National Data Protection Commission

OPINION/2022/22

I. Order

1. The Social Security Institute, I.P. requested the National Data Protection Commission (CNPD) to issue an opinion on the draft Protocol on the Automated Processing of Personal Data, within the scope of the Social Security Calculation Module, within the scope of the National Network for Integrated Continuing Care (RNCCI) , to be concluded between the Central Administration of Health Systems, I.P. (ACSS, IP), the Shared Services of the Ministry of Health, E.P.E. (SPMS, EPE), the Social Security Institute, I.P. (ISS, IP) and the Institute of Informatics,

1. P. (II.IP).

2. The request for an opinion was not accompanied by the Impact Assessment on Data Protection (AIPD), which, pursuant to paragraph 4 of article 18 of Law no. 43/2004, amended by Law no. .° 58/2019, of August 18, is mandatory, which was later sent to the request of the CNPD.

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 December August, which enforces the GDPR in the domestic legal order.

II. Analysis

4. The Protocol under analysis (hereinafter Protocol) aims to define the terms of collaboration between the Grantors "with a view to the electronic exchange of information regarding the management of episodes and the calculation for the purpose of the process of determining the amount to be borne by the user for the costs of social support and social security reimbursement to the user, within the scope of the RNCCI" (First Clause).

5. The National Network for Continuing Integrated Care (RNCCI), created by Decree-Law No. 101/2006, of 6 June, amended by Decree-Law No. 136/2015, of 28 July, is a organizational structure of public and private institutions providing continuous

health care and social support, created within the scope of the Ministries of Labour, Solidarity and Social Security and Health.

6. The RNCCI's objectives are the provision of health care and social support, in a continuous and integrated manner, to any person who is in a situation of dependence and loss of autonomy, or in a situation of serious mental health illness of which result in psychosocial disability.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

7. The Protocol under analysis concerns data processing for the management of integrated continuing care, initially carried out by the Mission Unit for Continuing Care (UMCCI), created by Council of Ministers Resolution No. 168/2006, of December 18, with the mission of conducting and launching the RNCCI coordination and monitoring project.

8. With the extinction of that Mission Unit, its powers were, under the terms set out in Decree-Law no. 124/2011, of 29 December, integrated into the ACSS, IP.

III. Purpose of treatment and legal basis

9. The processing of data to be carried out for the execution of the Protocol under analysis aims at managing episodes and determining the value of social support charges to be borne by the user, as well as the value of the Social Security contribution, within the scope of the RNCCI.

10. Under the terms of Clause Eight, the parties assume the obligation to ensure confidentiality in relation to personal data, namely by undertaking not to disclose, assign or communicate them to third parties, and also not to use them for purposes other than those provided for in the Protocol.

11. Also under the terms of the aforementioned clause, it is accepted that, by written agreement of the Parties responsible for

the treatment, the data may be used for different purposes (No. of the Protocol (final part in paragraph 4 of the clause).

12. Bearing in mind that this is personal data, in addition to special categories of data that, under Article 9 of the GDPR, benefit from a stricter regime of protection, it should be made clear that the misuse of purposes can only occur under the terms of the RGPD and the Law, and the possibility of the Parties being able to disengage from the obligation of confidentiality, provided for in the final part of paragraph 4 of clause Eight, must be reconsidered.

13. Clause Four says that the lawful ground for the processing of data is that enshrined in subparagraphs c) and e) of paragraph 1 of article 6 of the GDPR.

14. However, given that the data being processed constitute special categories of data, within the meaning of Article 9(1), more precisely health data, such a ground must be found among the grounds provided for in that article, more precisely, in subparagraph b) of paragraph 2 of that article, since the processing is necessary for the purposes of the obligations of the Granting Parties.

15. Although the IAPD refers to consent as one of the grounds for lawfulness, this is to be ruled out. In fact, access to the system is carried out at the request of the user, who must be informed that,

In order to process the request, personal data will be processed, and the information provided for in Articles 13 and 14 of the GDPR will be provided.

16. Furthermore, as explained in recitals o) and p) of the Protocol, the contribution of social security when the typologies of medium-term and rehabilitation units, as well as long-term and maintenance units, in the RNCCI, as well as the integrated mental health care is determined according to the user's income, being "necessary to obtain prior informed consent and the signature of the acceptance term by the user/family/representative" for the purposes of the value of the charges to be borne by the user. 0 which is supported by paragraph 4 of article 10 of Normative Order no. 34/2007, of 19 September, by providing that the internment will only take place when the user, or his/her representative, gives consent by means of a term of acceptance, in which he is responsible for the internment under the conditions set out in this term. Therefore, consent is not here considered as a legal basis for the processing of personal data.

