Law can be carried out with as much or more intensity by public entities than by private entities, considering further that the mission that the Portuguese Constitution assigns to the State Portuguese in the defense of those fundamental goods would justify greater accountability of this and not its exemption.

Furthermore, the statement that 'the application of this regulation will result in administrative overhead, which in many cases are not sufficiently justified by the benefits obtained with the new personal data protection regime in relation to the current regime', constitutes, as mentioned above, a statement of principle that the weightings of the European legislator expressed in the GDPR did not have a result balanced and that, therefore, the public authorities will compensate, in a first phase of application of the GDPR (cf. article 59 of the Proposal), does not comply with the regulation. Well, the expression of this judgment not only encourages public entities by delaying compliance with the GDPR, as it runs the risk of inspiring private entities to follow the same path, to in addition to questioning the role and performance of the Portuguese State as a co-legislator in the within the Council.

Therefore, there is no reason to exclude from the administrative and criminal sanctions regime

public entities. Under penalty of having to conclude by the violation of the principle of
equality, enshrined in article 13 of the CRP: the same restriction of the fundamental right
to the protection of the data of a specific citizen, in violation of the GDPR and the Constitution and law
Process No. 6275/2018 16
Portuguese crimes, perpetrated by a private entity, justifies the application of a sanction
payment to this entity, but no longer when carried out by a public entity.
It is reiterated that, contrary to what happens in other national legal systems in
European Union, where the susceptibility of a public entity to apply pecuniary sanctions
the other public entity would constitute a novelty, therefore posing new challenges
legal matters, namely in terms of the budget and management of public accounts, this
forecast in Portugal does not matter any news.
Moreover, it is important to remember that in the national legal system this possibility is not
restricted to the administrative offense sanctioning regime. It is recalled that the Portuguese State
approved, within the scope of the reform of administrative litigation in 2002, a rule that
subjects public entities to the obligation to pay court costs in the context of proceedings
in which they are a part. And, in the recent Bill No. 119/XIII/3rd (GOV), which establishes the
legal framework for cyberspace security, transposing Directive (EU) 2016/1148 of the
European Parliament and of the Council of 6 July 2016 on measures to
ensure a high common level of network and information security across the Union,
the solution found was to sanction public entities, without therefore understanding that the
The need for technology regulation is more intense in the private sector than in the
public.
There are therefore no new legal or financial issues that could justify
this discriminatory solution.
In short, the CNPD understands that the provisions of articles 44 and 54 of the Draft Law, when
not subjecting or exempting public entities from the sanctioning regime, violates the principle of

equality and weakens the protection of citizens' fundamental rights in the context of

processing of personal data carried out by public entities.

3. Matters of mandatory regulation by the national legislator

3.1. Accreditation and certification

With regard to article 14 of the Proposal, the option taken here is to attribute to the

IPAC, IP (Portuguese Accreditation Institute, IP), the competence of accreditation of

entities to which, in this way, will be recognized powers of certification of

Process No. 6275/2018 16v.

data treatments. This option is allowed by Article 43(1) of the GDPR16, but

depends on the CNPD's abstract definition of additional requirements or criteria for

accreditation.

However, paragraph 2 of article 14, when prescribing that IPAC take into account the

additional requirements established by the CNPD, when they exist, seems to presuppose that the act

of accreditation can be issued without further ado by IPAC, IP, while those requirements

additions are not approved.

However, it has already been mentioned that the European legislator did not leave room for the Member States to

regulate the accreditation and certification regime in different terms or in addition to the

which is established in articles 43 and 42, respectively. Therefore, paragraphs 2 and 3 of article

14 should, in this perspective, be eliminated.

Without prejudice to what has just been stated, it is important to point out aspects that, in any case,

would always deserve to be corrected.

Firstly, said additional requirements may not only be those approved

by the CNPD, since the RGPD recognizes the European Committee for the Protection

of Data the power to adopt additional criteria (cf. Article 43(3)).

On the other hand, it is indisputable that Article 43 makes accreditation dependent on the definition

prior notice of the additional requirements by the CNPD or the Committee. This is not, therefore, a

dispensable assumption; on the contrary, the GDPR assumes that when the entity

accrediting authority is other than the national data protection authority, that

has expertise in the protection of personal data, so the

accreditation of certification bodies in this area necessarily depends on the

fulfillment of the requirements that this authority or the Committee may establish.

Therefore, even if it were possible for the national legislator to regulate this matter, it would never

could do so without deleting the final part of paragraph 2 of article 14 which reads "when

exist", under penalty of ostensibly violating article 43 of the GDPR.

Likewise, the wording of paragraph 3 of article 14 reveals an error regarding the definition of the

object of certification. Strictly speaking, in accordance with Article 42(1) of the GDPR – where

16 But not in the Portuguese version of the GDPR, where, once again by gross error, the intervention of the two

entities is presented as cumulative.

recognizes the creation of certification mechanisms for the purpose of proving the

compliance of processing operations carried out by controllers and subcontractors –,

object of the certification are the data treatments (operation or set of operations of

data processing) carried out by a controller or subcontractor attached to a

specific purpose or for specific purposes.

Thus, even if it were possible to provide for certification, the wording of paragraph 3 of article

14, by establishing that certification focuses on procedures, would be violating article

43 of the GDPR. Indeed, if it is true that certification may concern a procedure,

it is also certain that it can affect products (a software, for example) implemented

by a responsible person or subcontractor, as well as about a service insofar as this

involves data processing operations in the relationship between the person responsible or a

subcontractor, on the one hand, and the customer or user, on the other hand (for example, the

e-mail).

In short, the wording of paragraph 3 of article 14 does not comply with the GDPR and would always have at least

less than ensuring that the object of certification was not more restricted than what arises

of the GDPR.

3.2. children's consent

With regard to paragraph 1 of article 16, the CNPD understands that the wording of the precept

needs to be revised, otherwise there will be doubts as to its scope of application.

In fact, from article 8 of the GDPR it follows that when dealing with the

offer of that type of service, and only in this case, the consent of the child is only relevant

if she is at least the age determined by national legislation (between 13 and 16 years old).

Regarding the age limit set in the Draft Law, the CNPD limits itself to noting that the

ratio of the GDPR was to let each Member State adjust the regime of the

children's consent to the national legal regime, depending, therefore, on the age

as relevant in each legal system for decisions about your life. In this point,

therefore, the RGPD did not intend to homogenize the regime, admitting solutions

differentiated in each state. However, since it is at stake to determine from what age

recognizes that a child has the capacity to consent to the restriction of a fundamental right,

Process No. 6275/2018 17v.

it would perhaps be expected that in the Proposal the criterion set in the

Penal Code, in article 38, no. 3, regarding consent as a reason for excluding

Criminal offense: 16 years. The argument, expressed in the explanatory memorandum that 13 years was

the age considered in a large number of Member States17 does not appear to be

decisive in a matter that the European legislator clearly left open for

harmonization of the solution in each State with the criterion assumed in the respective

national legal system.

3.3. Data processing for purposes of freedom of expression and information

Article 24 of the Draft Law seeks to implement the command contained in article 85.

GDPR in order to reconcile, by law, the right to data protection with the rights to freedom of expression and information.

However, the simple statement, in paragraph 1 of article 24 of the Draft Law, that the protection of personal data does not prejudice the exercise of those freedoms seems little enlightening and, to that extent, irrelevant. Likewise, the determination that certain rights of the holders of personal data must be "exercised within a framework of consideration with the exercise of freedom of information, press and expression academic, artistic or literal" is a poor contribution to the definition of a regulatory framework for the exercise of these rights.

In fact, if it is understood that the right to the protection of personal data cannot prevail over freedom of expression, information and the press, under penalty of individual expression and journalistic activity, essential in a democratic society, are not develop, it is also understood that those freedoms cannot crush the substantive legal dimensions protected by the data protection regime, in particular private and family life, individual freedom and the right to treatment discriminatory. For this very reason, the statute of journalists itself safeguards the protection of personal data, a fact that this Proposal for a diploma could not ignore.

For this reason, it was necessary to define here a set of rules that were sufficiently precise to ensure a balance between such fundamental rights. To that end, it would be better

17 Only five Member States have already passed national legislation implementing the GDPR

distinguish freedom of information and freedom of the press, on the one hand, from freedom of expression, namely for academic, artistic or literary purposes, on the other.

Freedom of information and of the press, as they are implemented within the scope of the exercise of a regulated professional activity – the journalistic activity –, are already in the statute journalists a harmonizing regime of the rights in tension, not requiring, therefore,

special regulation. In any case, it is important to note that freedom of information
must be developed with respect for the rights of data subjects and the principle of
dignity of the human person, justifying the inclusion in paragraph 4 of article 24 that its
exercise must be carried out within the framework of the regulated professional activity, rather than that
reference is provided for in a separate number.
On the contrary, the harmonization between freedom of expression and the rights of holders of
personal data demands greater attention from the legislator, which are not enough with formulas
generic terms such as those set out in paragraph 1 and paragraph 2 of article 24 of the Draft Law and that
they add nothing to the provisions of article 18 of the CRP. In principle, freedom of
expression, namely academic, artistic and literary, is subject to the regime of
protection of personal data, in particular the legal conditions provided for in articles 6 and
9 of the GDPR and the principle of minimization, and should therefore be specifically
any provision that departs from those rules is justified by the national legislature.
In this sense, a forecast of the type contained in paragraph 6 of article
24, which implements the principle of proportionality in the scope of the exercise of freedom of
expression. However, its wording raises doubts. In fact, either a comma is missing
following personal data, or is the judgment of proportionality limited to the data of
address and contact details, which is objectively inadmissible, when you think about all the
sensitive data that the European legislator and the constituent legislator wanted to protect
in particular, prohibiting as a rule their treatment.
3.4. Data processing for archiving purposes in the public interest, research purposes
scientific or historical or statistical purposes
The GDPR provides for a set of data processing situations in which it recognizes
Member States regulatory autonomy to ensure the application of the regime provided for therein and

define an appropriate balance between the interests of public archival, research and

scientific or historical and statistical and fundamental rights of data subjects

personal. For this purpose, it requires the adoption of adequate data protection measures.

and allows derogations in relation to certain rights of data subjects – cf.

Article 89 and recitals 156-163.

First of all, it is important to note that article 89 of the GDPR, while recognizing autonomy for

Member States to regulate data processing for archiving purposes of interest

public, scientific or historical research purposes or statistical purposes, imposes first

the duty to provide adequate guarantees of the fundamental rights of the holders of

data under the GDPR. In fact, in line with the provisions of subparagraph j) of paragraph 2 of the

Article 9 of the GDPR, which makes it dependent on whether the national law is sufficient to

legitimize the processing of data for these purposes of the legal provision of measures

appropriate and specific for the defense of the fundamental rights of data subjects,

with respect for the principle of proportionality and the essential content of the right to

personal data protection. Only then, in paragraph 2 of article 89, is it admitted that they are

derogations to certain rights of holders provided for in the GDPR are established.

Therefore, the national legislator cannot limit itself to repeating the provisions of paragraph 1 of article

89, with generic statements regarding the need to adopt technical and

organizational structures and their subordination to the principles of article 5 of the GDPR, and to be defined

also general derogations to rights, if in fact it intends to create special regimes

for the processing of personal data for these purposes. It is imperative to define the

specific regime for processing personal data.

But it is also important to draw attention to the fact that the solutions to which the national legislator

arrive, in this context, can hardly be common to the different

purposes

set out in article 89, because each of them justifies or can justify

different regime. In fact, so much so that there are national laws specifically regulating the

public interest archive, as well as statistical activity and clinical research. Per

That's right, the CNPD understands that the national legal regimes admitted by article 89 of the

RGPD must contain densified and specific rules, which translate an effective

balance between each of the interests in view and the fundamental rights of the holders

data, with provision of technical and organizational measures that for each type of

purpose are adequate to safeguard the right to protection of personal data and

providing for the conditions for the exercise of the rights of the data subjects provided for

in the GDPR to the extent that any derogations prove to be essential for

ensure the pursuit of each type of purpose.

