CNPD

National Data Protection Commission

OPINION/2022/11

I. Order

1. The Minister for Modernization of the State and Public Administration asked the National Data Protection Commission (CNPD) to issue an opinion on two draft regulatory ordinances of Law No. 61/2021, of 19 August, and the first makes the “First amendment to Ordinance No. 286/2017 and second amendment to Ordinance No. 287/2017, both of 28 September, which regulate Law No. 7/2007, of 5 February [. ..]» and the second to the «Regulation of numbers 6 and 7 of article 13 of Law no. 7/2007, of 5 February».

2. The request was accompanied by an impact assessment on the protection of personal data (AIPD).

3. 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 of August, which implements the GDPR in the domestic legal order.

II. Analysis

4. Although the two draft decrees aim to regulate the same legislative act - Law No. 61/2021, of August 19, which amended Law No. 7/2007, of February 5 -, and share the objective of simplifying the procedures related to the issuance and alteration of the citizen's card and the activation of the certificates associated with it, the truth is that the projects have very different objects and impact. For this reason, they will be analyzed separately here.

i. Draft Ordinance that regulates the simplification of procedures related to the alteration of citizen card data and activation of the respective certificates through facial recognition

5. We begin by considering the Draft Ordinance that makes the first amendment to Ordinance No. 286/2017 and the second

amendment to Ordinance No. 287/2017, both of 28 September, which regulate Law No. 7 /2007, of 5 February, last amended and republished by Law No. 61/2021, of 19 February. At issue is, essentially, the amendment to Ordinance No. 287/2017, where, with this Draft Ordinance, it is now defined: "[t]he cases and terms in which they can be submitted electronically and requests relating to the citizen's card by telephone", as well as "[the terms of activation of the citizen's card certificates through the use of a biometric system for comparing face images collected electronically in real time

Av. D. Carlos 1,134, Io T (+351) 213 928 400 geral@cnpd.pt

1200-651 Lisbon F (+351) 213 976 832 www.cnpd.pt

with the facial image contained in the information system responsible for the life cycle of the citizen's card" (cf. paragraphs c) and g) of article 1, of Ordinance No. 287/2017, introduced by article 3 of the Draft of Ordinance under analysis).

6. First of all, the procedure for renewing the citizen's card regulated in paragraph 3 of article 7 of Ordinance no. 287/2017 (in the now designed wording), in which an implicit request of renewal, deducted from the payment of the fee whose bank reference was sent of its own motion by post to the cardholder. In accordance with the provisions therein, together with the bank reference, the activation codes for the new card are immediately sent. Since the advantages resulting from the speeding up of the card renewal procedure under these terms are evident, the risks of misappropriation of the cardholder's identity cannot be ignored. But the aforementioned risks are mitigated by the determination that the renewal carried out under these conditions does not allow the alteration of any of the card data (cf. paragraph 4 of article 7 of Ordinance No. 287/2017, in the projected version) , and also by the mandatory delivery of the card in person (established by Article 31 of Law No. 7/2007, and reiterated in Article 7-B, added by the Project to Ordinance No. 287/2017).

7. Special attention deserves the article 7-C added by the Project to the Ordinance No. 287/2017, concerning the regulation of the use of facial recognition technology for the electronic activation of the certificates associated with the citizen card, when the card has been sent to the holder's address, or for electronic activation of the qualified certificate for qualified electronic signature.

8. In these non-face-to-face procedures, it is important to ensure that it is the cardholder himself who is executing the

application made available for the activation of digital certificates, due to the risks of identity appropriation and usurpation, which is why the legislator came to provide for the use of real-time facial recognition technology.

9. However, since facial recognition is fundamentally based on the comparison of images, it is essential to ensure that the system is not vulnerable to the presentation of, for example, high resolution videos to circumvent the requirement of detection of life. What seems to be safeguarded when considering the information contained in the AIPD (cf. step 8 of the flow described in "5.3.1.1 CC Activation Flow"; and in "5.4.2 Liveness Software", where de indicates that the software to be use «it ensures measurement of 3D depth, skin texture, eye reflections, among others - without the need for user interaction (e.g., no need for eye or face movements by the user)».

