__ D

National Data Protection Commission

OPINION/2022/68

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 establish the terms and conditions of access to the information system within the scope of the transfer of powers, in service and social monitoring service (SAAS) and monitoring of insertion contracts of beneficiaries of the Social Insertion Income (RSI), to be concluded with the Municipalities, under the scope of Decree-Law No. 55/2020, of 12 of August, and respective regulations. The Social Security Institute, I.P., (ISS), the Informatics Institute, I.P., (II, I.P.) and the municipalities are grantors in this Protocol.

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 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 n° 58 /2019, of 8 August, which enforces the GDPR in the domestic legal order.

II. Analysis

4. Law No. 50/2018, of 16 August, establishes the framework for the transfer of powers to local authorities and to inter-municipal entities, with Article 4(1) providing that the transfer of new powers , the identification of the respective nature and the way in which the respective resources are allocated are carried out through legal acts of a sectoral scope relating to the various areas to be decentralized from the direct and indirect administration of the State, which establish transitional provisions suitable for the management of the transfer procedure in cause.

5. Decree-Law No. 55/2020, of 12 August, implements the transfer of powers to municipal bodies and to inter-municipal

entities in the field of social action, under paragraphs c) and f) of article 3. °, and articles 12 and 32 of Law No. 50/2018, of 16 August.

6. For the exercise of these new powers, pursuant to paragraph 1 of article 6 of Law no. 50/2018, the guarantee of access by municipalities to the information systems used by the direct and indirect administration of the State is determined, for process management and other information integrated into the transferred competences. Thus, pursuant to articles 10 and 11 of Decree-Law No. 55/2020, it is recommended that the

Av. D. Carlos 1,134.1o T (+351) 213 928400 geral@cnpd.pt

1200-651 Lisbon F (+351) 213 976832 www.cnpd.pt

development of the social assistance and monitoring service and the signing and monitoring of the contracts for the insertion of RSI beneficiaries are carried out using a specific information system.

7. In turn, Ordinance no. 63/2021, of 17 March, regulates the provisions of paragraphs a) and e) of paragraph 1 of article 3 and article 10 of Decree-Law no. .° 55/2020, of 12 August, namely the terms of operationalization of the transfer of competences, in terms of assistance service and social monitoring (SAAS) of people and families in situations of vulnerability and social exclusion, to the municipal councils , and Ordinance No. 65/2021, of 17 March, establishes the terms of operationalization of the transition of powers in terms of the execution and monitoring of contracts for the insertion of RSI beneficiaries to municipal councils, taking into account the provisions of subparagraph f) of paragraph 1 of article 3 and in article 11 of Decree-Law n.° 55/2020, of 12 August.

8. It should be noted that Article 14 of Ordinance No. 188/2014, of 18 September, amended by Article 2 of Ordinance No. 63/2021 and Article 27(1) -A added to Ordinance No. 257/2012, of August 27, by article 3 of Ordinance No. 65/2021, states that access to the specific information system is restricted to data relevant to the pursuit of powers assistance and social monitoring and monitoring of RSI beneficiaries within the scope of the insertion contract.

9. Clause Two, which defines the scope and context of data processing, provides that "data processing is carried out within the scope of the service of care and social monitoring of people and families in situations of vulnerability and social exclusion and for Municipalities, as well as social emergencies" (emphasis added). Clarification of the text is suggested as its meaning is not

reached.

10. Regarding the lawfulness of the processing of personal data in question, Clause Four of the draft Protocol states that “1. The processing of personal data is carried out through the free, specific, informed and unequivocal consent of the respective holder or of his legal representative, for the purposes indicated in the previous clause, in accordance with the provisions of subparagraph a) of paragraph 1 of article 6. .°, in article 7 and article 14 of the RGPD as well as in compliance with Law No. 58/2019, of August 8, formalized by the informed consent document - whose model is attached to this Protocol, as Annex I, of which it forms an integral part'.

11. However, Annex II, which details the personal data of the data subject and the members of the household being processed, refers to data relating to health, which are part of the special categories of personal data provided for in Article 9 of the GDPR.