Thus, analyzing article 31 of the Draft Law, it is concluded that the rule of paragraph 1 has little

adds to the provisions of Article 89(1) of the GDPR, limiting itself to mentioning the

anonymization and pseudonymization measures, without specifying the indispensability that

such measures are suitable and sufficient for the protection of the fundamental rights of the holders

data, as required by Article 9(2)(j) of the GDPR. To that extent, the CNPD

recommends its elimination.

With regard to the rights of data subjects, in paragraph 2 of article 31 of the Proposal,

no weighting is, strictly speaking, made in the light of the principle of proportionality, in particular,

in terms of necessity. It is stated that the rights stated therein are harmed in the

as necessary, without any evaluative judgment depending on the different purposes

considered. And yet, when you think that some of the rights at stake

correspond to the essential content of the law

fundamental to self-determination

information, enshrined in paragraph 1 of article 35 of the CRP and in article 8 of the Charter of Rights

Fundamentals of the European Union, such as the right of access, are easily

realizes that it cannot be denied except in very exceptional circumstances. In that

In this sense, the CNPD recommends that this precept be revised, differentiating the regimes in depending on the purposes of the treatments. Thus, the CNPD understands that when the treatment for archiving purposes in the public interest, it does not seem to make sense to deny the right to access to data subjects, it is difficult to conceive that it is possible to deny the rights of rectification and limitation. In fact, it is not clear to what extent the exercise of these rights seriously impair or make it impossible to carry out the end-of-file of public interest. Only the right of opposition seems capable of being sacrificed in the face of public interest purpose of data processing.

A similar judgment of necessity applies when the purpose of the treatment is the investigation scientific or historical. In fact, the exercise of the rights of access and rectification by part of the data subject appear to be compatible with the research purpose, it is not glimpsing under what circumstances its pursuit may be harmed or

made impossible by that. But also the rights of limitation and opposition do not make it impossible or appear likely to seriously prejudice the investigation scientific research (where treatment is usually based on the consent of the data subject), as opposed to what happens in historical research where the right of opposition can harm seriously the same, so the CNPD believes that the legal derogation of this right for that purpose.

With regard to statistical purposes, except for exceptional situations to be provided for in the legislation In particular, the exercise of the rights of access, rectification and limitation does not affect your pursuit. In relation to the right of opposition, insofar as it is at stake carrying out an activity of public interest and, in some cases, corresponding to a legal obligation, their removal is justified, under penalty of seriously harming the statistical purpose.

In short, considering that fundamental dimensions are at stake in the context of

processing of personal data, the derogation of the rights of access and rectification cannot be determined without a specific foundation that fulfills its need, which as a rule it will not happen. The rights of limitation and opposition may, in relation to some of those purposes, be removed by legal determination.

As for paragraph 3 of article 31, the reference to Decree-Law n.º 16/93, of January 23, as it does not contain any personal data protection rule, therefore it is not known in what terms the rights of data subjects are weighted with that interest. Consequently, the CNPD recommends its densification or, if so it is not understood, the elimination of this paragraph 3.

Finally, Article 31(4) provides for a derogation from the purpose principle also in terms that deserve criticism. The standard focuses on consent for purposes of scientific investigation, to admit a generic consent. In fact, it determines that consent can cover several areas of investigation, which contradicts the requirement of the specificity of consent developed in Article 4(11) of the GDPR.

Specificity concerns, from the outset, the purpose of the treatment, not can be considered specific, this is circumstantial, a statement of agreement to the processing of personal data for any investigation or for any investigation in different areas of science. Consent must be given

for concrete and delimited projects, otherwise it will not be possible to perceive what is consenting, only admitting that in exceptional and duly justified consent covers parts of the project that may not be determined at an early stage of the investigation (cf. recital 33 of the GDPR) In fact, even the right to information, which requires free and informed consent, must be provided in in relation to delimited purposes, and it cannot be considered fulfilled with a

generic information on open purposes of processing (cf. subparagraph c) of paragraph 1 of the

Articles 13 and 14 of the GDPR).

The CNPD therefore recommends reviewing paragraph 4 of article 31, in order to comply with the

principle of purpose and the consent requirements provided for in the GDPR, under penalty of

have that rule for not complying with the GDPR.

3.5. Audience of interested parties and cooperation and coherence mechanisms

It is also important to take care of another aspect that stems from the one-stop shop model adopted

by the GDPR in the context of cross-border processing (i.e. a single processing authority

competent control to interact and assess the compliance of data processing

carried out by a company with establishment(s) in the territory of several States.

Member States, or the processing of data that affects persons in more than one Member State

- cf. Article 4(23) of the GDPR) and the application of the coherence mechanism provided for in

article 63 of the RGPD and which is related to the guarantee of contradictory or defense of the

interested parties, in particular data subjects.

Under the one-stop shop mechanism, in the context of cross-border processing

in which the controller18 or the processor19 has its establishment

principal20 in another State of the Union and the processing affects persons who are in the

Portuguese territory, the supervisory authority competent to assess and decide it will not be

18 Cf. Article 4(16)(a) GDPR.

19 Cf. Article 4(16)(b) GDPR.

20 On the densification of the concept of “main establishment” for the purpose of classifying a

particular supervisory authority as the lead authority, reference is made to point 2 of the Guidelines on

the identification of the lead supervisory authority of the controller or processor, the

GT29, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.

the CNPD but the national authority of the other State (cf. article 56 of the GDPR). Still

therefore, the CNPD, under the terms of article 4, no. 22, of the RGPD, should be considered a
the supervisory authority concerned21 on the grounds, by chance, of having received a possible
participation of the data subject, being as a rule through it that the data subject asserts his
interests in the procedure (from the outset, ensuring that it is done in the
Portuguese). Furthermore, the CNPD will have the opportunity to present its perspective to the
competent national authority, and if there is no consensus as to the content of the decision between
the two authorities, the European Committee, within the framework of the coherence mechanism, will be the
to settle the dispute and to determine the meaning or the criteria to be taken into account for the decision to be taken.
apply in the specific case (cf. Articles 63 and 65 of the GDPR).
Reflexively, the same will happen, as it is primarily up to the person responsible for the
treatment or subcontractor define which lead supervisory authority with whom
should interact, when the CNPD is only considered a supervisory authority
interested party and disagree with this classification, which should be clarified directly with the
of the controller or the processor, without waiving the
consultation with the other interested (or main) control authorities is necessary.
There and until the doubt is clarified, the CNPD will maintain the quality of control authority
interested party, but may, however, 'require [directly] the controller to
provision of additional information necessary to demonstrate where your
main establishment»22.
Another of the situations in which the CNPD will maintain a leading role, but will not be
originally considered the main authority under the GDPR, will be those in
that the supervisory authority legally defined as the lead authority decides not to handle the
case23 and the supervisory authority concerned is Portuguese. It will therefore be up to you to
21 That is, «a supervisory authority affected by the processing of personal data by the fact that: a) The person responsible
for the processing or the processor is established in the territory of the Member State of that processing authority
control; (b) data subjects residing in the Member State of that supervisory authority are

substantially affected, or likely to be, by the processing of data; or c) A submission has been

complaint to that supervisory authority'.

22 Points 2.1.1 and 2.1.2 of the aforementioned guidelines.

23 Cf. point 3.1 of the aforementioned guidelines.

conduct all the procedures necessary for the “good decision of the case” and assume the

entirety of the process.

However, within the scope of these procedures, it is important to ensure the right to be heard by the

interested parties, in particular, the interested party before the body with decision-making power. In

first phase, it is possible that this hearing will take place before the CNPD, which will then send

declarations by the interested party to the competent national authority. but arising

new elements relevant to the decision, it is important to ensure that the interested party is

heard again, which, in order to speed up the procedure, may have to take place before the

Committee (which must guarantee the exercise of the right expressed in Portuguese). IT IS

precisely this possibility that has to be provided for by law, so that it is considered

fulfilled, under Portuguese law, the duty of hearing when it has to be

exercised before another entity than the CNPD. In this sense, the CNPD recommends the

introduction of a rule that safeguards the interested parties' right to be heard, under the terms

of article 121 of the Code of Administrative Procedure and under the terms of article 50 of the

General Regime of Administrative Offenses, and which specifies the legitimacy of an authority

of control of another Member State or the Committee to fulfill the duty of hearing.

As is clear from what has been described above, when the CNPD assumes the quality of

main supervisory authority, it will be responsible for leading the process in question and interacting with

the controller(s) or processor(s) to the extent necessary and take

due account of the views of the other (interested) supervisory authorities. Therefore,

important will be to provide in Portuguese legislation causes for suspension of the process

directly linked to this circumstance of plurinational concertation, to avoid that these

new procedures may, by themselves, affect the effectiveness of the CNPD's decisions in

Portugal and, as a result, jeopardize the entire one-stop shop mechanism, as well as the

consistency in the application of the GDPR within the Union.

4. The system of administrative offenses

It is now important to focus attention on the system of administrative offenses dealt with by the

articles 37 to 45 of the Draft Law, with the exception of the provisions of article 44, which has already

object of appreciation above, in III. 2.2.

Process No. 6275/2018 21v.

By way of introduction, it is clarified that the CNPD is not indifferent to concerns about the

sanctioning framework provided for in the RGPD felt by the different actors in the

processing of personal data, especially by those who assume the role of responsible for the

treatment or subcontractor. The maximum limits defined in article 83, paragraphs 4 and 5, of the

GDPR, are objectively high and perhaps excessive when considering the level

general income in Portugal and the economic situation of organizations with

establishment in Portugal that process personal data. The CNPD is,

therefore, aware that the concrete application of that article and the fixing in each case of

a fine must be accompanied by a careful weighing of different factors

(e.g., the economic situation of the agent and the economic benefit resulting from the infraction), in the

context of the Portuguese reality.

However, the model on which the GDPR is based should not be forgotten, when it reserves

for supervisory authorities, prerogatives of action that are not limited to

necessarily on the national “agents” to whom they could potentially apply

sanctions of this type. It should be recalled, in this respect, the case of the control procedure of

coherence, explicitly provided for in article 63, but embodied in several norms of the

GDPR24. In such cases of cross-border processing (cf. article 4, paragraph 23) and

irrespective of whether the national supervisory authority (CNPD) appears as the supervisory authority main control (cf. article 56) or the supervisory authority concerned (article 4, paragraph 22), the consideration that will have to be carried out, also and still in the case of eventual application of fines (cf. recital 130), will respect situations of responsible for the processing with economic and technical capacity to carry out data processing simultaneously in several countries of the Union. It is not necessarily indisputable that whoever do so in this transnational context already reveals, in the abstract, a distinct economic situation of a great part of the national companies (more robust, therefore), we will have, however, to admit that this will indicate a context where the consideration of economic factors may fully justify the imposition of fines closer to the ceilings determined by the GDPR.

The CNPD also recognizes that, in terms of sanctions, legal diplomas (of the Union or national authorities) must delimit the exercise of power by administrative authorities to

24 In particular, article 65, no. 1, al. a), in conjunction with article 60(4).

determination of an administrative offense sanction through the most objective criteria possible, without thereby exhausting the decision-making autonomy necessary for the indispensable appreciation of the specific circumstances of a case. To that extent, it is always preferable legal solutions that define sanctioning frameworks with a smaller amplitude (between the minimums and maximums). Even when the legislative option is different, as in the case of GDPR, precise valuation criteria must be foreseen, not only to serve as a solid orientation of the valuation to be carried out by the administrative authority, as also so that the path taken by the administrative entity can be repeated and, possibly corrected by the courts.

4.1. Legal framework of sanctions

In a regulatory framework intended to be uniform across Europe, the maximum

defined in paragraphs 4 and 5 of article 83 of the GDPR do not appear to be able to be removed by the

Member States of the Union.

The. This is the first point to focus on. Assess whether or not the GDPR leaves room for

that Member States set lower ceilings than that set out in that article.

