Process no.

6276/2018 1

NATIONAL DATA PROTECTION COMMISSION

OPINION No. 14/2018

The Assembly of the Republic, through the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees, asked the National Data Protection Commission (CNPD) to issue an opinion on Draft Law No. 119/XIII/3a (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 20161 on measures to ensure a high common level of security for networks and information across the Union.

The request made aims to fulfill the powers conferred on the CNPD by Article 22(2) of Law No. 67/98, of October 26, amended by Law No. 103/2015, of August 24 of Personal Data Protection (LPDP), and the opinion is issued in accordance with the competence set out in paragraph a) of paragraph 1 of article 23 of the aforementioned law.

I. Proposed Law

The explanatory memorandum of the proposed law states that information networks and systems play a vital role in society, and their resilience and security are essential for the pursuit of economic and societal activities. It is also noted that the scope, frequency and impact of security incidents are increasing, constituting an important threat to the functioning of networks and information systems.

The draft law provides for the definition of a National Cyberspace Security Strategy, to be approved by resolution of the Council of Ministers, as well as the creation of a Higher Cyberspace Security Council and its respective composition and powers.

The National Cybersecurity Center is the competent national authority in the context of implementing the directive and, to that extent, operates as a national point of contact for international cooperation. By the proposed law, it acquires the nature of National Authority of

JOL 194 of 7.19.2016, p.1-30

1200-821 LISBON Fax: 213 976 832

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt



Cybersecurity, in which the national computer security incident response team (CSIRT) operates, whose powers are also defined in this proposal.

The draft law establishes generic obligations for the public administration and for operators of critical infrastructure, for operators of essential services and for digital service providers, regarding the application of measures for the prevention and management of risk and regarding the notification of incidents. to the National Cybersecurity Center. However, it refers to further legislation to complement the definition of safety requirements and incident notification requirements, within 150 days of the entry into force of the diploma (cf. Articles 12, 13 and 31).

The National Cybersecurity Center has supervisory and sanctioning powers, with infractions constituting administrative offences.

II. From the appreciation

The security of networks and information systems is naturally of particular importance for data protection, whenever the processing of personal data is involved. The scope of this directive and the proposed law that transposes it is broader, as it concerns any type of information, however, this information may also include information of a personal nature.

In accordance with article 2, paragraph 7, paragraph a) of the proposed law under analysis, the provisions of this law do not affect compliance with applicable legislation on the protection of personal data. This is a rule that is extremely important, for two reasons: on the one hand, because similar terminology ('safety', 'risk', 'incident', 'notification', 'technical and organizational measures') could to misunderstand the scope and possible competition of obligations in either context; on the other hand, because the legal obligations of the new data protection regime2 in terms of information security are much more demanding than those contemplated in the transposing directive, so it will be necessary to guarantee that the level of protection will always be the most

2 Regulation (EU) 2016/679 - General Data Protection Regulation (RGPD) and Directive (EU) 2016/680, on the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or enforcement of criminal sanctions.



high. Therefore, those responsible for processing personal data and processors will have to comply with the provisions of personal data protection legislation.

Regardless of compliance with the precepts regarding security and the notification of personal data breaches contained in the specific data protection legislation, Directive (EU) 2016/1148 expressly says that the data protection legislation applies to the processing of personal data. carried out within its scope.

Indeed, Recital 72 explains that sharing information on risks and incidents at the cooperation group and CS/RT network level and complying with incident reporting requirements to the competent national authorities or CSiRT may require the handling of personal data. This treatment must comply with the provisions of Directive 95/46/EC(...). This mention of the data protection directive should now be made for the new data protection legislative acts.

Thus, in line with the directive being transposed, the CNPD considers that, for the sake of clarity and legal certainty, a specific rule should be introduced in the proposed law transposing Article 2(1) of the Directive (EU ) 2016/1148.

Still regarding other aspects of convergence with the data protection regime, it should be noted that Directive (EU) 2016/1148, in its article 15, paragraph 4, provides that the competent authorities, in this case, the Center National Cybersecurity, work closely with data protection authorities when dealing with incidents that have given rise to the breach of personal data.

However, this provision is not transposed into the domestic legal system in the text of the draft law under consideration here. In the CNPD's view, this is a flaw that should be addressed in the legislative text, as cooperation between the two authorities at this level would certainly result in a more effective application of the applicable legal framework. In this regard, Recital 63 recognizes that personal data are in many cases compromised as a result of incidents, so that competent authorities and data protection authorities should cooperate and exchange information on all relevant issues to combat possible breaches of data. personal data resulting from incidents.

