National Commission

Data Protection

OPINION/2023/9

I. Request

1. The Data Protection Officer of the Social Security Institute, I.P. requested the National Data Protection Commission (CNPD) to issue an opinion on the draft of the Collaboration Protocol for the Integration of Professional Attributes of the Social Security Institute, IP, in the Professional Attributes Certification System (hereinafter Protocol), signed between the Agency for Administrative Modernization (AMA, IP), the Institute of Social Security, IP (ISS, IP) and the Institute of Informatics, IP (II, IP).

2. The request for an opinion was not accompanied by the Impact Assessment on the Protection of Personal Data (AIPD), which was requested and sent in the meantime.

3. The CNPD issues an opinion within the scope of its attributions and competences as an independent administrative authority with authoritative powers for the control of the processing of personal data, conferred by paragraph c) of paragraph 1 of article 57, paragraph b) of paragraph 3 of article 58 and paragraph 4 of article 36, all of Regulation (EU) 2016/679, of April 27, 2016 - General Regulation on Data Protection (hereinafter RGPD), 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 August, which implements the GDPR in the internal legal order.

II. Analysis

The. Object and scope of the Protocol

4. Law No. 7/2007, of February 5, which establishes the system for issuing and using the citizen's card, provides for Article 18-A, in the wording introduced by Law No. 61/2021, of 19 August, the possibility for the electronic signature promoted through the citizen card to contain the certification of a certain professional attribute, at the request of its holder (no. is carried out through the Professional Attributes Certification System.

5. In turn, Law No. 37/2014, of June 26, provides for a secure authentication system on websites, through the Digital Mobile

Key (CMD), which consists of an "alternative and voluntary authentication system of citizens on public administration portals and websites", with the management and security of the technological infrastructure that supports it being the responsibility of AMA (cf. article 1 and no. 8 of article 2 of Law no. 37 /2014, of June 26th).

6. Under the terms of article 11 of Ordinance No. 73/2018, of March 12, workers in public functions and managers may freely request that their public attribute be certified for subsequent signature with

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976832

geral@cnpd.pt

www.cnpd.pt

f

citizen's card or mobile digital key (no. 1), and other forms of adherence to public attributes may be defined by protocol with the AMA (no. 3).

7. In this context, the purpose of the Protocol under analysis is to "define the rules of cooperation between AMA and ISS, IP. within the scope of the implementation project of the Professional Attributes Certification System (SCAP) in electronic signature operations on digital documents and transactions and electronic authentication, within the scope of the positions and functions associated with the organic structure of the ISS, IP".

B. Persons responsible for processing personal data and subcontractor

8. Under the terms of Clause Two, AMA, IP and ISS, IP are considered responsible for the processing of personal data. 0 II, IP intervenes as a subcontractor.

9. In fact, pursuant to paragraph 5 of article 18-A of Law no. 7/2007, of February 5, the AMA is the entity responsible for the procedure for attributing professional attributes and, therefore, , for the processing of data that is necessary to fulfill this purpose.

10. The ISS intervenes in this Protocol as it is the Public Institute in which the workers whose professional attributes it intends to certify perform their functions.

11. OII, IP. intervenes in this Protocol for being the "public legal person that ensures the construction, management and operation of application systems and technological infrastructures in the areas of information and communication technologies of the services and bodies dependent on the Ministry of Labor, Solidarity and Social Security.

12. The obligations of those responsible and the subcontractor are indicated in clauses Seven and Eight, respectively.

13. In addition to the observations that, in relation to some of the obligations will be made, below, the provisions of paragraph g) of Clause Eight are not understood, when it is stated that it constitutes the subcontractor's obligation "[to comply with the rules defined by the Persons Responsible for processing in the framework of the GDPR, to transfer data to third countries or international organisations, within the limits imposed by Article 28(3) of the GDPR". However, number 3 of the aforementioned article establishes the obligations to which subcontractors are bound in any and all contexts within the scope of the relationship with those responsible, only calling international transfers as an illustrative example of one of these obligations, that is, the documentation of the instructions of the person responsible (paragraph a) of paragraph 3 of article 28), so that the content of that paragraph g) is not understood.

I

National Commission

Data Protection

14. Furthermore, the Protocol does not mention any need to transfer data to third countries or international organizations, nor is it understood to what extent these are necessary for the implementation of the Protocol, so that rule, contained in paragraph g) of Clause Eight of the Protocol must be reviewed, eliminating the reference to transfers which, under the terms of the RGPD, can only occur when and if the assumptions and terms of articles 44 to 46 are met.