The solution provided in paragraph 2 of articles 37 and 38 of the Draft Law seems to be based on the

understanding that the regulatory autonomy recognized by the European legislator to

national legislators allows to reduce, in abstract, the maximum limits of the GDPR according to

of certain criteria. In fact, the two articles define different sanctioning frameworks in

depending on the size of the companies and the collective or singular nature of the subjects that

perform data processing.

It is true that the preamble to paragraphs 4 and 5 of article 83 of the GDPR clearly assumes that the

pecuniary values entered there – 10 million euros and 20 million euros, depending on the

serious or very serious offence, or a percentage of turnover in the

company case – these are maximum limits and, therefore, it directly follows that the fines

they cannot exceed them under any circumstances.

But a careful reading of article 83 shows that it is aimed at defining the

limits on the application of fines by the supervisory authorities, i.e., it is addressed to each

national supervisory authority (in a judgment obviously liable to be controlled by the

Process No. 6275/2018 22v.

courts) and not the national legislator. It is enough, moreover, to compare the wording of paragraph 1 of article

83 with that of no. 1 of article 84: in that case, the addressees of the rule are the authorities of

control, this is addressed to the Member States, in their capacity as legislator. By the way,

the only provision of article 83 addressed directly to the national legislator, the one contained in the

7, had, precisely for this reason, to adopt a different wording from that of the other

Article numbers: 'Member States may provide'.

So much so that paragraph 9 of article 83 expressly provides for the direct applicability of the

article by the supervisory authorities when there is no national law25. and the reading of

recitals 150 and 148 reinforce this interpretation, highlighting that the provisions of

Article 83 is intended to direct and bindingly guide the supervisory authorities – in the

recital 150 reads 'This Regulation should define the breaches and the

maximum amount and the criterion for setting the value of the fines resulting therefrom, which should

be determined by the competent supervisory authority in each individual case'.

In the same vein, the other Union control authorities looked at this

question. In the guidelines on the application and setting of fines for the purposes of the Regulation

2016/67926, of GT29, at no time is considered, admitted or problematized the

possibility for Member States to determine criteria other than those

provided for in article 83, paragraph 2, and different frameworks from those set out in article 83, paragraphs 4 and 5.

The only circumstance in which freedom of modeling is allowed by each State is

concerning the enforcement of sanctions, 'This may in particular include

address notices, forms, deadlines for filing claims, appeals,

execution and payment'27. Immediately afterwards, however, he warns of the need for "such

requirements shall not[re]m

prevent, in practice, the achievement of effectiveness,

proportionality or deterrence. A more accurate determination of effectiveness,

of proportionality or deterrence will be carried out on the basis of emerging practice

within the supervisory authorities (in terms of data protection, but also

lessons learned from other regulated areas), as well as in the case law resulting from the

interpretation of those principles.'

25 In fact, the absence of this national law has nothing to do with the absence of a national definition of limits to the

sanctions, but rather with the absence of regulation, in certain Member States, of sanctions of this type.

26 Available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

27 Cf. P. 6 of the cited guidelines.

Thus, it has to be concluded that the GDPR left to the supervisory authorities the power to apply specifically fines in the maximum amounts provided for therein, naturally with the weighting the guiding criteria for calculating the fine referred to in article 83.

Hence, the establishment in abstract, in national law, of maximum limits lower than those foreseen in paragraphs 4 and 5 of article 83 of the GDPR constitutes a violation thereof. this conclusion is supported by the case law of the CJEU, in the judgment in Commission v Italian Republic (proc. 39/72); referring to legislation passed in the Italian Republic, the Court states that

'Any implementing arrangements which might impede the effect of Community regulations and thereby jeopardize their application simultaneous and uniform in the community space» – jurisprudence reiterated in the Variola judgment (proc. 34/73).

It is certain that the principle of the primacy of European Union law, enshrined in article 288 of the TFEU, it follows that regulations have mandatory value and are directly applicable in all Member States, thereby ruling out any possibility of a «State [...], unilaterally, annul its effects by means of an enforceable legislative act Community texts' (cf. the aforementioned judgment of the CJEU Costa/ENEL, case 6/64).

Furthermore, nowhere in Article 83 or in the recitals relating to the sanctions, space is opened for the autonomous consideration of the size of the company, by that the criterion adopted by the national legislator, to distinguish small and medium-sized companies to reserve the GDPR maximum cash limit for large companies, constitutes in itself a violation of the GDPR.

In this regard, it is important to remember that the importance recognized in the of the GDPR to small and medium-sized companies, contrary to what happened in the initial proposal for regulation, because it was concluded, within the institutions of the Union,

that the impact on personal data resulting from the conduct of those responsible for processing of personal data (and subcontractors) does not depend on the number of workers who are part of these organizations, but before the nature of the activity developed (categories of processed data, volume of processed data, categories of data subjects being processed, etc.). To that extent, the elevation at the discretion delimiter of the sanctioning frameworks of the size of the company contradicts the GDPR and the ratio underlying it.

Process No. 6275/2018 23v.

The same conclusion is reached in relation to the differentiation of sanctioning frameworks for natural persons. Once again, nowhere in Article 83 of the GDPR is distinguishes the regime according to whether the offense is committed by a legal person or by a person singular. It is only in recital 150 that the concrete fixing (by supervisory authority) of fines to persons other than companies – which covers also legal persons of a non-business nature, of private or public law – should take into account the general level of income in the Member State as well as the situation economic status of the person in question. Therefore, the GDPR, even in the recital, only admits that the maximum pecuniary limits are removed in concrete, in the weighting carried out by the supervisory authority. Moreover, in recital 148, it is admitted that 'if the amount of the fine liable to be imposed would constitute a disproportionate burden for a natural person, a reprimand may be issued instead of a fine being imposed', the which clearly shows that the framework of pecuniary sanctions in which the supervisory authority (in Portuguese case, the CNPD) moves must always be as provided for in paragraphs 4 and 5 of article 83, irrespective of the nature of the legal or natural person of the offender.

On the grounds set out above, the CNPD understands that the definition of maximum limits pecuniary amounts lower than the maximum pecuniary limits established in the GDPR violates this legislative act of the European Union and the principle of the primacy of Union law enshrined in the

Treated.

B. The same reasoning must apply to the setting of minimum limits, since the GDPR

does not leave room for the national legislator to define a different sanctioning framework than

is set out in paragraphs 4 and 5 of article 83 of the GDPR.

When it determines that 'Breach of the provisions set out below is subject, in

pursuant to paragraph 2, to fines up to ...', the GDPR exhausts the legislative power of

Member States regarding the definition of the sanctioning framework in relation to infringements

provided for in those numbers. Admitting only that power, under the terms of article 84 of the

GDPR, regarding the definition of criminal sanctions for the violation of the GDPR or to sanction

with a fine for breaches of GDPR provisions not sanctioned in article 83.

For the rest, the minimums, as set out in the Draft Law, would always give rise to

reservations, first of all because, as far as natural persons are concerned, a limit is foreseen

lower than expected today in the LPDP. When one is aware that the GDPR intends

Process No. 6275/2018 24

strengthen the protection of personal data, defining a sanctioning framework particularly

heavy, cannot but conclude from the disproportionate and ineffective character of

a legal rule that sets a lower limit than the minimum limit set in the national law of

twenty years ago, therefore, in violation of the provisions of the GDPR (cf. paragraph 1 of article 83).

ç. Moreover, the fact that the GDPR only refers to the maximum amount of the fine allows us to deduce that the

sanctioning regime thus established follows a sanctioning model similar to that of the

competition, set out in Regulation (EC) No. 1/2003, of the Council of 16 December

2002 (cf. article 23), and which inspired the model enshrined in the national

competition approved in Law no. 12/2012, of 8 May (see article 69). In this regime, the

maximum value of the fine presents itself as an insurmountable ceiling or threshold in the process

specific way of determining the fine, which takes as a reference an 'amount

baseline', from which the different criteria or mitigating factors apply and

aggravation.

In fact, the fact that the GDPR has only defined the maximum fines points to the meaning that they do not act as «[…] the maximum limit of a legal measure of the sanction, but [rather as] an insurmountable threshold in an operation to determine the sanction that is not guided by it»28. And that in the concrete application of article 83 the supervisory authority can (and must) only make use of the criteria defined in paragraph 2 of the same article, in order to determine the specific amount of the fine to be imposed, without appear to be able to meet other criteria laid down by national law.

To avoid possible judgments of unconstitutionality arising from the violation of the principle of the legal determination of the fine (as the administrative control authority is responsible for a very broad discretion in the concrete definition of the fine), it is admitted to recognize in this maximum set by the GDPR a true maximum of a legal sanction measure, with effective guiding function in the process of concrete determination of the fine29, to which join the criteria of paragraph 2 of article 83, inferring from paragraphs 4 and 5 of the same article

28 JOSÉ LOBO MOUTINHO, «Portuguese legislator. Need - Some notes on the sanctioning regime in the General Regulation on Data Protection (Regulation (EU) 2016/679)», in Forum on Data Protection Data, No. 4, January/2017, CNPD Edition, p. 40- (p. 53).

29 In this sense, LOBO MOUTINHO, ob. cit., pp. 53-55 and German case law cited therein.

that this minimum is 0. This solution would allow the applicator of the standard (control authority or court) determine a value between the maximum and the minimum, as a starting point for the fine calculation.

4.2. Criteria for determining the amount of the fine

The Draft Law assumes in article 39 three criteria for the concrete determination of the fine, in addition to those set out in Article 83(2) of the GDPR. As mentioned, the European legislator does not seem to leave room for the Member States to come

define other weighting criteria in relation to the infractions provided for in paragraphs 4 and 5 of the article 83. Only under article 84, therefore, for offenses not sanctioned in the GDPR, is that it will be possible for the national legislator to add criteria, as long as they guarantee sanctions that are effective, proportionate and dissuasive.

It is true that Article 83(2)(k) of the GDPR admits the consideration of other aggravating or mitigating factors applicable to the factual circumstances, such as benefits economic gains or losses avoided as a result of the infringement. The question that prevails is whether the choice of factors should not be made only in the specific case, by the entity (administrative or judicial) that apply the specific rule, and no longer by the legislator national of each Member State. It appears, therefore, that the provisions of article 39 of the Proposal or the criteria of the General Regime of Administrative Offenses cannot be considered in the scope of the offenses listed in article 83 of the GDPR.

In any case, and in the event that the national legislator intends to maintain the provisions of Article 39 for possible new sanctions, it is always noted that the criterion provided for in Article 39(1)(a) of the Proposal seems to confuse two distinct aspects, one relevant, another irrelevant.

In fact, it is necessary to consider the economic situation of the agent, in the case of a person individual, or the turnover and annual balance sheet, in the case of a legal person. THE consideration of the offender's economic situation, also provided for in article 45 of the General Administrative Offenses, is specified in recital 150 of the GDPR, although only for people who do not have a business nature. It is, however, important to note here that the turnover and annual balance sheet of a legal person does not depict

necessarily the economic situation of the company, so this would be the define a different regime for legal persons and natural persons, to the detriment of of the former in a regime aspect that does not seem to justify special differentiation in light of

of the principles of equality and justice.

On the other hand, the Draft Law seems to want to limit itself in this paragraph to legal persons of a business nature (when referring to the turnover), which is strange because leaving out of the criterion of economic situation legal persons deprived of non-profit purposes profitable. However, there is no relevant reason not to consider the economic situation of such organizations when the amount of the fine is being set, concluding here too for violating the principles of equality and justice.

It should also be noted that the criterion defined in subparagraph b) of paragraph 1 of article 39 is already covered by the criterion established in point a) of paragraph 2 of article 83 of the GDPR, when orders the duration of the infringement to be taken into account, so its autonomy in this article 39, as if it corresponded to a different criterion, constitutes an unnecessary repetition and which only creates confusion.

