CNPD

National Data Protection Commission

OPINION/2021/52

I. Order

1. The Secretary of State for the Presidency of the Council of Ministers asked the National Data Protection Commission (CNPD) to issue an opinion on the Draft Decree-Law that «regulates the legal framework for cyberspace security and defines the obligations in of cybersecurity certification pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019".

2. The CNPD issues an opinion within the scope of its powers and competences as an independent administrative authority with powers of authority to control the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57, subparagraph b) of Article 58(3) and Article 36(4), all of Regulation (EU) 2016/679, of 27 April 2016 - General Data Protection Regulation (hereinafter GDPR), in conjunction with the provisions of article 3, paragraph 2 of article 4 and paragraph a) of paragraph 1 of article 6, all of Law No. 58/2019, of 8 December August, which enforces the GDPR in the domestic legal order.

II. Analysis

3. Law No. 46/2018, of 13 August, which establishes the legal framework for cyberspace security, transposing into the national legal system Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 August July 2016, refers to complementary legislation defining the security requirements of networks and information systems, as well as the rules for defining incidents. This Draft Decree-Law intends to regulate the aforementioned regime, also including the provisions relating to the implementation in the same framework of the obligations in terms of cybersecurity certification provided for in Regulation (EU) 2019/881 of the European Parliament and of the Council, of 17 December. April 2019.

4. Since the data protection legal regime contains some rules whose ratio is common to the cybersecurity legal regime and, above all, which the recipient entities have in common, the perspective of the CNPD, in issuing this opinion, is to that the present Project should seek to respect a certain conceptual harmonization to facilitate the application by the entities of those regimes and correct some of the difficulties that their articulated application has raised. Regarding this last point, the CNPD will

try to leave some contributions drawn up following its experience in the context of security incidents that affect personal data.

5. Thus, the CNPD begins by pointing out that, among the different obligations imposed by the Project on entities subject to the cybersecurity regime, it is important to consider the adoption of measures at the organizational level and related to

Av.D. Carlos 1,134.1o 1200-651 Lisbon

T (+351) 213 928 400 F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

to human resources. In fact, demonstrating experience that part of security incidents result from human error or organizational failure, the CNPD recommends that:

i. Article 7 specifies, in addition to the elements listed therein, that the security plan also includes a description of organizational measures and, in particular, training of human resources;

ii. In Article 8(1)(a), a summary description of human resources training activities on network and information systems security issues is added.

6. With regard to risk analysis, experience has shown that it is important that this analysis is not compartmentalized, but rather covers the network and the entire information system and, therefore, considers all its implications for personal data as well. Thus, to prevent a partial view of the risks and the disregard of the consequences on the people to whom the information concerns the introduction of measures to mitigate a certain risk, the CNPD recommends that in article 10 of the Project, eventually, in no. 2, it is expressly required that the obligation to carry out the risk analysis and to document that analysis reflects an overall view of the risks.

7. Still within the scope of the same article 10, the reason why, among the factors to be considered in the risk analysis, other factors that cannot fail to be decisive in this assessment are not listed. From the outset, the omission of reference to the sensitivity or criticality of the information existing in the information systems, to the existence of reliable mechanisms for traceability, as well as recovery and redundancy, and also the adequacy of the human resources assigned to each specific function in this context. The CNPD therefore considers it essential to expressly provide for these factors in the list of paragraph

4 of article 10 of the Project.

8. With regard to the notification of incidents, understanding that the obligation to notify the National Cybersecurity Center (CNCS) only arises when the incidents have a relevant or substantial impact (cf. Article 10 of the Project), the CNPD understands that , in the context of a regime that also seeks to promote the active accountability of the entities subject to it, the provision of the obligation to internally record all security incidents proves to be appropriate and relevant. Such a complementary obligation allows not only the rationalization of the judgment on the relevance or substance of the impact, by the entity itself, but also the ex post verification of this evaluative judgment by the competent administrative entity. This obligation will also be relevant for the purpose of identifying flaws in the security of the network and the information system, by allowing the detection of the possible recurrence of incidents.

9. In this sense, the CNPD recommends the introduction in Chapter IV, or Chapter III, of a rule that provides for the obligation of internal recording of security incidents.

10. Regarding the system of notification obligations, it is noted that the period provided for in paragraph 1 of article 13 of the Project runs the risk of being too short, since, with the period of two hours to carry out the notification and give priority to the mitigation and resolution of the incident, the notification can be translated into a mere formality empty of descriptive content that allows the recipient to make an accurate assessment of the incident. Bearing in mind that the European legislator, in the context of personal data breaches (i.e. security incidents that affect personal data), has set a deadline for complying with the notification obligation of 72 hours (cf. Article 33 of the GDPR), the CNPD takes the liberty of suggesting that the time period set out in Article 13(1) of the Project be reconsidered.

11. In relation to article 16 of the Project, the CNPD allows itself to point out a conceptual inconsistency. In Article 16(2), when it is intended to list the effects that incidents can produce, causes of incidents are also provided, as appears to be the case with "malware infection", "intrusion" and "attempt to intrusion". And in the same provision, strangely, there are omitted

consequences that Article 4(2) of Directive (EU) 2016/1148 itself states as consequences of security incidents, namely, in addition to availability (indicated in point b) of the Article 16(2) of the Draft), 'authenticity, integrity and confidentiality'.

12. Note that this observation is not merely formal, since, as highlighted at the beginning of this opinion, the entities subject to the regime under analysis are also subject, as a rule, to the GDPR, which contains provisions relating to incidents and the obligation to notify them, for reasons of security and certainty in the application of the law, it is important that the national legislator does not introduce differences, in relation to European Union legislation, in the characterization of incidents and their possible effects.

13. The CNPD therefore recommends revising paragraph 2 of article 16 of the Project, for the sake of clarity and legal certainty in an article entitled “Taxonomy of incidents and effects”.

14. A final note to highlight that this diploma could be an opportunity to densify the obligation of collaboration between the GNSC and the CNPD, summarily provided for in paragraph 8 of article 7 of Law No. 46/2018, of 13 August, in particular taking into account the provisions of recital 63 of Directive (EU) 2016/1148. Indeed, it refers to the duty to cooperate and exchange information between the two entities when security incidents with breach of personal data occur, which the mere reference to "acts in collaboration with" contained in that legal precept does not sufficiently reflect.

III. Conclusion

15. On the grounds set out above and for the purpose described in point 4, the CNPD recommends:

i. The addition, in the context of the obligations provided for in article 7 and in subparagraph a) of paragraph 1 of article 8 of the Project, of organizational measures and, in particular, training of human resources on security issues information networks and systems;

ii. The express requirement, in Article 10 of the Project, possibly in paragraph 2, that the obligation to carry out the risk analysis and to document this analysis reflects an overall view of the risks;

iii. The provision in paragraph 4 of article 10 of the following factors to be considered in this risk analysis: sensitivity or criticality of the information existing in the information systems, existence of reliable mechanisms for traceability, as well as recovery and

redundancy, and also adequacy the human resources assigned to each specific function in this context;

iv. The introduction in Chapter IV or Chapter III of a rule that provides for the obligation of internal recording of security incidents;

v. The reconsideration of the period of time established in paragraph 1 of article 13 of the Project for the execution of the duty to notify security incidents;

saw. The revision of paragraph 2 of article 16 of the Project, for the sake of clarity and legal certainty in an article entitled "Taxonomy of incidents and effects", as set out above in points 11 and 12.

Lisbon, May 4, 2021

Filipa uaivao (President, who reported)