15. Since there is only one subcontractor, it is suggested that, formally, the reference to subcontractor be entered in the singular.

w. Personal data subject to processing

16. As set out in Annex I to the Protocol, the data to be transmitted by the ISS, IP to AMA, IP are the following: name of the worker, category or function, designation of the service to which the worker belongs and situation before the body (A- Active; B- Not Active; C - Irregular).

17. Taking this information into account and the fact that the Protocol does not indicate anything in this regard, it is concluded that the official is identified, apparently, through his name. However, this identification clearly does not constitute a unique and error-free identifier, so a secure identifier must be transmitted. From an operational point of view, the omission of a secure identifier constitutes a weakness, which must be overcome by considering that the citizen card number is also an element to be transmitted by the ISS, IP to the AMA, IP, for identification purposes unambiguous of the worker.

d. Legal basis

18. The use of the CC or CMD by ISS.IP workers constitutes a personal data processing operation, for which ISS.IP and AMA, IP are responsible.

19. Now, for a data processing operation to be considered lawful, it must be legitimized by one of the legality grounds provided for in article 6 of the RGPD.

20. A careful reading of article 6 of the RGPD easily leads to the conclusion that there is no legal norm that imposes, or allows, the employer to require its workers to use their CC or CMD as work tools (cf. Law no. 7/2007, of February 5, Decree-Law no. 74/2014, Law no. 37/2014 of June 26).

21. From the outset, it is also not possible to frame the processing of personal data in the need to comply with a legal obligation, nor in the legitimate interest of the person responsible for this corresponding to a public entity [cf. points c) and f) and final part of paragraph 1 of article 6 of the GDPR],

í

22. For this reason, and rightly so, paragraph 1 of Clause Six provides that «[the] adherence to the electronic signature promoted through Citizen Card or Digital Mobile Key will be subject to the manifestation of free will of workers in functions

public authorities and ISS directors. IP, which will be carried out through the Professional Attributes Certification System, pursuant to Article 18-A of Law No. 7/2007, in its current wording, and Article 11.3 of Ordinance No. 73/2018, in its current wording».

23. In this regard, the reservations expressed by the CNPD regarding the use of individual authentication mechanisms based on the CC or CMD as an instrument for the performance of professional functions remain current.

24. It is recalled, in this regard, what was said in this regard in Opinion No. 66/2017, of December 19, of the CNPD regarding Ordinance No. 73/2018, of March 12.

25. Consent, in order to be valid, depends on the fulfillment of very demanding requirements, which aim to guide the rights, freedoms and guarantees of the holders of personal data [cf. Article 6(1)(a) and Article 4(11) of the GDPR],

26. In this case, this expression of will (or consent) for the processing of personal data must meet the requirements set out in paragraph 11) of article 4 of the RGPD, a provision of direct application in the national legal system. Thus, the expression of will must be: free, specific, informed and unambiguous. This implies that the existence of conditions of freedom for the manifestation of that will is demonstrated. Now, in the context of labor relations, the worker finds himself in a situation of dependency that does not allow, from the outset, the free formation of will.

27. The letter of the law is clear when it establishes that the CC holder only uses its electronic certification functionalities "[whenever you want" (cf. no. 5 of article 18 of Law no. 7/2007, of February 5) Thus, for the adherence to these means to be effectively free, those responsible must be able to guarantee the worker an alternative means that allows the authentication of the worker without using his personal civil identification document.

28. However, given that the use of the digital CC or CMD implies the processing of personal data, if the law makes the processing dependent on the expression of will of the respective data subject, then they must be fulfilled, in particular, the conditions required by the RGPD and by the national legal order for the expression of this will, so that the legal basis of the processing of personal data can be verified. In other words, the alternative cannot be between authentication and signature with or without professional attributes, through CC or CMD, but between these means and a means that guarantees that the worker does not have to use his CC or CMD.

29. Since free will formation depends on the existence of an alternative to the use of those means, because any of them presupposes voluntary and free use by workers, if an alternative to the use of those means is not guaranteed, the processing of personal data will be unlawful .

30. In addition to this aspect, it should be noted that the Protocol is completely silent on the terms of the consent to be given, with no information having been sent to the CNPD on how this consent will be obtained, nor whether it is the holder who enters all the personal data or if these are transmitted by ISS, IP, following a request from the holder, or even as to the information to be transmitted to the data subject. Thus, with regard to this particular aspect, the CNPD only emphasizes the need to comply with the provisions of articles 13 and 14, depending on whether the information is obtained from the holder or not, respectively.

31. On the other hand, as the processing of personal data is based on consent, the data subject must be able to revoke it at any time, so the Protocol must provide for how that revocation can be formalized by the data subjects and how the follow-up to be given to your revocation request.

32. The protocol is also silent with regard to the obligations of those responsible for the exercise of other rights by the holders.