Inadmissible, in view of the GDPR, is the reference, in subparagraph c) of paragraph 1 of the same article 39, the size of the entity, taking into account the number of workers and the nature of the services provided. This is, as mentioned above, a criterion not accepted by the GDPR, by the irrelevance of company size when it is certain that a company with one or two workers can affect in a particularly intense way the fundamental dimensions of people – for example, a company that provides a computer application (app) through which sensitive data shared with third parties is collected and even transferred to territory outside the Union. It is certain that within the scope of the respective European legislative procedure this criterion was initially considered, in order not to be accepted in the text of the pleading, with very few exceptions. From which it follows that the imposing their weighting contradicts the GDPR and should therefore be eliminated. as if mentioned, the only number to which the supervisory authority should pay particular attention is, in the specific case, to the holders of personal data affected by the breach, this, yes, provided for in Article 83(2)(a) of the GDPR.

4.3. The typification of administrative offenses

It is also noted that in the Draft Law an effort is made to classify the illicit misdemeanors. However, considering the case law of the CJEU referred to above in II.2, the CNPD understands that the GDPR leaves no room for Member States to introduce amendments to the sanctioning regime provided for in paragraphs 4 and 5 of article 83. with the same grounds, the national legislator should not repeat the rules of the GDPR.

To that extent, the CNPD recommends the elimination of paragraph 1 of article 37, with the exception of the point (e) and point (l), concerning the obligations that Member States may define in the scope of matters covered by articles 85 et seq. of the GDPR, as well as the subparagraph u) of paragraph 1 of article 38 of the Proposal.

In any case, it will always be said that some of the provisions set out in paragraph 1 of article 37 and 38 of the Draft Law violate the GDPR, as is the case with paragraph h) of article 37.

In it, regarding the failure to provide information under the terms imposed by articles 13 and 14 of the GDPR, the relevant information is distinguished from the non-relevant (whose omission would give rise to a serious misdemeanor), a distinction that is neither consecrated nor recognized in article 83 of the GDPR.

In fact, in subparagraph b) of paragraph 5 of this last article, it is sanctioned as a misdemeanor very serious violation of the rights of data subjects under Articles 12 to 22, not distinguishing, nor leaving space to distinguish according to the elements information omitted. Consequently, paragraph 1(b) would always have to be deleted. of article 38 of the Proposal.

Furthermore, where the Draft Law could have autonomously provided for punishable, limited itself to qualifying as a very serious infraction "Violation of the rules provided for in chapter VI of this law".

In fact, in subparagraph l) of paragraph 1 of article 37, there is a total lack of specification of the

conducts that, within the scope of Chapter VI of this law, justify the qualification as

serious misdemeanor, in violation of the principle of typicality of illicit acts.

Among the different articles provided for in this chapter, one can only find

sufficiently dense obligations, the violation of which may give rise to a sanction in the

Process No. 6275/2018 26

following articles (some of which only after changing their wording as if

underlines throughout this opinion):

i.

ii.

iii.

iv.

v.

In article 24, only the provisions of paragraph 6;

In article 25, only paragraph 2;

Article 27;

In article 28, in paragraphs 4, 5, 7 and 8;

In paragraph 6 of article 28 (or in the new article that regulates the treatments

of biometric data), after specifying the limits of the

treatment.

It also results from subparagraph k) of paragraph 1 of article 37 and article 52 of the draft law that

the same conduct (non-compliance with CNPD orders or prohibitions) is sanctioned

as a misdemeanor and as a crime. In consideration of the principle ne bis in idem¸

it would be important to correct the provisions of subparagraph k) of paragraph 1 of article 37. Indeed, recognizing the

GDPR give the Member States the autonomy to define sanctions of a different nature for

infractions provided for in article 83, the national legislator may define as a crime the infractions

provided for in subparagraph e) of paragraph 5 and in paragraph 6 of article 83, option followed in this Proposal

of Law. What should be avoided is to qualify the same conduct, without any distinction, as

crime and misdemeanor.

Thus, it will only make sense to keep the refusal to cooperate with

the CNPD. Simply, as this infraction is qualified as a serious infraction

(cf. article 31 of the GDPR and point a) of paragraph 4 of article 83 of the GDPR), the national legislator

cannot elevate it to a very serious offence.

4.4. Other aspects of the administrative offense regime

It is important to underline that article 45 of the Draft Law, when determining the application

subsidiary of the General Regime for Administrative Offenses «In everything that is not provided for in the

present law on administrative offences (…)», must be revised, in order to

safeguard the provisions of the GDPR. Therefore, the following wording is recommended for the part

initial of article 45.º: In everything that is not provided for in the GDPR and in this law in

misdemeanor matter (…).

Process No. 6275/2018 26v.

It should also be noted that, as the General Regime for Administrative Offenses applies subsidiary,

and taking into account the provisions of article 8 of this Regime, it is essential to provide in the Proposal

of Law that, in this matter of administrative offence, negligence is always punishable. It is

provision recommended here does not contradict article 83 of the GDPR, because in the

subparagraph b) of paragraph 2 of this article, it is necessary to take into account the intentional or

negligent of the infringement.

4.5. jurisdictional protection

Finally, still in the context of the supervisory authority's activity, the CNPD would like to

draw attention to Articles 34 and 36 of the Proposal.

Article 34 (jurisdictional protection) provides, in its paragraph 2: “[T]he actions brought against the CNPD

fall within the competence of the administrative courts'. According to paragraph 1 of this article, the

bringing actions by any person against CNPD decisions covers

expressly those of an administrative offense nature.

It is strange why the legislator seems to defend (with this paragraph) a regression

in the rehearsed path with the substantial specialization of the so-called “courts of

specialized competence” they know about specific subjects. without prejudice to

need to carry out periodic considerations on the effectiveness of changes

past, the removal of administrative offense matters from what was, since 201130,

its “natural seat”, in terms of jurisdiction, does not present, at first

In view, any appreciative element in the face of the presently known paradigm.

In fact, the specialized competence of the 'court of

competition, regulation and supervision [to] know about the issues relating to the appeal,

review and execution of decisions, orders and other measures in the process of

administrative offense legally susceptible to challenge […] by the other entities

30 Cfr. article 2 of Law no. 46/2011, of 24 June, which adds article 89-B to Law no. 3/99, of 13 January. THE

jurisdiction of this court is provided for in article 112 of Law no. 62/2013, of 26 August,

successively amended, lastly by Organic Law No. 4/2017, of 25 August (Law on the Organization of

Judiciary System).

independent administrative bodies with regulatory and supervisory functions»31, which included the

CNPD

As paragraphs 1 and 2 of article 34 of the Draft Law under analysis are written, there is no

may fail to conclude that a change in the current situation is intended, giving the

administrative courts competence to judge the 'actions brought against the decisions,

namely of an administrative offence nature […] of the CNPD'.

If, on the one hand, considering the specificity of the matter on which the

administrative courts and recognized that it is the experience, no longer negligible, of the

of competition, regulation and supervision in that context, raises the greatest of doubts

make such a sensitive change, on the other hand, cannot fail to exist

formal consequences of such an option. If the legislator effectively intends to continue

with this modification, it will be necessary to provide for the corresponding formal amendment to article 112, no.

1, subparagraph g), of the Law on the Organization of the Judiciary System.

In the opposite case, and in the wake of what was defended by the CNPD, it is considered that paragraph 2 of the

Article 34 should reflect the provisions of the Law on the Organization of the Judiciary System,

maintaining the distinction of the competent courts to hear respectively the actions of

administrative nature and those of an administrative offense nature. Therefore, the mere remission

for that law will be sufficient for one to be able to know, at every moment and in the face of

matters of an administrative or administrative nature (or even civil, if applicable), to which

court is responsible for resolving disputes that may arise between the CNPD and any person

singular or collective.

In this sense, the following wording is proposed for paragraph 2 of article 34 on guardianship

jurisdictional:

2- The competence to hear the actions proposed against the CNPD belongs to the administrative courts, with

exception of actions to challenge sanctioning resolutions, whose jurisdictional competence is assessed in the

terms of Law No. 62/2013, of 26 August.

As for article 36 (Legitimacy of the CNPD), which maintains the regime currently in force,

it should be noted that the legislator chose to abandon the wording of article 22, paragraph 6, of the

LPDP, which is equivalent to removing the representation of the CNPD in court by the Ministry

31 Cf. Article 112(1)(g) of the Law on the Organization of the Judiciary System.

Public. From here, what is accepted and accepted, the possibility of full exercise

of the judicial capacity conferred on the CNPD, even if renewed, in this legal seat, to the

specific matters of the General Regulation on Data Protection and the law that the

executes.

This is an essential aspect in the context of protecting fundamental rights, in particular taking into account the level of specialization and technicality that the protection of data and the experience and expertise that the CNPD has.

In this sense, the power to bring violations of the regulation to the attention of the judicial authorities and to bring actions – option admitted by the GDPR in paragraph 5 of article 58.º32 – will allow a direct intervention of the national supervisory authority in the processes in which it may intervene, irrespective of the quality in which it comes to do so, waiving the representation in court by the Public Prosecutor's Office.

5. Criminal sanctions

The least correct aspect is the frame of the penalties provided for the crimes listed in the Section III of the Draft Law. In fact, situations that are not in line with the criteria of effectiveness, proportionality and deterrence that recital 152 postulates and the Article 84 of the GDPR prescribes as guidelines for the remaining "rules relating to other sanctions applicable in case of violation of the provisions of (…) GDPR".

Here too, despite the space for conformation being much wider for the legislator national law, the regulation did not leave the full determination and free of possible additional sanctions to those included in the GDPR. It is not disputed that the Portuguese regime ensures "adequate procedural guarantees in accordance with the general principles of Union law and the Charter, including effective legal protection and a fair process' (cf. recital 148 of the GDPR), but it is no longer understood how can be considered effective, proportionate and dissuasive penal frameworks that even reduce compared to what existed in the LPDP.

It is positively noted that all crimes listed in this section are now public, given the elimination of paragraph 3 of article 44 of the LPDP, now transposed to the

32 See Recital 129 of the GDPR.

Article 47 of the Draft Law. In it, the aggravation provided for in paragraph 2 for

undue access to personal data provided for in Articles 9 and 10 of the GDPR.

Equally positive is the autonomous forecast of the crime of data embezzlement, duly

densified in article 48 of the Proposal.

As for what is foreseen for the violation of the duty of secrecy (Article 51 of the Proposal for

Law), in terms of penal frameworks, the apparent regression that can be seen is not understood.

In paragraph 1 of article 51 of the Draft Law, a framework for the penalty of

imprisonment of up to one year and a fine of up to 120 days for "Who,

obliged to professional secrecy under the law, without just cause and without due

consent, reveal or disclose all or part of personal data…». comparing

with the same precept of the LPDP, it is observed that the agent responsible for the same conduct

was punished “with imprisonment of up to two years or a fine of up to 240 days”. It is accepted that the legislator

wanted to grade the violations of paragraph 1 and paragraph 2 differently, contrary to the

what happened in the LPDP. However, given the seriousness of the conduct at issue here and

taking into account the legal interest at risk, it is difficult to admit that the conduct of paragraph 1

of article 51 can be revised to lower limits, and the legislator can and should, if

this is its intention, to aggravate the other hypotheses provided for in paragraph 2 of that item.

As a general note regarding the envisaged frameworks and taking into account the known complexity and the

that is still expected to occur in the areas of violation of norms, boosted by

technological means increasingly intrusive and capable of disruptive and injurious actions

the right to the protection of personal data and, consequently, the right to privacy

of private life, both constitutionally provided for, it is proposed a reconsideration of the

same by the legislator, in the sense of a possible generalized aggravation,

albeit limited by relevant constitutional and doctrinal criteria. All this because,

According to paragraph 1 of article 118 of the Penal Code, “Criminal proceedings are extinguished.

if, as a result of the statute of limitations, as soon as the crime has been committed, the

following terms: (…) c) Five years, in the case of crimes punishable by the penalty of

imprisonment whose maximum limit is equal to or greater than one year, but less than five years; d) two

years in the remaining cases.'