IV. Rights of data subjects

17. Nothing is said about the holder's personal data or its exercise. Although it is not necessary to explain the rights of data subjects, which will always result from the GDPR and the law, it is certain that Clause Five states that it is up to those responsible to define their respective responsibilities, namely with regard to the rights of the data subjects".

18. Thus, the Protocol must indicate, at least, with which entity or entities the holders of personal data can exercise those rights.

V. Data controllers and subcontractors

19. In Clause Five, ACSS, IP and ISS, IP assume themselves as "jointly responsible for the processing of data" provided for in the Protocol, explaining that it is up to them to determine the purposes and means of processing personal data to be carried out by the subcontractors , define the respective responsibilities, namely with regard to the rights of the holders, committing to make available to each other all the information necessary to demonstrate compliance with the obligations provided for in the legislation on data protection.

20. In fact, ACSS, I.P. is the entity responsible for coordinating and monitoring the management of continued care integrated within the scope of the RNCCI, in articulation with the other competent bodies, as provided for in subparagraph g) of paragraph 2 of article 3 of Decree-Law no. 35/2012, of February 15, in its current wording.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

21. For its part, the ISS, I.P. is, under the terms of the respective statutes approved by Ordinance 135/2012, of 8 May, last amended by Ordinance No. 46/2019, of 7 February, and the legal regime established by Decree-Laws No. 101/ 2006, of June

6th and n.° 8/2010, of January 28th, both in their current wording, the body responsible for attributing the user's contribution and social security in the scope of the costs with the provision of care of social support, in the medium-term and rehabilitation and long-term and maintenance units, as well as in all types of mental health care.

22. The II, IP, under the terms of Decree-Law No. 196/2012, of 23 August, is the body responsible, in particular, for ensuring the construction, management and operation of application systems and technological infrastructure in the areas of information and communication technologies of the services and bodies under the Ministry of Labour, Solidarity and Social Security.

23. SPMS, EPE, is responsible for the maintenance, evolution and application support of the RNCCI, sharing with II, IP the responsibility for the management of technological infrastructures and software, so they assume the quality of subcontractors, as identified in Clause Six.

24. It is established that processors may not subcontract unless they have written authorization from those responsible for the treatment, the choice of these processors being conditioned by the requirements set out in paragraph 3 of the same clause.

25. The CNPD has nothing to oppose that II, IP and SPMS, IP are included in the Protocol as grantors, however, it notes that, in the case of subcontractors, the contracts entered into between responsible and subcontractors. In fact, the Protocol is not enough for this purpose, and the duties enshrined in Article 28(3) must be explained in the said contract, and very particularly, that subcontractors can only act upon documented instructions. of those responsible for the treatment.

26. The CNPD notes the need for processors to document all incidents, in order to be able to fulfill the obligations set out in paragraph 4 of Clause Six, that is, comply with the obligation to "make available to those responsible for the treatment all the necessary information to demonstrate compliance with the obligations set out in the legislation in force in terms of data protection".

SAW. Categories of personal data to be processed and data processing

27. In order to carry out the obligations arising from the law and this Protocol, bidirectional communication of personal data is necessary.

28. Admission to the RNCCI is made upon a proposal from one of the teams providing integrated continuous care or from the discharge management teams, when a situation of dependence is found, and presupposes admission to one of the units or

teams that make up the organization.

29. ACCS1 undertakes to make available to the ISS, IP, through SPMS, IP and II, IP, the data of the episodes of continued care, as well as the requests for calculation of the sharing of the costs between the user and the Social Security which are detailed in the Annex, according to two situations: 1) for the purposes of initial data recording and 2) information that is added to that when there is an episode to notify, cancel or reverse.

30. The first of these moments, the following data are indicated: identifier of the initial data record; unique episode identifier; SPMS episode number; the typology of integrated continuing care; the date of the proposal being evaluated at ECL [Local Coordinating Teams]; the state of the episode; identification of the local or regional coordination team; and the identification of the Caregiver Rest field.

31. As regards the second of these moments, the following are indicated: the date of the proposed transfer of typology; the date of cancellation, or closing, or reopening of the episode; the reason for closing the episode; the effective admission date; identifier of the last calculation.

32. It is up to the ISS, IP to process these data in information systems and to allocate the co-payment due by the user and by social security, with the data relating to the status of these requests, as well as the amounts calculated for the sharing of the charges will be consulted by the ACSS in the ISS, IP systems. The data to be made available by the ISS, IP to the ACSS, IP2, regarding the creation of the episode for each reimbursement calculation request, are, according to the Annex, the following: request identifier; Request Date; the calculated daily amount payable by the user; the calculated daily amount to be reimbursed by social security; the calculated daily amount payable by the responsible financial entity (EFR); the order type; the reason for not creating the episode; the user's pronunciation; and the date of signature of the Term of Acceptance.