12. Thus, under the terms of subparagraph a) of paragraph 2 of this article, its processing is possible if the data subject has given his explicit consent to the processing of such personal data for one or more specific purposes.

13. In order to justify the lawfulness of the processing, the Social Security Data Protection Officer, in her assessment of the AIPD, invokes Authorization No. information regarding the Social Action Information Subsystem, where it is determined "It must, however, endeavor to collect the prior and informed consent of the data subjects regarding matters of a sensitive nature, namely those relating to the privacy and health data of potential beneficiaries" .

14. It is important to clarify that the legal framework today is substantially different, with the entry into force and application of the RGPD, so the provisions of that authorization must be reviewed, in order to find the legal basis that best suits the new legal framework. suit. Now, if in 2005, in view of the law in force, there was no other legal basis to support the processing of sensitive data, now the RGPD offers, among the range of grounds of paragraph 2 of article 9, conditions that better are suitable for this treatment.

15. Mainly because, as highlighted in Article 4(11) of the GDPR, consent to be valid must be free. And, in the type of situations

envisaged here, it is difficult to ensure an effective freedom of expression of will. As explained in recital 42 of the GDPR, consent should not be considered to be free if the data subject does not have a true or free choice or cannot refuse or withdraw consent without prejudice. Precisely, in the present case, the refusal of consent or the decision to withdraw it has extremely serious consequences for the data subject, who may be deprived of fundamental social support for a dignified life.

16. Furthermore, pursuant to recital 43 of the GDPR, consent should not constitute a valid legal basis for the processing of personal data in specific cases where there is a clear imbalance between the data subject and the controller, namely when the latter is a public authority.

17. In this way, and because the data subject does not have a valid alternative to consent, it is understood that, in this case, there are no conditions for the free expression of consent, and therefore cannot constitute a valid legal basis. for the processing of personal data.

18. The architecture of the legal basis for the processing of data in question must therefore begin by considering one of the situations provided for in Article 6 of the GDPR. It is understood that subparagraph c) of paragraph 1 applies in the case under analysis, insofar as the processing is necessary for the fulfillment of a legal obligation

to which municipalities become subject with the transfer of competences in social matters operated by Decree-Law No. 55/2020, of 12 August. Then, in view of the processing of special categories of data provided for in article 9 of the GDPR, the reason for exclusion from the prohibition of their processing must be indicated.

19. In these terms, the processing of special categories of data is possible if, pursuant to Article 9(2)(b) of the GDPR, their processing is necessary for the purposes of complying with obligations and exercising specific rights of the controller or data subject with regard to legislation... on social security and social protection insofar as such processing is permitted by Union or Member State law... which provides for adequate guarantees of rights fundamentals and interests of data subjects.

20. However, Decree-Law 55/2020, while attributing powers to Municipalities in social matters, does not provide for adequate safeguards in order to protect personal data and other fundamental rights (cf. recital 52 of the GDPR), as it should have been

guaranteed by the legislator.

21. Therefore, in order to remedy the legislative omission, it is important to ensure that the aforementioned safeguard measures are expressly included in the text of the Protocol.

22. In view of the foregoing, the CNPD suggests the elimination of paragraphs 1 and 2 of Clause Four as well as Annex I - Model of Informed Consent. It also recommends amending paragraph 3 of this Clause in the part relating to the rights of the data subjects referred to therein (rights of access, rectification and erasure), placing them in the Fourteenth Clause relating to this matter.