Now, the growing specialization that this matter demands from criminal investigation,

associated with the degree of sophistication that is beginning to be observed in criminal practices linked to

Process No. 6275/2018 28v.

violation of the protection of personal data, increasingly demand forensic checks

of great magnitude, sometimes extremely prolonged, due to the extent of the violations and

by the number of data subjects involved, often of a transnational scope. if

it is certain that the criterion of the desirability of the investigation cannot dictate, without further ado, the

proportionality of the penal frameworks, it is, on the other hand, essential to guarantee that the

said frames, associated with the existing statute of limitations, are compatible in a way

to ensure that these criminal practices are effectively punished.

It can be seen that the legislator wanted to reserve for breaches related to data

provided for in articles 9 and 10 of the GDPR aggravated frames (cf. articles 46, paragraph 2; 47,

2 and 48, no. 2, all of the Draft Law), but it is essential to understand, here too, the

amendments brought by this European legal instrument, namely with regard to the

catalog of data held by special categories or sensitive data, which is now smaller than

that what existed in the LPDP, the result of the extirpation of the concept of private life from the group of

specially protected personal data.

Finally, with regard to penal frameworks and their proportionality, especially in view of

of the provisions of article 84, no. 1, in fine, of the RGPD, the discrepancy between the

deterrent capacity of fines, with maximum limits that reach and can even

exceed ten or twenty million euros, depending on whether paragraph 4 or 5 of the

Article 83 of the GDPR and criminal sanctions that have a maximum monetary value of 120,000.00

(one hundred and twenty thousand euros)33. Without prejudice to recognizing the structural differences that

distinguish the dogmatic logic of administrative offenses and the one that guides sanctions
criminal offenses, this does not detract from the argument that we defend for a review, in the light of the said
effectiveness, proportionality and deterrence, of the lowest marked frames.
A final note regarding the penal law system. In article 56, paragraph 2, of the
The proposed law provides for the accessory sanction of publicizing the conviction on the Internet.
Considering that the publication of personal data may be at stake (when the offender
is a natural person) and that the online publication implies the global dissemination of information and
perpetuation, this sanction has an intolerable conditioning impact on the lives of
33 Cf. Article 47 of the Penal Code.

people, transforming the sentence into a perpetual penalty, which appears to be inadmissible in the
our constitutional framework.
The CNPD therefore recommends the elimination of paragraph 2 of article 56 of the Draft Law.
6. Matters of optional regulation by the national legislator
6.1. Processing of personal health data
Article 29 of the Proposal, under the heading Treatment of special categories of data
personal data, refers only to the processing of personal health data and only to impose
the duty of secrecy to those who have the legitimacy to carry out them within the scope of subparagraphs h) and i) of the
Article 9(2) of the GDPR.
It is important to clarify that this rule cannot be understood as meaning that any of the
categories of persons referred to therein are entitled to process personal health data and hence
the extension of the legal grounds will take place. Is that the legitimacy to access
health data within an organization depends on the effective and demonstrated need
access to this
information, not only in implementing the principle of
proportionality, but also for reasons of information security and the protection of

Dice. Broad terms referring, in the abstract, to the possibility of access
undifferentiated to all those who somehow work or collaborate within a
organization, when it comes to particularly sensitive data such as
health, is therefore in objective contradiction with the principles of protection of personal data
and, in particular, with points c) and f) of paragraph 1 of article 5 of the GDPR.
In fact, it is not possible for the holders of bodies such as the board of directors of a
hospital have a need to know personally identifiable health data
users of the same, or that, without further ado, access by workers
administrative files to clinical files. The same can be said for students, who do not
perform or need to perform any operation on personal data. Being
certain that the greater the range of people who access health data, the greater the
the risks to the security, integrity and confidentiality of that data.
Process No. 6275/2018 29v.
Moreover, the vast majority of health professionals are already subject to the duty of
secrecy, either by virtue of the deontological norms emanating from the respective orders
professionals, either under contract.
The same happens in paragraph 3 of article 29, where it is accepted that the holders of organs and
workers access personal health data in the context of monitoring,
financing and supervision of the activity of providing health care. Note that
the activities described here do not imply, nor should they imply, as a rule, access to data
relating to identified or identifiable persons, with access to information being sufficient
anonymized. Whoever takes financing decisions has, under no circumstances,
to know the identity of the holders of personal data. In fact, this would be a way of
circumvent legal prohibitions on access to health data and genetic data by
pharmaceutical laboratories or other companies whose direct object is not to carry out
diagnosis or provide health care.

And even within the scope of the inspection of the activity of providing health care, this inspection can be carried out by resorting to anonymized or coded information, not as a rule, it is necessary to know the identity of the holders of the health.

Therefore, the CNPD recommends clarifying the provisions of this article, in order to safeguard the principle of proportionality in access to information, imposing measures technical and organizational, namely access profiles, which guarantee the principle known as need to know. It also recommends eliminating the reference to categories of persons who cannot access personal health data, under penalty of violation of the principles and rules of information security and the deontological duties to which health professionals are required.

Considering now Article 30 of the Proposal, the CNPD has the greatest reservations as to the compliance with the GDPR and the CRP. There, the possibility of creating databases or centralized health records, specifying that they will be based on unique platforms. This rule appears without any justifying framework, namely in the explanatory memorandum, which makes it possible to understand the raison d'être of your prediction.

This article does not define the essential aspects of data processing so that it can be regarded as legitimizing the treatment: from the outset, it does not define who is or can be responsible for such databases, nor their purposes. The open content of standard would allow any entity, public or private, or natural person to create a of centralized health data, which cannot be the result intended by the legislator national law, as it contradicts the specific and reinforced protection required by paragraph 1 of article 9 of the GDPR for health data.

Added to these objections is the risk that the centralization of clinical information always

matters: the evident economic value of health data (very useful for

laboratories

pharmacists and for

insurers, for example) is boosted

exponentially with their centralization (due to the amplitude and greater ease of

information relationship), being correspondingly accompanied by the increase

risk of personal data breach. In this regard, it should be noted that they are not only

the security and inviolability requirements foreseen in the RGPD that these bases of

data must respect, but all the requirements set out in the GDPR.

It is that the risk to the rights and freedoms of citizens of the existence of a

with these characteristics is likely to cause such damage, especially in the

concerning the possibility of giving rise to discrimination, damage to reputation,

loss of confidentiality of personal data protected by professional secrecy, or the

any other major damage of an economic or social nature, which cannot

be tolerated. Furthermore, it is emphasized that health information encompasses information

about the person collected during registration for the provision of health services, or

during that service34, which is likely to include other personal data especially

protected, such as data revealing racial or ethnic origin, beliefs

religious or philosophical as well as genetic data or data relating to sexual life or

sexual orientation.

The probability and seriousness of the risks to the rights and freedoms of citizens that a

such processing of personal data would entail requires careful consideration and

of an impact study, as well as a broad public discussion.

34 Cf. referred to in Directive 2011/24/EU of the European Parliament and of the Council

Thus, considering the open content of the rule that provides for the possibility of creating

centralized health records or databases, in terms that imply a risk of
unbearable restriction of the right to the protection of these data and other fundamental rights, and
therefore constituting an unjustified and unnecessary conditioning or restriction
of that right, the CNPD considers that article 30 does not comply with the principles of protection
data, does not respect the protection provided by article 9 of the GDPR and does not present the
normative density required to a restrictive norm of rights, freedoms and guarantees, to
in addition to understanding that the proportionality of such restriction is not demonstrated, in the
terms of paragraph 2 of article 18 of the CRP. On these grounds, the CNPD recommends the
elimination of article 30 of the Proposal.

6.2. Processing of data of deceased persons

Article 17 of the Proposal provides for the extension of the regime provided for in the GDPR to the treatment
of sensitive personal data of the deceased, i.e. the personal data listed in the
Article 9 of the GDPR. The solution found here does not contradict the GDPR - which, although
directly applying only to the processing of personal data of living persons,
admits in recital 27 that Member States apply the regime to
deceased persons – and accompanies the protection of the personality after the death assured
by the Portuguese Civil Code (Article 71(1)). However, limited data protection
listed in article 9 of the GDPR leaves, to a large extent, unprotected
protection of the personality rights of deceased persons, as they do not fit,
for example, data relating to image or privacy.

For this reason, under penalty of an irremediable contradiction between the present Law Proposal and
the Civil Code regime regarding the protection of the personality rights of persons
deceased, it is recommended to specify in paragraph 1 of article 17 the data subject to secrecy,
namely those relating to communications, as well as identity, image and
privacy of private life.

It is also important to note the incongruity of the wording of the final part of paragraph 1 of article 17.

After determining the protection of the personal data of the deceased persons who are part of
in the categories provided for in paragraph 1 of article 9 of the GDPR, the cases provided for in

paragraph 2 of the same article. If the situations provided for in Article 9(2) of the GDPR do not
apply to the data of deceased persons this can only mean that their processing
it's always forbidden. Assuming that this is not the intention underlying this forecast, the
CNPD recommends that in the final part of paragraph 1 of article 17 of the Proposal, instead of
"except for the cases provided for in paragraph 2 of the same article", it is prescribed in accordance with
as provided for in paragraph 2 of the same article.
A different issue, which cannot be overlooked, concerns the recognition, in the
2 of article 17, to the heirs of the legitimacy to exercise the rights provided for in
GDPR
It will be noted, from the outset, that the Civil Code recognized the legitimacy of family members and heirs
of the deceased in relation to the various personality rights, but not in relation to the right to
privacy of private life – this solution is probably due to the fact that
be able to assume that the will of the family members and heirs coincides with that of the person
deceased as to the defense of her good name and her image, but already the same presumption
cannot be asserted as to his private life. In fact, the private life of the deceased
is often unknown to surviving family members, and it cannot be assumed that this
want your family members or heirs to access information about your life
intimate relationship, your health, your sexual orientation, etc.
Note that, in the terminology of data protection, the right of access, as well as the
right of rectification and the right to erasure are intrinsic rights of the data subject and
differ, and therefore cannot be confused with them, in relation to other positions
subjective legal issues, namely, access by third parties, the obligation of accuracy of
personal data (paragraph d) of paragraph 1 of article 5 of the GDPR) or the obligation to delete the

information (paragraph e) of paragraph 1 of article 5 of the GDPR).

Thus, if one understands the recognition of certain categories of legitimate third parties

to ensure the defense of the honor and reputation of the deceased, such rights are already

carefully recognized in the Civil Code (cf., for example, article 71, paragraph 2, and 79, paragraph

2), so it is not necessary to reiterate these faculties in this Law Proposal,

under penalty of generating legal uncertainty, without adding any legal effect

new.

Process No. 6275/2018 31v.

Furthermore, the exercise, by the deceased's heirs, of the right of access (titled by the

deceased) to personal data is a solution that allows insurers, especially in the

scope of life insurance, indirectly access the deceased's health data, in the

cases where the latter has not specifically consented. What is the legislator doing

allow a result that, at least apparently, seems to have wanted to seal in the context

access to personal data contained in administrative documents (cf. article 6, paragraph 5,

of Law No. 26/2016, of August 22).

For all the reasons mentioned, the CNPD recommends the elimination of paragraph 2 of article 17.

6.3. video surveillance

As noted above, in II.3., privacy is not classified by the GDPR as

a specially protected data, so the conditions that legitimize its treatment –

regarding the dimensions that go beyond those covered in paragraph 1 of article 9 of the RGPD – they must

can be found in article 6 of the GDPR. One of the processing of personal data that has

now to be framed in this article is the result of the use of

video surveillance, precisely because of the impact it has on people's private lives.

