National Data Protection Commission

OPINION/2022/73

I. Order

1. The Social Security Institute, I.P., submitted to the National Data Protection Commission (hereinafter CNPD), for an opinion, the draft Protocol that aims to define the terms of collaboration between the grantors, with a view to the communication of personal data, by via electronic means between the ISS, I.P., the Santa Casa de Misericórdia de Lisboa (SCML) and the Central Administration of the Health System, I.P., (ACSS, I.P.), and the competent entities of the Ministry of Health, under the scope of Law n. 100/2019, of September 6, of the ECI and of Regulatory Decree No. 1/2022, of January 10.

2. The request is accompanied by the Data Protection Impact Assessment (AIPD).

3. The CNPD issues an opinion within the scope of its attributions and competences as an independent administrative authority with authority to control the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57, in conjunction with subparagraph b) of paragraph 3 of article 58, and with paragraph 4 of article 36, all of Regulation (EU) 2016/679, of 27 April 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 domestic legal order.

4. Law No. 100/2019, of 6 September, which approved the Statute of the Informal Caregiver, regulates the rights and duties of the caregiver and the person cared for and establishes the respective support measures.

5. Under the terms of paragraph 1 of article 8 of this law, experimental pilot projects are developed for people who meet the conditions set out in the Statute of Informal Caregiver.

6. The terms and conditions of implementation of the aforementioned pilot projects were, in turn, regulated by Ordinance No. 64/2020, of 10 March, having created a framework and monitoring program, as well as support measures to the informal caregiver.

7. For the purposes of applying the aforementioned Law, protocols may be established between social security services and entities from different sectors, namely health, justice, education, employment and professional training and security forces - cfr.

Article 13(1)(1).

8. It is therefore important to regulate the sharing of personal data between the ISS, I.P., the SCML and the ACSS, I.P within the scope of support for the Informal Caregiver, and in particular with regard to the flows of treatment of crucial information for the identification of the healthcare referral professional (PRS), and the healthcare professional

II. Analysis

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976832

geral@cnpd.pt

www.cnpd.pt

social security reference (PRSS), the definition of the Caregiver Specific Intervention Plan (PIE) and the maintenance or cessation of the ECI and other support measures, which is now being implemented,

9. The data that are recorded and shared are those contained in Annex I in the proposed Protocol, with a distinction being made between the attributes that are automatically obtained from the Social Security information systems and the attributes that are manually introduced by the various stakeholders responsible for processing the data. The data listed are related to the process, the informal caregiver, the people cared for, the professionals, the Specific Intervention Plan, institutional articulation and process management.

10. The personal data that can be processed are adequate, relevant and necessary for the purposes in question, in compliance with the principle of data minimization provided for in subparagraph c) of paragraph 1 of article 5 of the RGPD.

11. However, and following the recommendation made by the AIPD, it is suggested that access to data be delimited by geographic area, in order to ensure that technicians from a given area can only access processes in that same geographic area. Likewise, it is agreed with the need to identify in the Protocol which entities will have access to each data subject to treatment. This measure aims to reinforce compliance with the principle of data minimization and the need to know principle, limiting access to strictly necessary data.

12. As for the legal basis, Clause Four provides that the processing of personal data provided for in this Protocol is necessary for the exercise of the public attributions of the ISS, IP and SCML, within the scope of social action, and the public attributions of the ACSS, I.P. and other services of the Ministry of Health involved in the provision of health care and the management of the health system, under the terms of Law No. To that extent, the processing of data carried out within the scope of this protocol is legally based on the provisions of subparagraph e) of paragraph 1 and paragraph 3 of article 6 of the GDPR and subparagraph b) of paragraph 1. 2 of article 9 of the same legal diploma.

13. With regard to data retention periods, Clause Fifth of the Protocol governs. However, the Protocol refers to the Joint Normative Circular No. 8/2020/ACSS/ISS regarding the definition of the articulation model between the entities and structures that make up the Social Security and Health areas within the scope of the Informal Caregiver Statute. In point 10 of the circular, it is established that the termination of the Informal Caregiver Statute determines the termination of the PIE (Specific Intervention Plan) for the caregiver. In Clause Fifth of the Protocol, it is indicated that the data are kept while they are in use and, after the termination of the ECI, they are still retained for 2 years for audit purposes.

14. However, regarding this retention period, it is recommended that Clause Five be densified, indicating the user profile that will have access to the data when they change from “Data in use” to “Data on file”. It is also proposed to include a provision for an automatic deletion of data after the expected retention period.