23. In turn, Clause Five, relating to the personal data being processed, refers to Annex II. The personal data of the applicant and the members of his household referred to therein result from the list of mandatory documentation that must accompany the application addressed to the competent Social Security services for the attribution of RSI and the social report provided for in articles 3 and 16. of Ordinance 257/2012, amended by Ordinance 65/2021. Note that Annex II refers to a civil identification document (Portuguese, foreign), while paragraph a) of paragraph 1 of article 3 of Ordinance 257/2012 refers to “photocopy of civil identification documents”. The CNPD expresses, once again1, the reservations that the copy of the identification document raises regarding the value of the proof of identity, since the digitization of an identification document

1 See Opinion No. 31/2017, of May 17, 2017, available at https://www.cnpd.pt/decisoes/historico-de-decisoes/?vear-2017&tvpe=4&ent= and also the Opinion No. 142/2020, of December 3, 2020, available at https://www.cnpd.pt/decisoes/historico-de-decisoes/?yeam2020&type=4&ent= and Opinion 2021/118, of September 7 2021, available at https://www.cnpd.pt/decisoes/historico-de-decisoes/7yeam2Q21 &tvpe=4&ent=

it is easily manipulated, thus not guaranteeing the veracity of the data, in disregard of the principles of accuracy and completeness of personal data enshrined in points d) and f) of paragraph 1 of article 5 of the GDPR.

24. It is reaffirmed that the simple copy of the identification documents constitutes a document without any probative legal value, precisely because of the ease of handling, so it is recommended to opt for other forms of proof of the applicants' identity

and the consequent revision of the list of mandatory attachments.

25. A reference to the 10-year period for data retention provided for in Clause Six of the Protocol is required. The IAPD does not present any justification for this period, so the CNPD is not in a position to comment on compliance with the principle of limitation of conservation provided for in paragraph e) of article 5 of the RGPD.

26. Pursuant to paragraph 1 of Clause Seven and Clause Ten, the ISS, I.P., and the Municipality are responsible for the processing of personal data, with II, I.P being the subcontractor. From the analysis of the Protocol, it appears that we are dealing with a case of joint liability, under the terms of 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 Ten be amended in order to contain an express reference to the existence of an agreement between the two controllers that enshrines their respective responsibilities for compliance with the RGPD.

27. Note that regarding the definition of the role of subcontractor, the draft protocol, in recital

b), provides that the II,I.P. intervenes in this protocol because it is 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, under the terms of paragraph c) of paragraph 2 of article 3 of Decree-Law no. 196/2012, of 23 August, while the AIPD only indicates the role of «ensuring «(...) access to training, in distance modality - e-learning format, through the Training Portal - https://portalformacaoii.sea-social.pt/SGForm/».

28. On the other hand, it appears that the draft Protocol is completely silent on the implementation of the form of communication between the Municipalities' computer networks and the II, I.P. In fact, in the AIPD, access control section, network security indicates that “the Institute of Informatics' interoperability platform is integrated and is permanently monitored by the Operational Control Center”. In turn, in «Annex III - Draft Term of Responsibility» of the Protocol, it is stated that each municipal employee with functions to perform within the scope of the Social Assistance and Monitoring Service (SAAS), will hold

access to the specific information system called “WebSISS”, not being, therefore, through the interoperability platform of II, I.P.

29. In addition, from the analysis of the description of the implementation of controls, it appears that, in general, they all refer to the interoperability platform of the II, I.P. The only one that specifically refers to the WebSSIS system is the control of «Integrity Monitoring». Thus, it appears that the AIPD is not focused on what is defined for the operationalization of the protocol.

30. Not being provided for in the IAPD, the assets on which personal data depend (e.g., computer equipment, software, networks, people, paper or paper transmission channels), attention is drawn to the need, in communications between the II, I.P. and the Municipalities, there is the capacity to guarantee the correct identity of the sender and recipient of the transmission of personal data. Thus, and in accordance with the technical requirements of Resolution of the Council of Ministers No. 41/2018, it is recommended to use secure communication technology (for example, VPN), with a strong authentication system (preferably through certificates) , so that the transmission of data between entities from different technological environments is carried out safely.

31. In accordance with paragraph 5 of Clause Eight of the draft Protocol, each query/change is auditable at all times, in the information system, as to the user who performed it and the respective date/time. These audit data are kept for a period of 2 years. The CNPD notes that, when preserving the information that has been consulted/changed, it is relevant to indicate who will have access to these audit records and what are the safeguards for them to be of restricted access, so it is recommended to introduce an item containing these indications.