In this context, it is important, first of all, to assess the extent to which the Portuguese State can

define specific legal rules on video surveillance, in the context of the GDPR. Now, in order

Portuguese legal system is recognized today, in paragraph 2 of article 1 of Law n.º 34/2013, of 16

May, that the private security activity has a subsidiary and complementary role
of the State's public security forces and services. As such, installation and
use of video surveillance systems developed within the framework of this legal diploma with the
purpose of guaranteeing the safety of people and goods is perceived by the legislator as
a processing of personal data carried out in the exercise of a complementary activity and
related to the exercise of the public interest security function, which is why it is even
mandatory by law in the context of certain private activities (cf. article 8 of that law). It's the
Article 6(2) grants Member States the legislative power to discipline
specifically the necessary treatments that prove necessary to guarantee that
public interest. In addition to the situations covered by Law No. 34/2013, of 16 May,
and other situations in which special laws impose the duty to use systems of
Process No. 6275/2018 32
video surveillance for reasons of public interest, it is still possible to frame the use of
such systems under the Labor Code (cf. Article 88(1) and (2) of the GDPR).
In this perspective, it is recognized that the consecration in the
this Draft Law, in article 19, of conditions and criteria for the delimitation of the
scope of data processing resulting from video surveillance systems, taking into account
account of the significant impact that it is likely to have in the legal sphere of
citizens and that the treatments are no longer subject to prior control by the CNPD
passing on to those who want to use such systems the responsibility to assess whether
complies with the principles and rules of personal data protection.
However, it is not enough to refer to the requirements provided for in article 31 of Law no.
16 of May, being essential to specify in paragraph 1 of article 19 that the
processing of personal data resulting from the use of video surveillance systems has
to respect the principles and rules defined in the GDPR.
Regardless of the cases provided for by law, it may still be lawful to carry out

personal data resulting from the use of video surveillance systems or the use of
other devices that allow the processing of personal data, namely of
image and sound35, pursuant to Article 6(1)(f) of the GDPR, provided that
respecting the conditions set forth therein and observing the remaining obligations determined
in the Regulation.
With regard to the limits on data processing resulting from the use of
video surveillance systems or other devices, set out in paragraph 2 of article 19 of the
Proposal, as a materialization of the weighting of the different interests and rights in
game, in the light of the principle of proportionality, they must apply, not only to the
treatments based on legal provisions, but also for those based on
in a legitimate interest of the person responsible or a third party. In fact, considering that the
said systems involve a substantial risk to the freedom and privacy of
persons, the legal imposition of limits on processing does not eliminate all possibility that the
35 It is recalled that there is an increasing use of mobile devices that allow image capture,
sound, etc., integrated into automobiles, eyewear, helmets, with the apparent purpose of protecting people and
goods, and who collect personal data on public roads and in other places intended to be used with reservation.

carry out, and therefore, to that extent, this legal norm is still acceptable in the face of the
jurisprudence of the CJEU.
Indeed, the Breyer judgment36 admits a national regulation as long as it does not reduce
the scope of the basis of legitimacy based on the pursuit of the legitimate interest of the
responsible, that is, provided that the Member State does not categorically and
generalized the possibility of some categories of personal data to be processed without
allow for a balance of opposing rights and interests at stake in a specific case
(cf. point 62).
However, paragraph 2 of article 19 must still be revised in order to serve as a rule of conduct

effectively guiding and proportionate for these data processing. Thus, the CNPD

recommends that in point a) a maximum measure for capturing the public road be defined

to cover access to the property, to reduce legal uncertainty and arbitrariness (e.g., 30

cm). Likewise, in subparagraph c) the reference to areas where the

privacy is too vague a formula, since from the outset the privacy of

customers and workers must be respected wherever they are; it is recommended,

therefore, its replacement by customer rest or leisure areas, as well as

intended for the reserved use of customers, namely (…), highlighting the protection of the

workers' privacy in point d). In this paragraph, from the perspective of the CNPD, it must be

It is prohibited to affect the access and interior of the rest or leisure areas of the

workers, as well as areas intended for their reserved use,

namely (…).

The CNPD also understands that the capture of sound must be prohibited by rule, admitting

only during the period in which the establishments where the

video surveillance are not open to the public or in operation.

In this regard, the CNPD cannot but regret the fact that the Proposal did not

disciplined the use of different technology, namely video cameras or

other devices coupled to unmanned aerial vehicles (drones), considering the

impact that its use can have on people's privacy and freedom.

It would be important, from the outset, to differentiate the regime according to the purpose and context of the

36 Process C-582/14, available at http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

its use, namely within the scope of the exercise of regulated professional activities

(e.g., journalist), of unregulated professional activities, but where the impact on the

data protection can be minimized relatively easily (e.g. artistic activity), and

within the scope of non-professional activities.

6.4. Access to administrative documents

Article 86 of the GDPR gives Member States the power to define the terms in
that personal data contained in official documents held by an authority
public or a public or private body to carry out the tasks of
public interest may be disclosed in order to accommodate public access to such
documents with the right to the protection of personal data under the terms of this
regulation.

The Portuguese State therefore has the power to reconcile public access to documents
officials with the right to the protection of personal data, but only under the terms of the present
regulation. This means that the national regime must respect the principles, conditions
of lawfulness and, above all, the rights of the holders provided for in the RGPD.

The Bill, in this matter, includes an article on access to official documents
(Article 26), which determines that access to administrative documents containing
personal data is governed by the provisions of Law n.º 26/2016, of 22 August – access law
administrative documents (LADA). LADA itself reserves the legal regime of
protection of personal data, in paragraph 3 of article 1, regarding access to documents, and in
1 of article 10 and in subparagraph c) of article 20, with regard to the disclosure of
documents on the Internet and the reuse of documents. Now the remission of the Draft Law
for LADA and the exception of the data protection regime, forces the interpreter to return to the
GDPR, in a circular logic, failing to reach the exact regime of access to
administrative documents containing personal data (which, under the terms of subparagraph
b) of article 3 of the LADA, correspond to the concept of article 4 of the GDPR).

This is further hampered by the fact that Article 1(4) of LADA sets out a
series of special regimes, including some relating to databases that are not
Process No. 6275/2018 33v.
subject to the GDPR, but rather to Directive 2016/680, which makes the

scope of remission to LADA.

Especially when considering that the regime of access to nominative documents of the

LADA does not guarantee the rights of data subjects under the GDPR, even

based on the fact that the protection of these rights must be reconciled with the protection of the right to

access to administrative documents.

In fact, the RGPD reinforced the right to information, under the terms of articles 7, 13 and

14th, without having correspondence with LADA. It would be unnecessary here to recall the

importance of the right to information for the legal relevance of consent (cf. n.º 11

of article 4 of the GDPR).

On the other hand, access to personal data under the terms of subparagraph b) of paragraph 5 of article 6.

of LADA is based on one condition (the direct interest, personally and constitutionally

protected) that does not coincide with the conditions of the GDPR, and even admitting that the fact that

personal data contained in administrative documents may justify the reduction of

protection of its holders, this justification must take place for reasons related to

with the specific exercise of public activity and not simply because the data

personal data are in the possession of public entities. Otherwise, national law entails

a regime differentiation of access to personal data that goes against the principle of

equality. This is typically what happens with personal health data, whose

access is different depending on whether the GDPR or LADA37 applies.

Another essential aspect concerns the guarantees of non-reuse of

documents that contain personal data and non-reversibility of anonymization - the

GDPR contains rules guiding the measures to be adopted to comply with the principle of

data minimization, which is not the case with LADA.

Finally, the absence of inspection and corrective powers of the competent entity to

monitor access to administrative documents containing personal data

unprotects data subjects in terms that are not, strictly speaking, compatible with the

GDPR

37 It is enough to take the example of the vital interests of the holder himself, who, when he is unable to consent, may justify access by third parties, a hypothesis not covered in paragraph b) of paragraph 5 of article 6. not be a personal and direct interest of the third party.

Process No. 6275/2018 34

On the face of it, only one of two solutions can ensure that the conciliation between the two rights mirrored in LADA is made under the GDPR. Or is it considered that exceptions of the legal regime for the protection of personal data expressed in LADA imply the subjection of access (and other personal data processing operations) to the administrative documents with personal data to the RGPD, in which case the provisions of Article 26 is of no use and must therefore be deleted, or if it is forced to conclude that this simple reference to the law on access to administrative documents does not meet the limits set out in article 86 of the GDPR, as the conciliation between the right to public access to administrative documents and the right to protection of personal data does not comply with the GDPR.

Also related to the disclosure of personal data, the wording of article 27 of the Bill is indecipherable. If the aim is to guarantee the principle of minimization of personal data within the scope of public procurement, then the criterion will not be that of sufficient identification of the public contractor (which corresponds to a public entity and therefore of a collective nature) but rather the identification of the co-contractor and respective representatives. It must also be ensured that, being necessary in the context of this type of procedures information about the employees of candidates or competitors, the it is given in aggregate form (without the respective identification), only justifying the identification of the holders after the award, for the purpose of proving the correctness of the information provided.

6.5 Publication in official journal

Article 25 of the Proposal falls within the scope of the regime for public access to official documents, provided for in article 86 of the GDPR, which gives the Member State the function of reconciling that regime with the right to protection of personal data.

Thus, in this article, the national legislator provides for some specific conditions of processing of personal data published in official journals, which should be highlighted by the positive.

Process No. 6275/2018 34v.

However, the CNPD could not fail to refer to the wording of paragraph 4 of this article, as it is revealing some misunderstanding in the concepts, contradicting the provisions of article 17 of the GDPR

Let's see. The concept of de-indexing is distinct from that of “delisting”, which allows a search carried out in a search engine, based on the name of a natural person, do not return links (to websites where the information is published) that the data subject has requested to delete. If the search is done through of a search key other than the holder's name, the list of results presented will then allow, through the available link, to access the information that is published. The big difference is that the massive aggregation of information around a person by searching for their name. This is the right to erasure or right of elimination (of certain links), recognized by the CJEU in the Google Spain judgment38, still in the light of the legal framework of the Data from 1995, and now enshrined in the new legal regime of the GDPR, as "the right to be forgotten' by search engines.

A completely different situation is the process of de-indexing or non-indexing to a search engine. This is about indexing pages (webpages) and not indexing of 'personal data'. It is a prior decision of the entity that manages or administers a site of the Internet if you want to index your website (or part of it, only selected pages) at

search engines. If you choose not to index, searches performed on the search engine will not

will point to that website. If you choose indexing, you can also choose which

the pages you want to index to the search engine and searches will only return

results from those pages.

This judicious choice may, for example, allow the information available on the

of a local authority's Internet, on tourism, heritage, cultural agenda, activity

policy, availability of application forms, etc., is indexed to the

search engines, appearing in the results list when searching for the name of the county

38

http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dda5f416897cd042ffb918c2f6bd5a55c

d.e34KaxiLc3qMb40Rch0SaxyNbNv0?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=firs

t&part=1&cid=258643

Process No. 6275/2018 35

or a local thematic area, as pages on the municipality's website relating to

city council decisions on granting licenses to natural persons,

disciplinary proceedings or other personal data are not returned in

searches by the search engine, regardless of whether searching by the individual's name

or by the date of the council meeting. This information would only be available through the

direct access to the municipality's website and not via an external search engine.

It follows that the right to erase personal data published in a newspaper

oficial cannot be carried out "through the de-indexing of these personal data in

of search».

It would not be possible to give enforceability to a holder's request to de-index his

personal data from a search engine; at most, the page where

contain this personal data, as well as all other information - personal or not

– that was contained on that page.

It is doubtful that this is the path intended by the legislator. Furthermore, the right to

deletion (of some links from search engines) must be carried out with the

responsible for processing the search engine; de-indexing a search engine, not

being

a

right

rightfully

recognized,

only

he can

to be

carried out

fur

“manager/administrator/responsible for the website, which in this case would be the newspaper

official. However, the national legislator, in paragraph 5 of article 25, determines that the person responsible for the

processing of data published in the official journal is "the entity that orders the

publication', which will most likely not have that decision-making power (as would be the

case, for example, of publications in the Electronic Gazette).

It is not, therefore, about effecting the exercise of the right to erasure through de-indexation

of search engines and this provision should therefore be removed. If the legislator

national government intends to determine that the pages of official newspapers that contain data

personal data are not indexable by search engines, the following wording of paragraph 5 is suggested

of article 25:

4 - previous no. 5

5 – Official journal electronic pages that contain personal data are not indexed to search engines.

search.