VII. Information security

33. Regarding access to information, paragraph 4 of Clause Three of the Protocol provides that «it is preceded by articulated authentication between SPMS, EPE and II, IP, through the assignment of an application user and

1 It should be noted that the Annex mentions that the exchange of information takes place between SPMS, EPE and ISS and between this entity and that entity, bidirectionally. However, taking into account the positions that each of the entities involved assumes in the Protocol, the reference to SPMS, EPE (because subcontractor) is presumed to be a mistake, so it was understood as alluding to ACSS, IP as the person responsible.

2 Ditto.

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

of a password, being only allowed to workers duly accredited in the respective systems». It follows that ACSS, IP and ISS, IP will unilaterally determine which workers are authorized to access the interconnection system.

34. However, with ACSS employees as end users of the interconnection system and SPMS as a subcontractor for technological management, it is important to specify how the management of the access allocation life cycle is carried out. In particular, it must be enshrined in the Protocol that it is the responsibility of the ACSS to maintain an up-to-date list of officials accredited for access.

35. It should also be clear how the request for the attribution and cancellation of user accreditations is carried out, that is, if it is addressed to SPMS, EPE, which, in turn, requests it to the Ii, IP or if this is done directly to the ISS, IP.

36. In paragraph 1 of Clause Three, it is stated that “access to information is carried out in real time, through electronic data communication between the systems of the Grantors, using web services specifically implemented”. In turn, p. 15 of the AIPD, when describing and evaluating the controls implemented to deal with general risks related to the security of personal data, it is said that the “identifying code of the entity responsible for the request” is SPMS, EPE.

37. This explanation allows us to understand that, as long as access is obtained from the SPMS, EPE network, to the dedicated and secure circuit between this entity and II, IP, it is possible to invoke the web services of II, IP, passing the identification code of the SPMS. If this is the case, it is recommended to adopt configurations in the networks managed by SPMS, EPE, which ensure that only the servers where the applications for queries and sending data to the ISS are hosted can invoke the web services in question.

38. The wording of paragraph 4 of Clause Nine must be amended, bringing it into line with the provisions of paragraph 2 of

article 33 of the GDPR, with the understanding that, as soon as the subcontractor becomes aware of a data breach personal data, immediately notify the person responsible for the treatment.

VIII. Data registration and conservation

39. It is established, in numbers 6 and 7 of Clause Three, that all information queries carried out under this Protocol are subject to registration by SPMS, EPE, for a period of two years. And that II, IP, proceeds with the access records carried out within the scope of the protocol, under the terms of its audit policy. Nonetheless,

nothing is said about who will have access to these audit records and what are the safeguards for them to be of restricted access, which must be provided for in the Protocol.

40. As for the period and retention of data necessary for the life cycle of care provision, paragraph 2 of Clause Two governs, which must be reconsidered. In fact, it is said that "[t]he data made available under this Protocol are processed exclusively for the purposes set out in the same and only during the respective period of validity". However, taking into account that the retention of data also constitutes, within the meaning of paragraph 2) of article 4 of the RGPD, a processing operation, it is inferred that the data will be processed - and maintained - while the Protocol is in force. This is not acceptable, as it would allow the data to be kept long beyond the time necessary to use it for the purposes for which it was collected.

41. On the other hand, this information seems to contradict what is extracted from the IAPD, namely in its point 2.2.1.3. (page 12), regarding the conservation periods. In fact, that section of the IAPD begins by stating that “under the terms of point e) of article 5 of the GDPR, personal data obtained through interconnection are only kept for the time necessary for the pursuit of the purposes for which they are intended”, concluding, in the table presented there, that the retention period of the "data on file" is 2 years. Since the data must be kept for the time necessary for the pursuit of the purposes for which they are intended, it is assumed that the period of two years is intended to be counted after the termination of the care provision relationship, which is not clear.

42. Bearing in mind the foregoing, the period of retention of the personal data necessary for the implementation of this Protocol

must be clearly established, which cannot be, in the first place, the period of validity of the same, since it would have as a consequence, if the Protocol never expired, the data would be kept indefinitely.

IX. Conclusion

43. Based on the above reasons, the CNPD recommends revising the text of the Protocol, adapting it to the legal requirements of data protection.

44. Furthermore, it suggests that the name of the European Data Protection Committee be indicated in Portuguese, replacing the English name given in paragraph 2 of Clause Thirteen.

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

Approved at the March 2, 2022 meeting

Filipa Calvão (President)