10. Simply, this fact does not rule out the hypothesis, even if remote, of the use by third parties of video images collected in other contexts (eg, in public spaces; electronic platforms with image transmission). Considering the accelerated technological evolution that brings with it renewed opportunities for

misappropriation of someone else's identity, the CNPD especially recommends the permanent and continuous evaluation of the solution as a whole, especially taking into account that computer attacks have been proving to be increasingly cunning and effective.

11. Still on the subject of the facial recognition procedure, the provision, in paragraph 4 of article 7-C, of elimination of face images (collected in real time) and images of the front and back of the citizen card after completion of the card certificate activation procedure (see also the provisions of 5.4.6.12 Point of Attack, 17 -Service and facial recognition, of the AIPD). It is still important to contractually ensure that subcontractors do not (re)use the images for the purpose of evolutionary development of facial recognition and life detection technology.

12. In this regard, it should be noted that the AIPD indicates that the platform used to implement this facial recognition and life detection procedure, provided by a Portuguese company, is hosted on the Amazon Web Services cloud (cf. 5.10 and 5.12), the IAPD also identifies the protocol for transmitting personal data via the Internet (see also 5.4.6.9). The use of this platform

therefore means that personal data are transferred to the cloud (and kept there, albeit for a certain period of time) of another company based in the Republic of Ireland, which, in turn, integrates a corporate group (Amazon) whose parent company is headquartered in the United States of America.

13. In an opinion to another draft diploma1, the CNPD has already warned about the indispensability of complying with the rules of the RGPD with regard to international data transfers, in the context of subcontracting relationships, especially when, as here happens, the processing of biometric data is at stake - specially protected data, pursuant to Article 9(1) of the GDPR.

14. The fact that the servers to which the biometric data (and other personal data) are transferred are located in the territory of a Member State of the Union is not, per se, sufficient to guarantee compliance with such rules (unlike the which seems to be assumed in the AIPD). And the Court of Justice of the European Union has already drawn attention to the inadmissibility of the processing of personal data in the situation where the subcontracting company (or subcontractor, as is the case here) located in a Member State of the Union is subject to legal rules binding regulations of a third State that may affect the protection guaranteed in the territory where the database is housed, because such rules bind it to make available to the public authorities of that State the data stored or processed by it2.

1 Cf. Opinion/2021/99, of July 22, 2021, available at https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2021&tvpe=4&ent=

2 Cf. Schrems II judgment of 07.16.2020 (C-311/18).

15. In addition, once the Active Directories (AD) consolidations are completed and the activity records (/ogs) are sent to the parent company in the United States of America, which implies the international transfer of personal data, although the servers

are located in the territory of a Member State of the Union, it is important to find solutions that guarantee compliance with Chapter V of the GDPR and the case law of the CJEU, namely through the adoption of appropriate additional measures3.

16. Thus, unless the adoption of additional protection measures - which are not demonstrated in the AIPD - is demonstrated, the transmission of personal data (in particular, biometrics) to the aforementioned platform, which uses the cloud computing services of Amazon Web Services, contradicts the provisions of chapter V of the GDPR.

17. In view of the provisions of article 7-D, added by the Project to Ordinance No. 287/2017, it is only noted, regarding the audiovisual recording of the video call sessions, that the reason for the conservation period is not reached of three years established in paragraph 3 of the same article. No explanation can be found in the AIPD - which regarding this treatment is limited to stating "[t]he process of changing address through video call is in accordance with GNS Order 154/2017, concerning the Identification of natural persons through identification procedures distance using videoconferencing (used within the scope of the eIDAS regulation)', and there is no reference to such a period of time in the Union regulation, in the aforementioned GNS regulation and in Decree-Law No. 9 February, amended by Law No. 79/2021, of 24 November, the CNPD cannot understand the reason for such a period. If it is intended to provide proof of the alteration of the citizen's card details, or if a reasonable period is established for the holder to complain about the alteration carried out - prima facie appearing to be excessive the period of three years for this purpose - or, if it is understood that you can do so at any time, the storage period should correspond to the validity of the card.

18. It is therefore recommended to consider whether the period established in article 7-D is in fact adequate for the purpose pursued with the conservation of the recording, in the light of the principle of limitation of conservation, enshrined in subparagraph e) of Article 5(1) of the GDPR.

