OPINION/2021/127

I. Order

1. The Social Security Institute, I.P., submitted to the National Data Protection Commission (hereinafter CNPD), for an opinion, the Protocol that regulates electronic interoperability between the information system supporting the activity of the courts, the computer support system the activity of enforcement agents and the information systems of social security, the salary guarantee fund and the general retirement fund in connection with the execution of attachments of social benefits and pensions.

2. The CNPD issues an opinion within the scope of its attributions 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, 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.

3. The request is accompanied by a draft interoperability protocol proposal, an annex with technical and functional specifications regarding data communications and the Data Protection Impact Assessment (AIPD).

4. Intervening in the Protocol are the Institute of Financial Management and Justice Equipment (IGFEJ, I.P.), the Institute of Social Security, I.P., (ISS, IP), the Institute of Financial Management of Social Security, (IGFSS), the Institute of of Social Security of Madeira, I.P.-RAM (ISSM-I.P.-RAM), the Social Security Institute of the Azores. I.P.-RA (ISSA.I.P.-RA), Caixa Geral de Aposentações, I.P. (CGA), the Institute of Informatics, I.P. (II, IP) and the Order of Solicitors and Enforcement Agents (OSAE).

5. Pursuant to paragraph 5 of article 132 of the Code of Civil Procedure, approved by Law n.° 21/2013, of 26 June, in its

current version, communications between courts or enforcement agents and the Social Security can be carried out electronically, by sending structured information and interoperability between the information system to support the activity of the courts and the Social Security information system, under the terms provided for in an ordinance of the members of the Government responsible for the area. of justice and social security. Thus, Ordinance No. 331-A/2009, of December 3, with the last wording given by Ordinance

II. Analysis

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

358/2019, of 8 October, regulates the interoperability between the IT System that provides support to the Courts and the Social Security Information System.

5. It should be noted that, after the request for indictment was submitted, Ordinance No. 137/2021, of June 30, was published, which makes the first amendment to Ordinance No. 358/2019, of October 8, and which extends electronic communications between enforcement agents and Social Security, the Salary Guarantee Fund and Caixa Geral de Aposentações, covering the awarding of social benefits and pensions paid by these entities, at the same time time that electronic communications between judicial courts and Social Security, the Salary Guarantee Fund and Caixa Geral de Aposentações are regulated in the context of obtaining information contained in the databases of these entities for deductions of amounts in social benefits and pensions paid by them.

7. Paragraph 5 of article 2 of this Ordinance refers to the previous number 4 of Ordinance no. 358/2019, of 8 October, which establishes that the achievement of interoperability between the aforementioned information systems is carried out by means

of a protocol to be concluded between the Institute of Financial Management and Justice Equipment, I.P., the Institute of Social Security, I.P., the Institute of Financial Management of Social Security, I.P., the Social Security Institute of Madeira, IP-RAM , the Instituto da Segurança Social dos Açores, IPRA, Caixa Geral de Aposentações, I.P., the Instituto de Informática, I.P., and the Ordem dos Solicitors and Execution Agents, which now takes place.

8. Therefore, the basis of legitimacy for this data processing is considered to fall under Article 6(1)(c) of the GDPR.

9. Under the terms of Clause 1,a, the purpose of the Protocol is to regulate the terms and conditions of the interoperability of personal data, by electronic means, between the enforcement agent, Social Security, the Salary Guarantee Fund and Caixa Geral de Pensions within the scope of attachment of social benefits and pensions in the executive processes of the judicial courts, in order to comply with the provisions of the Ordinance. Attention is drawn to the possible need to update the object of the Protocol with the changes introduced by Ordinance No. 137/2021, of June 30th.

10. Paragraph 1 of clause 2.a of the Protocol provides that "Electronic communication of data between the systems of the granting entities is carried out using web services, specifically implemented in order to protect the supply of data, and through a secure channel , the parties agreeing to implement this electronic interoperability process, in accordance with the technical and functional specifications contained in the document annexed to this protocol».

11. However, from consulting the Annex to which you refer, there is no information about the secure channel used, and the same Annex is still silent as to the communications architecture for the transfer of data between IGFEJ, I.P., and II, I.P./CGA. It should be noted, however, that from reading the IAPD framework on the identification of security controls, networks and interoperability appear as an acceptable risk, so it appears that their study has been carried out.

12. Therefore, the CNPD recommends that the Protocol contain the necessary measures for the existence of a secure communication channel, complying with security requirements, namely the configuration of a VPN, secure data encryption and secure communication protocols.

13. It is important to mention that, under the terms of paragraph 1 of Clause 2.a, the Protocol contemplates the electronic

communication of data between the systems of the granting entities, and it is up to the IGFEJ, I.P., II, I.P., and CGA to ensure the development of the services necessary in this area, in accordance with the requirements that may be defined by the Working Group that monitors the implementation of this interoperability (cf. Clause 7 a). Given that, in the preamble to the Protocol, it is stated that communications between courts or enforcement agents and Social Security can be carried out electronically, it is important to emphasize that what is authorized, by means of a protocol, is the interoperability between the computer system that provides support to the Courts and the Social Security information system.