33.In turn, in the AIPD, point 2.3.1, Assessment of security controls, indicates for encryption that "The communication of data, within the scope of this protocol, is carried out through secure communication (HTTPS), with the encrypted and secure data in transit'. Thus, it is recommended that all communications be encrypted, using the HTTPS protocol, using Transport Layer Security (TLS), in its most recent version.

34. The protocol refers in Clause Eight (Management of the information system) to accreditation in the WebSSIS system by identifying users authorized by the Municipality, with a view to assigning a user code and a password, personal and

non-transferable. In this regard, we take the opportunity to make the following recommendations: a) there must be a policy of using strong credentials with long, unique, complex passwords with numbers, symbols, uppercase and lowercase letters; b) lock accounts after several invalid login attempts, and c) if feasible, the use of a password, preferably in combination with another factor (2FA).

EC»

National Data Protection Commission

35. On the other hand, given the access to personal data by the various municipalities, it is suggested that II, I.P. carry out a periodic verification that the defined security measures are in place, ensuring that they are effective and regularly updating them, especially when processing or circumstances change, including those implemented by municipalities in the context of data processing.

36. With regard to Clause Eleven, concerning the subcontractor's obligations, paragraph 2 provides 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 conditions applicable contractual terms 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".

37. It is understood, therefore, that the wording of Clause Eleven 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 whereas the subcontractor may only carry out further subcontracting if those subcontractors provide 'sufficient guarantees that appropriate technical and organizational measures are 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 RGPD to data subjects under the terms of its article 21,°.

38. Therefore, it is recommended that Clause Eleven 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.

39. Finally, Clause Fourteen provides that the exercise of rights by data subjects can be done with the Municipality, and a point of contact related to the RGPD for data subjects for data protection matters must be identified. data to respond to the exercise of rights, treatment of incidents of violation or requests for clarification and be the link between the various entities both in the execution of associated activities, as well as in the clarification of doubts related to the RGPD.

40. In this regard, it is only recalled that, pursuant to Article 26(3) of the GDPR, in the case of joint controllers, the data subject may exercise the rights conferred on him by the GDPR in relation to each of the data controllers, and that clause must be interpreted in accordance with such power.

41. Bearing in mind the reference made in that clause to a contact point related to the GDPR, it is also worth remembering that, like any public body, municipalities have a duty, as

responsible for processing personal data, to designate a data protection officer (DPO) in accordance with Article 37(1)(a) of the GDPR, to publish the EPD's contact details and to communicate them to the CNPD. Finally, under the terms of paragraph 4 of article 38, data subjects may contact the EPD on all matters related to the processing of their personal data and the exercise of their rights. Therefore, the CNPD recommends reformulating paragraph 1 of Clause Fourteen, replacing the reference to a contact point with the reference to the EPD.

III. Conclusion

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

a) Elimination of numbers 1 and 2 of Clause Four and Annex I - Model of Informed Consent. It also recommends amending paragraph 3 of this Clause in the part relating to the rights of the data subjects referred to therein (rights of access, rectification and erasure), placing them in the Fourteenth Clause relating to this matter;

b) The reformulation of Clause Ten in order to contain an express reference to the existence of an agreement between the two controllers that delimits their respective responsibilities for compliance with the RGPD;

c) The introduction of an item that expressly refers to the implementation of the form of communication between the computer

networks of the Municipalities and the II, I.P network, as well as the indication of the use of secure communication technology, with a strong authentication system, so that the transmission of data between entities from different technological environments is carried out securely.

d) The introduction of a point c) in paragraph 1 of Clause Eight containing the recommendations referred to in point 34;

e) The addition to no. 5 of Clause Eight in order to indicate who will have access to the audit records and what are the safeguards for them to be of restricted access.

National Data Protection Commission

f) The reformulation of Clause Eleven in order to include references to the obligations of subcontractors set out in paragraphs 2 and 4 of article 28 of the RGPD; and

g) The amendment of paragraph 1 of Clause Fourteen, stating that the contact point must be the EPD.

Approved at the meeting of July 28, 2022

7/

Cy

Filipa Calvão (President)

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