6.6. labor relations

Also in the field of industrial relations, the GDPR left room for the Member States
to regulate the processing of workers' personal data. However, that doesn't mean
extensive legislative freedom, but rather forcing the adaptation of national legislation to the
new model of administrative supervision that the GDPR enshrines. One of the consequences
of this new model is the end of prior administrative control by the
national law, so the simple reference to the Labor Code, as set out in no.
of article 28 of the Draft Law (even if read together with paragraph 2 of article 62 of the
Proposal), does not appear to be a solution consistent with the GDPR or at least
clarifying enough. Suffice it to think that such a reference covers the provisions of
articles 20 and following of the Labor Code, namely in the part where it is foreseen
the prior intervention of the CNPD.

Therefore, it is suggested that paragraph 1 of article 28 of the Proposal be revised, determining that the
employer may process the personal data of its employees for the purposes
defined and with the limits defined in the Labor Code (…), instead of “under the terms
defined in the Labor Code […]'.

But Article 28 raises further reservations.

In paragraph 2 of this article it is specified that the provisions of paragraph 1 “[…] also cover the
processing carried out by a subcontractor or certified accountant on behalf of the employer
for industrial relations management purposes […]'. Now, the specific reference to the legitimacy
of subcontractors to process personal data is, under the GDPR, incomprehensible. One
processor processes personal data in the name and on behalf of the person responsible for the
processing (here, the employer), so the legitimacy for such processing stems from
exclusively of the contract under which that subcontracting relationship is constituted (and
from which, by imposition of the RGPD, the obligation of confidentiality arises), not being

necessary for national law to provide for such a possibility.

Stranger still is the autonomy of the treatment carried out by a «certified accountant

on behalf of the employer, for the purpose of managing industrial relations'. Since then, the

accountants can only process personal data of employees of a certain

entity as subcontractors – i.e., in the name and on behalf of the employer – by the

that the need to make this specific professional activity autonomous is not achieved.

Process No. 6275/2018 36

But, more importantly, is the purpose defined here: «for the purpose of managing

labor". It is unknown that the accounting profession encompasses the entire management of

labor relations, just thinking about disciplinary procedures or occupational medicine

work to realize that there is a whole set of personal data that these, in the exercise

of their profession, they do not sue, nor can they sue under any circumstances.

Finally, still with regard to paragraph 2 of article 28, the processing of data by the

subcontractors and certified accountants to enter into a contract for the provision of

services and subjection to equal guarantees of secrecy. It is important to clarify that the contract of

provision of services is not to be confused with the contract or legal act that formalizes the

subcontracting regulated in article 28 of the GDPR. This last article imposes clauses

specific data protection, so the conclusion of the contract for the provision of

service, per se, no guarantee arises from the perspective of the protection of personal data.

In conclusion, paragraph 2 of article 28 of the Proposal adds nothing relevant to the

provided for in article 28 of the GDPR, rather contradicting or impairing the scope of the

foreseen, the CNPD recommends its elimination.

With regard to paragraph 3 of article 28, the CNPD admits that the wording derives from a

any lapse which actually renders the precept incomprehensible. It is intended, perhaps,

clarify that the worker's consent is not, as a rule, a condition of

lawfulness of processing of personal data by the employer, precisely because the

non-parity nature of the employment relationship does not ensure freedom of expression
of the worker's will, an essential requirement of legal relevance of the consent
(cf. Article 4(11) and recitals 42 and 43 of the GDPR). For that reason, the GT2939
understands that only when the processing results in a legal or material advantage for the
worker is that his consent may be waived, this circumstance being the only
exception. As worded, Article 28(3)(a) of the Proposal restricts
excessively the relevance of worker consent, thereby eliminating
any margin of free will of the workers even when there are conditions for the
its manifestation. For this reason, the CNPD recommends that subparagraph a) be revised,
39 GDPR Consent Guidelines, revised and approved April 10, 2018, available at
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
Process No. 6275/2018 36v.
becoming included in it If the processing does not result in a legal or
economic for the worker.
As for subparagraph b), the provisions of paragraph 4 of article 7 seem to want to implement the provisions of paragraph 4 of
article 7.
of the GDPR. In fact, consent constitutes a condition of autonomous lawfulness in
in relation to the contract, in accordance with article 6 of the GDPR, since when the data is
necessary for the conclusion or performance of the contract, an expression of will in the
the sense of authorizing the processing of the same data cannot be formed freely; so,
only with regard to data that are not necessary for the performance of the contract is that the
consent may apply. The intention of the national legislator appears to be to clarify the
meaning of Article 7(4) in the context of industrial relations. Once the norm has
labor relations, where the GDPR leaves room for the national legislator,
it is admitted that this specification, reiterating part of the provisions of paragraph 4 of article 7, does not
degrades the value of the GDPR standard.

Finally, article 28, in paragraphs 7 and 8, also deals with the "transfer of
personal data of workers between companies that are in a relationship of control or
group, or maintain common organizational structures', in terms that do not give rise to
reservations to the CNPD, taking into account the provisions of paragraph 2 of article 88 of the RGPD.
In any case, it is always pointed out that the reducing terms in which the norm is
express may cover the international transfer of data to entities
subcontractors, when they are in a domain or group relationship or maintain
common organizational structures, which is often the case. Now, as long as the
subcontracting requirements as well as those relating to international transfers are
fulfilled, under the terms of the GDPR, it will not be possible to limit the transfer to
subcontractors. In this regard, see opinion 2/2017 of GT29, of June 8,
2017, on data processing in the workplace40.
A different matter is the one regulated in paragraph 6 of article 28.º. Here, the treatment of
workers' biometric data if the purpose is to control attendance or
access to the employer's premises. It is recalled that Article 9(1) of the GDPR

40 WP 249, available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

expanded the categories of specially protected data (sensitive data), introducing there
biometric data that allow the unambiguous identification of data subjects. if
whether the option to legally frame this type of data processing is understood,
considering the final part of paragraph 2 of article 88 of the GDPR, it must, however,
alert to the indispensability of regulating, conditioning or limiting, the treatment,
because the mere assertion by national law of its admissibility does not allow its
realization in compliance with the GDPR.
The CNPD notes that the employer's interest in protecting information that exists or
circulates within the scope of the organization's activity may justify the use of biometrics to

access control, not only to the premises (physical access control), but also to the
electronic devices (logical access control), for user authentication. So,
it is recommended that in the final part of the standard the reference to access control to
computer systems and applications.
Furthermore, the processing of biometric data involves such a degree of complexity
technique that requires the careful definition of rules and limits for its conception and realization.
The law must therefore impose, from the outset, that the biometric system does not allow the
reversibility of the biometric data (to prevent the risk of decoding and
reproduction).
You must also prohibit the registration and storage of the feature image
biometric (e.g., digitized representation of fingerprints, iris, geometry of the
hand or facial geometry), only admitting a digital representation (template).
Considering the risks arising from the relationship of personal information and the principle
of data minimization enshrined in Article 5(1)(c) of the GDPR, must
processing is still limited to the collection and use of a single biometric data by
worker.
All this must be defined in this article, or in a separate article dedicated to the treatment of
biometric data, and the definition of
other aspects of data processing, such as the weighting of false rates
admissible acceptances or false rejections (as a way of ensuring the adequacy of the
Process No. 6275/2018 37v.
processing for the intended purpose, pursuant to Article 5(1)(c) of the GDPR) and the
permissible ways of storing biometric data41.
The CNPD understands that it is essential that the law also excludes the possibility of
of this type of information systems with other technologies, such as
interconnection with video surveillance systems.

6.7. Treatments of health data by insurers

The CNPD cannot fail to point out the fact that the GDPR, in its article 9, does not legitimize directly the processing of health data within the scope of insurance contracts, an aspect that the Bill did not take heed despite the warnings issued by the sector of activity insurer. Being certain that the consequence of this absence of legal discipline is the duty erasure of health data processed by insurers.

Indeed, the contract itself is not a condition of lawfulness to process sensitive data, and the subparagraph b) of paragraph 2 of that article limits the intervention of the national legislator to matters of labor, social security and social protection legislation. In this way, one could only include health insurance here, insofar as they can still be considered as a form of social protection. Furthermore, there would still be the possibility that the legislator, in terms of subparagraph g) of the same number, consider the public interest to be treatment of health data in the insurance activity. Now, if you can keep up that within the scope of compulsory insurance the important public interest is already recognized, since the the same is not the case with regard to other types of insurance, namely health insurance. life. It should be noted that even though the insurance activity may be recognized as having some public (as an activity subject to public regulation), it is very difficult to be a qualified public interest, as required by paragraph g).

Thus, the CNPD understands that for non-compulsory or health insurance, only paragraph 4 of article 9 can serve to legitimize the Member States to provide by law new treatment conditions.

41 For a more complete understanding of the issues that this type of treatment raises, despite being a a document dated (2004) and therefore potentially outdated, you can see the CNPD Deliberation on the Principles on the use of biometric data in the context of access control and assiduity, accessible at https://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-BIOM-assiduidade-acesso.pdf

Following any of the paths mentioned here, it is imperative that national law provide for not only the possibility of processing health data, but also the respective regime of the same, namely, the limits to which it necessarily has to be subject and the security and impact mitigation measures on the rights of data subjects – which, from the perspective of the CNPD, will make more sense to be implemented in the legislation that regulates this sector of activity.

7. Final or transitional provisions

The text of the Draft Law suffers from some legal lapses that should be corrected, and which reflected not only in the explanatory memorandum but in the article itself.

In addition to stating, in the explanatory memorandum, that "the GDPR becomes effective" on the 25th of May 2018 and in paragraph 2 of article 62 it is established that "All the rules that provide for authorizations or notifications of processing of personal data to the CNPD […] are no longer effective on the date of entry into force of the GDPR'. Now, the GDPR is very clear to establish in the article 99, which enters into force on the 20th day after the date of its publication (having been published in May 4, 2016) and which is applicable from May 25, 2018. That is, the legislator European Union has ensured a two-year transitional period for Member States, administrative entities and the different organizations that handle or process data personnel to properly prepare for the new legal framework.

Regardless of the difficulty you may feel in matching the concepts signed in the Portuguese legal system some legal solutions of Union law European Union (such as the differentiation between validity and application of a legal diploma), does not it can be claimed, much less asserted, that the Regulation is no longer in force and therefore producing legal effects on the Member States of the Union since 2016.

From the outset, it imposes on them the duty to take the necessary measures to ensure the full application of the GDPR as of May 25, 2018 and, at a minimum, not to adopt measures that are likely to jeopardize their effective implementation42.

42 Cf. CJEU Wallonie Judgment (C-129/96), paragraphs 44 and 45, even with regard to the period of transposition of directive, but the arguments reflected therein are, by a majority reason argument, valid for the European regulations.

Process No. 6275/2018 38v.

This legal precision – the applicability of the GDPR being delayed for two years – does not can, therefore, be ignored in the present Law Proposal, requiring legal rigor in the wording of the provisions contained in a Bill of this nature.

It adds that this imprecision legal has practical consequences relevant.

Specifically, the provisions of paragraph 2 of article 62 of the Draft Law, when determining that the rules that provide for authorizations and notifications to the CNPD cease to be in force on the 25th of May 2016, has an absurd result. That is, a legal diploma in force, at best of the hypotheses, in May 2018 it retroactively determines that the rules that support the authorizations already issued by the CNPD have ceased to be in force since May 2016, withdrawing with this legal basis for the decisions of the CNPD. Note that these are the same norms that served and serve as a basis for sanctioning those responsible for processing data without prior notification. This cannot be the intended result, so the CNPD considers it imperative to review Article 62(2), in the final part, cease to be in force on the date of application of the GDPR.