14. In turn, clause 1,a of the Protocol provides that it "is intended to regulate the terms and conditions of the interoperability of personal data, by electronic means, between the enforcement agent, Social Security, the Salary Guarantee Fund and Caixa Geral de Aposentações". And in paragraph 2 of clause 2.a of the Protocol it is stated that "communication between systems requires prior authentication both between the IGFEJ, I.P., and the II, I.P. as between IGFEJ, I.P., and CGA, by assigning an application user and a password». Thus, with the execution agents as end users of the interoperability system, it is important to specify in the Protocol how access is allocated and their life cycles are made.

15. It is also important that the Protocol determines that it is up to the Order of Solicitors and Enforcement Agents to maintain an updated list of enforcement agents and request the allocation or cancellation of users to the entity that maintains the computer support system for the courts, namely the IGFEJ, I.P.

16. It should be noted that the records of all consultations, accesses and information sent under this Protocol are kept for a considerable period (cf. paragraphs 3 and 4 of Clause 2.a). Thus, the CNPD recommends that in the Protocol it is clarified who will have access to these audit records and what safeguards to adopt so that they are of restricted access.

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

í

17. In turn, Clause 3.a defines that the data to be made available to the enforcement agent under the Protocol are those contained in the Annex: information on a beneficiary (date of birth and date of death of a beneficiary, name and address of employers associated with the beneficiary, address, NIF, NISS, full name, CGA identification number, beneficiary's civil identification number), information relating to a legal person (name, address, NIF, NISS of the members of Organs statutory bodies) and record of attachments (bank identification number, NIF and NISS of the pledged beneficiary, CGA beneficiary number, professional certificate, name and NIF of the recipient). The data being processed are adequate and limited to what is necessary for the purposes in question, in compliance with the principle of necessity and data minimization provided for in Article 5(1)(c) of the GDPR.

18. As regards the data retention period, paragraph 5 of Clause 2.a sets a maximum period of 20 years. However, article 6 of Ordinance No. 331-A/2009, of 3 December, with the last wording given by Ordinance No. 358/2019, of 8 October, provides that "the personal data contained in the consultation records referred to in the previous numbers are kept only for the period necessary for the pursuit of the purposes for which they are intended, and must be destroyed automatically: a) 10 years after their collection; b) or after the filing of the court case, if the case remains pending for a period longer than that provided for in the previous paragraph.». Therefore, in compliance with the principle of limiting data retention provided for in point e) of article 5 of the GDPR, it is recommended to reformulate paragraph 5 of Clause 2.a in order to comply with this provision or, alternatively, its elimination.

19. Pursuant to Clause 4.a, ISS, I.P., IGFSS, ISSM, I.P.-RAM, ISSA are responsible for processing. I.P.-RA, the CGA, I.P. and the OSAE. The IGFEJ, I.P. and II, I.P are subcontractors since they are responsible for the management of technological infrastructure and software, given their attributions, provided for in article 3 of Decree-Law No. 164/2012, of 31 July, and in Article 3(2)(a) of Decree-Law No. 196/2012, of 23 August, respectively. The obligations of controllers and processors are regulated in Clauses 6.a and 7.a in accordance with the provisions of Articles 24 and 28 of the GDPR.

20. A note only regarding the identification of the parties' interlocutors and their respective contacts for the purpose of monitoring the execution of the protocol that is considered positive, as well as the obligation to carry out all communications in writing.

21. In turn, in the chapter "3. Validation of the IAPD", in the table on compliance with good security practices of the controls

implemented for the treatment of risks related to data security, encryption appears as not applicable, which does not appears correct. In fact, it may be inferred that no

0

PAR/2021/40 3

CNPD

National Data Protection Commission

encrypting information in data transfers or in the repositories where they are stored is considered. Therefore, a revisitation of this point of the AIPD is suggested.

22. Finally, with regard to the security measures listed, without prejudice to the need for additional clarifications on omitted points identified above, they seem appropriate. However, the need for permanent verification of compliance is underlined.

III. Conclusion

23. Thus, on the grounds set out above, the CNPD recommends:

The. The reformulation of paragraph 1 of Clause 2.a of the Protocol in order to contain the measures necessary for the existence of a secure channel of communication;

B. The implementation in paragraph 2 of Clause 2.a of the form of attribution of accesses and respective life cycles;

ç. The introduction of an item that assigns to the Order of Solicitors and Enforcement Agents the obligation to maintain an up-to-date list of enforcement agents and to request the assignment or cancellation of users to the entity that maintains the computer support system for the courts, namely the IGFEJ, I.P;

d. That the Protocol clarifies who will have access to the audit records and what safeguards to adopt so that they have restricted access; and

and. That the data retention period be harmonized with the provisions of article 6 of Ordinance No. 331-A/2009, of 3 December, in the current wording.

Approved at the meeting of September 21, 2021

Filipa Calvão (President)

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