15. Under the terms of Clause Six of the draft Protocol under analysis, the ISS, I.P., SCML, ACSS, I.P. and the other services of the Ministry of Health that intervene in the processing of personal data regulated in the Protocol, with II, I.P being the subcontractor. This is a case of joint liability, pursuant to Article 26 of the GDPR, which presupposes the existence of an agreement that duly reflects the respective roles and relationships of the joint controllers in relation to the data subjects. The CNPD thus suggests that the content of Clause Six be amended in order to contain an express reference to the existence of an agreement between the controllers that enshrines their respective responsibilities for compliance with the GDPR or, alternatively, that this delimitation be expressly regulated herein. .

16. As for the Eighth Clause, concerning the subcontractor's obligations, paragraph 2 states that 'The choice of further

subcontractors is deemed to be delegated to the subcontractor, without prejudice to the provision of an updated list with their identification, together with the contractual conditions applicable and the right of opposition'. It should be noted that Article 28(2) of the GDPR provides for the possibility for a processor to contract another processor, subject to prior “specific or general” authorization from the controller, but obliges the processor to inform the controller “of any intended changes in terms of increasing the number or replacement of other processors, thus giving the controller the opportunity to object to such changes”.

17. It is understood, therefore, that the wording of Clause Eight is too general and permissive, not complying with the legal requirements of subcontracting provided for in paragraphs 2 and 4 of article 28 of the GDPR, since the subcontractor may only carry out further subcontracting if these subcontractors provide 'sufficient guarantees that appropriate technical and organizational measures will be carried out...'. It is also suggested to replace the reference to the right of opposition by the possibility of opposing, since that expression is attributed in the GDPR to data subjects, under the terms of its article 21.

18. Therefore, it is recommended that paragraph 2 of Clause Eight be corrected and that references to the obligations of subcontractors set out in paragraphs 2 and 4 of Article 28 of the GDPR be inserted therein.

19. It is noted that the Protocol does not contain anything about the rights of data subjects, so it is recommended to introduce an item that expressly contemplates them and regulates the way in which these rights are exercised.

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

20. The data is registered and shared through the Collaborative Platform for Content Management, accessible on the Social Security extranet, whose management and maintenance is the responsibility of ISS, I.P. According to Clause Nine of the Protocol, the IT solution that allows shared access is based on an infrastructure of servers physically in the II, I.P. data

processing center, and located on the MTSSS computer network, being made available to external entities through the Extranet. of this same network.

21. Note that it is not clear what mechanism this Extranet has to control access to the network, so it is proposed to interconnect with the private networks of the Ministry of Health and SCML, through VPN, or, alternatively, the implementation of a strong authentication system (preferably through certificates).

22. In turn, point e) of Clause Ten states that “the authenticity of the platform is guaranteed by a Digital Certificate, through data encryption between the browser (client) and the platform (server) vveb”. It is safeguarded that this encryption must resort to the use of Trcmsport Layer Security (TLS), in its most recent version.

23. Finally, the Eleventh and Twelfth Clauses of the Protocol regulate the accession by the services of the Ministry of Health and Santa Casa da Misericórdia de Lisboa through the provision of an updated list with the identification of users, being obliged to communicate any change. It is recommended to use strong credentials with long, unique, complex pctsswords and with numbers, symbols, uppercase and lowercase letters, as well as the implementation of two-factor authentication mechanisms.

III. Conclusion

24. Based on the above grounds, the CNPD recommends:

a) Amendment of Clause Three in order to establish the delimitation of access to data by geographic area, as well as identify in the Protocol which entities will have access to each data subject to processing;

b) The densification of Clause Five with the indication of the user profile that will have access to the data when they change from «Data in use» to «Data on file» and also the inclusion of the provision of an automatic data elimination process after the period expected retention;

c) The reformulation of Clause Six in order to contain an express reference to the existence of an agreement to be concluded between the controllers that enshrines their respective responsibilities

w

compliance with the GDPR or, alternatively, that the delimitation of responsibilities is expressly regulated herein;

d) Correction of paragraph 2 of Clause Eight and that references to the obligations of subcontractors set out in paragraphs 2 and 4 of article 28 of the GDPR are inserted therein;

e) The introduction of an item that expressly contemplates the rights of data subjects and regulates the way in which these rights are exercised; and

f) The reformulation of Clause Nine, providing that the interconnection with the private networks of the Ministry of Health and SCML takes place through VPN, or, alternatively, the implementation of a strong authentication system (preferably through certificates).

Lisbon, August 10, 2022

Maria Cândida Guedes de Oliveira (Rapporteur)

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