19. A final note to recommend the amendment of the heading of section IV-A, added by article 5 of the Project to Ordinance No. 287/2017 - «Data processing» -, since all the articles of the Project and not just that section, regulates the processing of personal data. Bearing in mind that this section only includes Article 9-A, which is entitled 'Data Processing by WADA' and where the status of subcontractor is clarified

3 Cf. Recommendation 1/2020 of the European Data Protection Board.

of this entity, 'Subcontractor' or 'Subcontracting of data processing' is suggested as the title of the aforementioned section.

ii. Draft Ordinance that regulates the indication of address by a national citizen without a fixed postal address

20. The second draft ordinance, which regulates paragraphs 6 and 7 of article 13 of Law no. 7/2007, of 5 February, introduced by Law no. 61/2021, of 19 February August, establishes the terms for formalizing the indication of address by a national without a fixed postal address and approves the authorization model of the entity to which the address to be indicated refers.

21. In this Draft Ordinance, it is worth highlighting only the aspect of the regime that, from the perspective of the CNPD, needs to be revised. At issue is the authorization model of the entity to which the address to be indicated, approved in an annex to the Project, refers.

22. Article 4(3) of the Project provides for an electronic form to be made available on the digital justice platform at https://justica.gov.pt. This form will be accessed and submitted by a representative of an entity (among the types of entity provided), in order to generate an authorization for a specific national citizen without a physical postal address to indicate the address of that entity to receive correspondence related to the card. of citizen.

23. Simply, the Project is silent on the accredited authentication of the entities - and, therefore, of the users, as representatives of these entities - for the access to the form, nothing is said about this aspect in chapter 9 of the AIPD, which allows to assume that access is free. However, the CNPD points out that free access, accompanied by the mere requirement of a simple copy of a document attesting to the powers of representation, does not seem to prevent the sending of authorizations by individuals who do not represent the entities, through forgery of documents.

24. In fact, even if the intention to simplify this procedure is understood, the reason why it is not required, instead of a simple copy of a suitable document certifying the representative's powers for that purpose, forms of qualified authentication. In fact, the requirement for such a copy will still be incomprehensible if the form supports the qualified digital signature.

25. The CNPD therefore recommends reconsidering this option.

26. A final note, to point out that the reference to the indication by the entity of the e-mail address, contained in paragraph 4 of article 4 of the Project, is not accompanied by the provision of its insertion in the aforementioned

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

authorization form, nor is it included in the table where the data of the form in the IAPD are listed, therefore it is recommended to insert it in the referred form.

III. Conclusion

27. On the grounds set out above, regarding the Draft Ordinance that makes the first amendment to Ordinance no. 286/2017 and the second amendment to Ordinance no. 7/2007, of February 5th, the CNPD recommends:

The. the permanent and continuous evaluation of the solution as a whole, for face recognition in real time, especially taking into account the accelerated technological evolution that brings with it renewed opportunities of misappropriation of the identity of others and the fact that computer attacks reveal themselves more and more more cunning and effective;

B. the consideration of the period of conservation of the audiovisual recording of the video call sessions established in article 7-D, in the light of subparagraph e) of paragraph 1 of article 5 of the RGPD;

ç. the amendment of the heading “Data Processing” of section IV-A, added by Article 5 of the Project to Ordinance No.

28. Also within the scope of the same Draft Ordinance, the CNPD recommends contractually ensuring that subcontractors do not (re)use the images for the purpose of evolutionary development of facial recognition and life detection technology; and warns of the need to adopt additional protection measures, because the transmission of personal data to the aforementioned platform, which uses cloud computing services under the conditions described above, implies not only the possibility but also the effective transfer of data to a country that does not offer an adequate level of protection, in breach of chapter V of the GDPR.

29. Regarding the Draft Ordinance that regulates paragraphs 6 and 7 of article 13 of Law No. 7/2007, of February 5, introduced by Law No. 61/2021, of February 19, August, the CNPD recommends:

The. The provision of forms of qualified authentication of entities in accessing the authorization form;

B. the insertion in the aforementioned authorization form of the entity's electronic address.

Lisbon, February 3, 2022

Filipa Calvão (President, who reported)