Tel: 213 928400 Fax: 213 976832

www.cnpd.pt

PRIVACY NAIL

Weekdays from 10 am to 1 pm

doubts@cnpd.pt



In this way, a rule should be added to the draft law, possibly in its article 7 (in which articulation and close cooperation with other entities is already foreseen), which determines the cooperation between the National Cybersecurity Center and the CNPD when this becomes aware of incidents that have resulted in a personal data breach.

As for the scope of application of the proposed law, doubts are raised about the scope of subparagraph e) of paragraph 1 of article 2, when it is established that the law applies to any other entities that use networks and information, in addition to applying to Public Administration, critical infrastructure operators, essential service operators, digital service providers. All obligations are defined in terms of these last actors. Only Article 20, on voluntary reporting of incidents, will be able to encompass other entities in addition to those specifically identified. If so, perhaps the application of the law should be specifically restricted to the entities referred to in subparagraph e), only for the purposes of article 20, rather than leaving the applicability of the law open to any entities with no specific purpose.

Regarding the competences of the CSIRT team, known as «CERT.PT», listed in article 9 of the draft law, attention is drawn to the competence provided for in paragraph b) of the article: Monitoring cyberspace.

In fact, this is a competence that is too vague and comprehensive, if not unfeasible and inappropriate in this context.

Comparing the attributions of the CSIRT teams, provided for in Annex I of the directive, with the text of the proposed law, there is great coincidence, with the exception of this paragraph b) of article 9. The corresponding competence in the directive is in paragraph 2(a), i. of said annex and prescribes: monitoring incidents at national level.

It is therefore considered that the wording of paragraph b) of article 9 of the proposed law should be amended, in order to replace cyberspace monitoring with monitoring of incidents at national level.

Still in the context of the obligations and attributions of the CSIRTs, listed in Annex I to the directive, it should be noted that the

proposed law only establishes the competences of the teams, but not their obligations.

Case No. 6276/2018

3

NATIONAL COMMISSION ■ DATA PROTECTION

Finally, it is worth noting the negligible value of the fines foreseen, within the scope of the sanctioning regime defined in this draft law, in particular if one takes into account that networks and information systems play a vital role in society (...) and that this type of incident can jeopardize the regular functioning of society, cause danger to human life, financial losses, as well as compromise the confidentiality, integrity and availability of information on Public Administration networks and systems, operators of essential services and providers of digital services, as stated in the Explanatory Memorandum.

Although there is no distinction between the public and the private sector, with public entities also being subject to pecuniary sanctions, it appears that the punishment for a very serious infraction based on a maximum fine of 5 thousand Euros3 is far from constituting a effective, proportionate and dissuasive sanction, as required by Article 21 of the directive.

Furthermore, insofar as the security of the processing of personal data also depends on the security of information systems and networks, there is a clear relationship with the European data protection regime, which penalizes the breach of rules in a much more severe way. concerning obligations relating to the adoption of adequate security measures.

III. Conclusion

On the grounds set out above, the CNPD considers, in short, the following:

1. The scope of Article 2(1)(e) of the proposal must be clarified.

2. A specific rule should be introduced regarding the application of data protection legislation to the processing of personal data carried out within the scope of this law, in accordance with the provisions of Article 2(1) of the directive being transposed.

Amount that can be reduced by half in the event of negligence (cf. article 25 of the proposed law)

Rua de São Bento, 148-3° • 1200-821 LISBON

Tel: 213 928 400 Fax: 213 976 832

www.cnpd.pt

GEggm

PRIVACY LINE

Weekdays from 10 am to 1 pm

doubts@cnpd.pt

Case No. 6276/2018

3v.

3. Provision must be added that provides for close collaboration between the National Cybersecurity Center and the CNPD when the latter deals with incidents that have given rise to the breach of personal data, in compliance with Article 15(4) of the directive.

4. The text of paragraph b) of article 9 of the proposal, on the competences of the CSIRT teams, should be amended, in order to replace the competence of the CSIRT team to monitor cyberspace for the monitoring of incidents at national level, as shown in Annex I to the directive.

5. The amounts of the fines provided for in the draft law must be adjusted, in compliance with article 21 of the directive, which determines that the sanctions must be effective, dissuasive and proportionate, in particular taking into account the value of the property to be defended.

Lisbon, April 17, 2018

Filipa Calvão (President)