In addition to the observation made above, in II.2, about article 61, it is also important to leave here last two notes regarding final and transitional provisions, specifically in relation to to article 63 of the Proposal. Firstly, Law No. 67/98, of October 26, was amended by Law no. 103/2015, of 24 August, and should therefore be referred to as such. In

secondly, this law cannot be revoked by this diploma until it has been transposed
Directive (EU) 2016/680 on the protection of natural persons with regard to the
processing of personal data by the competent authorities for the purpose of prevention,
investigation, detection or prosecution of criminal offenses or enforcement of criminal sanctions, and
the free movement of such data. In fact, until the law transposing the
Directive 2016/680, the processing of personal data carried out for prevention purposes,
investigation, detection or prosecution of criminal offenses or enforcement of criminal sanctions
must respect the right to the protection of personal data enshrined in article 35 of the CRP and
in Article 8 of the Charter of Fundamental Rights of the European Union, and is therefore considered
essential to safeguard your subjection to the current legal data protection regime
personal data, enshrined in the LPDP.
For the rest, a rule that determines that all references to the LPDP would be useful
consider made for the GDPR.
Process No. 6275/2018 39
IV. conclusions
1. On the grounds set out above, the CNPD concludes that several provisions of the
Draft Law do not respect European Union law, insofar as they affect
on matters for which the GDPR has not given Member States
autonomy to legislate, at times replicating the rules of the GDPR, at other times contradicting
even the regime provided for in the GDPR.
For this reason, the CNPD recommends eliminating the following provisions:
i. Standard on the scope of application: article 2;
ii. Rules relating to the CNPD: paragraphs 3 and 4 of article 4, points d), e) and g) of paragraph 1 of the
article 6, paragraph 1 of article 7, article 8 (new wording proposed for articles
7th and 8th);
iii. Rules regarding the data protection officer: article 9 (with proposal

reworded), article 11, paragraphs 3 and 4 of article 12 and article 13;

iv. Norms on accreditation and certification: paragraphs 2 and 3 of article 14;

v. Rules on the rights of holders: articles 18 and 20;

saw. Rules on retention periods: article 21 (on retention periods

conservation, with the exception of paragraph 2, which should be revised)

vii.

International transfers: article 22

viii. Final and transitional provisions: Article 61(2).

2. The CNPD also recommends the elimination of the exceptional regime provided for in articles 23,

44 and 54 of the Proposal for data processing carried out by public entities.

This exceptional regime consists, on the one hand, in the provision that the treatments

carried out by public entities, just because they are carried out by them, can continue

purposes other than those that justified the collection of data, which translates into the denial

of the purpose principle, in violation of Article 5(1)(b) of the GDPR.

On the other hand, public entities are still exempt from the application of sanctions in

case of violation of the GDPR, which violates the principle of equality and weakens the protection of

fundamental rights of citizens in the context of processing of personal data

carried out by public entities, when it is certain that these can be as or more

intensely intrusive on the privacy and liberty of citizens, than those driven to

Process No. 6275/2018 39v.

cable by private entities, and that there are no reasons to justify this solution

differentiated, when in the last two decades the sanctioning regime in the

Data protection was the same for public and private entities.

3. In matters where the GDPR instructs the Member States to define, through

legislation, aspects of the data protection regime, it should be noted that the Draft Law

assumes a vague and open content, failing to provide specific rules for the aspects

of the regime on which it applies.

i.

This is the case with article 24 regarding data processing for purposes of

freedom of expression and information, where it was justified to differentiate the

freedom of information and freedom of the press, on the one hand, freedom of

expression, namely for academic, artistic or literary purposes, for

another – for this last group of cases to establish a specific regime

that materializes the principles of data protection, since this is not,

as in the first, a regulated professional activity.

ii. Likewise, in article 31, data processing for the purpose of archiving

public interest, scientific or historical research purposes or statistical purposes

are not the object of definition of specific rules, considering that

the provisions of paragraphs 1 and 3 of that article must be eliminated, due to their uselessness.

As regards the derogation from the exercise of rights generally

stated in paragraph 2 of article 31, a suggests its amendment (or the regulation of the

matter at its own headquarters), taking into account that only with regard to treatment with

public interest archival, historical research and statistical purposes

justified withdrawing the exercise of the right of opposition, as there is no rule

reason to exclude the remaining rights of access and rectification, provided for in paragraph 1

of article 35 of the CRP, nor the right of limitation.

The CNPD also recommends the revision of paragraph 4 of article 31, in order to comply

the purpose principle and the consent requirements set out in the GDPR,

under penalty of having that rule for not complying with the GDPR.

iii.

The CNPD also proposes the introduction of an article that ensures compliance with

duty of hearing in the context of cooperation procedures with

supervisory authorities of other Member States and consistency with the

Committee, by virtue of the one-stop shop model, as well as the prediction of causes of

suspension of the procedure directly resulting from the concertation

plurinational.

4. With regard to the system of administrative offences, the maximum limits of fines

defined in paragraphs 4 and 5 of article 83 of the GDPR cannot be removed by

Member States of the Union, nor can they lay down minimum limits.

i.

Therefore, the CNPD believes that paragraph 2 of articles 37 and 38, where it is

provides for a sanctioning framework different from that provided for in the GDPR, and differentiated

depending on the size of the companies and the collective or singular nature of the

subjects who carry out data processing (factors that the European legislator does not

considered in the definition of the sanctioning framework), in clear violation of the GDPR and

of the primacy of Union law.

ii.

The CNPD also recommends the elimination of article 39 of the Proposal, for

repeat or add weighting criteria, when the GDPR, in paragraph 2 of article 83,

closed to the national legislator such possibility in relation to the infractions foreseen

in the GDPR, referring only to the specific applicator of the norm - the

national authority or the court – the discovery of other criteria.

iii. The GDPR leaves no scope for Member States to introduce changes to the

list of offenses provided for in paragraphs 4 and 5 of article 83, so that the CNPD

suggests the elimination of paragraph 1 of article 37 of the Proposal, with the exception of subparagraph

e) and point l), concerning the obligations that Member States may define

within the scope of matters covered by articles 85 et seq. of the GDPR, as well as

as in subparagraph u) of paragraph 1 of article 38 of the Proposal.

iv. It is also recommended the classification of infractions related to the obligations

generically covered in subparagraph l) of paragraph 1 of article 37 of the Proposal, which

are those provided for in paragraph 6 of article 24, in paragraph 2 of article 25, in article 27, in

paragraphs 4, 5, 7 and 8 of article 28 and paragraph 6 of article 28 (after reformulation in the

terms proposed by the CNPD).

Process No. 6275/2018 40v.

v.

The CNPD also advises the revision of the wording of article 45, regarding the application

subsidiary of the General Regime of Administrative Offenses, so that

also provided for in the GDPR, and the introduction of a provision providing that,

in administrative offences, negligence is always punishable.

saw.

The CNPD also recommends that paragraph 2 of article 34 of the Proposal be amended,

per

in order to safeguard the expertise in the field of

infringements by the competition court, regulation and supervision.

5. In relation to the criminal sanctions provided for in Section III of the Draft Law, the CNPD

understands that the penal frameworks should be reviewed. From the outset, the frame defined in the

article 51 of the Proposal, as it represents a regression in relation to the

criminal sanctions currently provided for in the LPDP, but also those provided for in articles

46, 47 and 48, which do not seem to correspond to effective, proportionate and

deterrents as required by Article 84 of the GDPR. In addition to the notorious gap

between the deterrent capacity of fines, with maximum limits that reach and can

even exceed the ten or twenty million euros, and the criminal sanctions that have

maximum pecuniary one hundred and twenty thousand euros.

The CNPD also recommends the elimination of paragraph 2 of article 56 of the Draft Law, for
provide for an ancillary sanction of publicity on the Internet of the application of criminal sanction,
what it means to transform the sentence into a perpetual sanction.

6. In matters where the GDPR leaves room for national legislative discipline, the
CNPD recommends the change in the following terms.

i.

The clarification of the provisions of article 29 on the processing of health data, in
in order to safeguard the principle of proportionality in access to information,
imposing the adoption of technical and organizational measures, namely profiles of
access; also considers that the reference to categories of persons who
they cannot, in any case, access personal health data.

ii.

The CNPD believes that the provisions of article 30 of the Proposal are inadmissible, due to the content
vague and open with which it admits the creation of health records or databases
centralized, without the normative density required of a restrictive rule of rights,
freedoms and guarantees and capable of providing an assessment of proportionality
of such restriction, in direct violation of data protection principles.

iii.

In relation to article 17 of the Proposal, where the extension of the envisaged regime is foreseen
in the GDPR to the processing of sensitive personal data of deceased persons, the
CNPD recommends that data subject to confidentiality be added to paragraph 1,
namely those relating to communications, as well as data relating to the
identity, image and intimacy of private life. It is also recommended to
correction of the incongruity in the wording of the final part of paragraph 1 of article 17, and the
elimination of paragraph 2 of article 17, in line with the protection provided by the

Civil Code and with the rights provided for in the GDPR.

iv. With regard to the video surveillance regime, provided for in article 19 of the Proposal,

in addition to suggestions to make the wording of paragraph 1 more accurate, the CNPD proposes to

revision of the limits established in paragraph 2, in order to clarify the treatments that remain

prohibited because they represent a disproportionate restriction of fundamental rights

of data subjects.

In this regard, the CNPD regrets the fact that the Proposal did not discipline the

use of video cameras or other devices attached to vehicles

unmanned aerial vehicles (drones).

v. Regarding the conciliation of access and disclosure of administrative documents that

contain personal data with the regime provided for in the RGPD, the CNPD understands that the

Article 26 of the Proposal adds nothing from this point of view and should therefore be

eliminated. In fact, or is it considered that the reservations of the legal protection regime

of personal data expressed in the law on access to administrative documents

imply the subjection of access and other data processing operations

personal data to the GDPR, in which case the provisions of article 26 have no

utility, or if you are forced to conclude that the simple reference to the law on access to

administrative documents does not comply with the limits set in article 86 of the GDPR,

Process No. 6275/2018 41v.

because this legal diploma does not materialize essential guarantees of protection

of the data.

The text of article 27 of the Draft Law must also be revised, so that

complies, as intended, with the principle of data minimization

personnel within the scope of public procurement.

It is also proposed to revise paragraph 4 of article 25, concerning the publication of data

personal information in official newspapers, due to the misunderstanding on which it is based on concepts

technicians, in order to prevent the contradiction of the provisions of article 17 of the GDPR.

saw.

Regarding data processing in labor relations, the CNPD proposes to review the

paragraph 1 of article 28, to make it more precise, as well as paragraph a) of paragraph 3, under

penalty of contradicting the GDPR as to the relevance of consent.

It also proposes the elimination of paragraph 2 of the same article.

Regarding the provisions of paragraphs 7 and 8 of article 28, as written,

warns of the risk that arises from limiting transfers to

subcontractors in violation of the GDPR, when the assumptions provided for in this

are filled.

With regard to the processing of biometric data, provided for in paragraph 6 of article

28th considers the CNPD to be essential for the legal definition of the regime of this

treatment, because the mere assertion by national law of its admissibility does not

guarantees that they are carried out in compliance with the GDPR. It is further recommended that

rule out the possibility of relating this type of information systems

with other technologies, such as interconnection with

video surveillance.

vii.

The CNPD also points out the absence in the GDPR of a direct basis for the legality of the

processing of health data within the scope of insurance contracts and the need

definition of a specific legal regime on this treatment, warning from the

since the mere legal provision of treatment is not sufficient.

7. Within the scope of final or transitional provisions, in addition to the elimination of paragraph 2 of article

61, understands the CNPD that paragraph 2 of article 62, in the final part, should be revised, taking into account

account that the GDPR has been in force since 2016.

The CNPD also warns that article 63 cannot provide for the

repeal of the LDPD, until Directive (EU) 2016/680 on

protection of natural persons with regard to the processing of personal data

by the competent authorities for the purpose of prevention, investigation, detection or

repression of criminal offenses or enforcement of criminal sanctions, and free movement

of that data.

Finally, the CNPD recommends introducing a provision to the effect that

all references to the LPDP are considered to be made to the GDPR.

Lisbon, May 2, 2018

Filipa Calvão (President)