33. In particular, it is not indicated by what means the data subject can exercise, namely, the right of access, rectification or deletion of data, and there must be provision, in the Protocol, with whom and by what means to exercise them.

34. However, Article 5 of the GDPR enshrines the principles which must be respected when processing personal data. Under the terms of paragraph d) of paragraph 1 of that article, personal data are "[exact and updated whenever necessary; all appropriate measures must be adopted so that inaccurate data, taking into account the purposes for which they are processed, be erased or rectified without delay." Thus, it is recommended that the Protocol specify how the sending, rectification and deletion of data will be managed, so that, at all times, the accuracy of the data is guaranteed.

35. In this regard, it should be noted that the only rules relating to the obligation to guarantee the up-to-dateness of the information affect the ISS, IP, exclusively, with the responsibility of "ensuring the up-to-dateness of the information made available pursuant to the provisions of paragraphs e) and f) above ". However, these paragraphs only refer to the obligations of AMA, IP, to "monitor the development of the works" and to "ensure the existence of a test period, lasting no less than 30 days, to correct anomalies and carrying out the changes necessary for the full functionality of the platform's software".

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

{

36. Therefore, the Protocol must be expanded in order to specify how the process of sending data, rectifying and deleting the same is managed.

37. Although article 5 of Ordinance No. 73/2018, of March 12, prohibits SCAP users from using authentication and qualified signature related to professional, business or public attributes when they no longer hold the Even so, mechanisms must be envisaged that prohibit such use from the outset, assuming that the SCPA reflects, at every moment, the current reality and that the communication mechanisms between the SCAP and the adhering bodies, in this case the ISS, IP, allow a constant update of information, since the guarantee of updating data is an essential element for the proper functioning of a system with the characteristics of SCAP and it is of the utmost importance to define the responsibilities for updating user information, in particular of information relating to the position.

It is. conservation period

38. The Protocol is still vague as to the period of retention of personal data. In fact, it only states that they are obligations of those responsible for the treatment "[define the periods of conservation of personal data or, when this is not possible, indicate the circumstances that dictate the end of the conservation" [paragraph d) of Clause Seven) .

39. Now, as the Protocol also provides that the data "are kept for the period strictly necessary to pursue the purpose set out in this protocol" (No. later moment the determination of a period that can be defined immediately, because it does not depend on the will of the contracting parties. Thus, the text of the Protocol should clarify this norm, explaining the period, or the event that determines the period of conservation and the erasure of the same.

40. The Protocol does not say anything about the retention period of file data, as well as the Access Logs, either by the ISS, IP, through the subcontractor, II, IP, or by the AMA, as recognized in the DPIA itself (point 2.2.1.3). Since the establishment of security measures and auditing mechanisms is an obligation of those responsible, the Protocol must be reviewed and expanded, in compliance with the obligations laid down in paragraphs 1 and 2 of article 5 of the RGPD.

41. It is also important to point out that there is a lack of elements that would allow the CNPD to pronounce fully on certain technical aspects. Namely, it is not possible for the CNPD to pronounce on the aspects that require the materialization of the work foreseen in Clause Three of the Protocol, but which have not yet been implemented, such as the technical characteristics of the Interoperability Platform of the

Public Administration and subsequent integration with SCAP; the technological solution to guarantee the certification of professional attributes with a citizen's card through SCAP or technological solution of the interfaces that allow the interconnection of data made available by the ISS, IP intended to guarantee the certification of professional attributes with a citizen's card.

42. The only description of the technical implementation, in the Protocol, is found in Clause Four and refers to good practices and HTTPS access. In that same clause, it should be noted that communications between II, IP and AMA, IP are carried out through an exclusive connection channel for this data transmission, in compliance with the technical requirements of Resolution of the Council of Ministers No. 41 /2018.

III. Conclusion

43. Based on the reasons set out above, the CNPD recommends that the Protocol be revised in order to provide for:

The. the addition of the citizen's card number to the list of data to be transmitted by the ISS, IP to the AMA, IP, for the purposes of secure identification of workers, for the purposes of professional attribute certification;

B. predicting how data subjects can exercise their rights, including revoking consent;

w. reference to the way in which the sending, rectification and deletion of data is managed, so that, at all times, the accuracy of the data is guaranteed;

d. clear identification of data retention periods or situations that lead to their deletion;

It is. forecasting the retention period of file data and access logs;

f. take care that the communications between the II, IP and the AMA, IP are carried out through an exclusive connection channel for the transmission of data.

44. It is also recommended that workers be guaranteed alternative means of authentication of the worker in the systems and digital signature that does not require the use of the Citizen Card or the Digital Mobile Key, for example, the creation of a worker card.

Approved at the meeting of January 19, 2023

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt