National Data Protection Commission

OPINION/2022/72

I. Order

1. The Social Security Institute, LP. (ISS, IP) requested the National Data Protection Commission (CNPD) to issue an opinion on a Convention that aims to determine the terms and conditions of cooperation between this Institute, the Social Security Institute of the Azores, IP.RA, (ISSA, IP RA), the Social Security Institute of Madeira, IP-RAM (ISSM, IP RAM) and the Institute of Informatics, IP (II.EP) and the Caisse Nationale d'Assurance Vieillesse (CNAV), in regarding the electronic exchange of information on deaths/existence of insured persons, in accordance with Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems and Implementing Regulation (EC) No. 987/2009 of the European Parliament and of the Council of 16 September 2009, which lays down the detailed rules for implementing Regulation (EC) No.

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

3. The request made and the opinion issued now derive from the attributions and powers of the CNPD, as the national authority for controlling the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57 and by paragraph 4 of article 36 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Regulation on Data Protection - RGPD), in conjunction with the provisions of article 3.", in Article 4(2) and Article 6(1)(a), all from Law No. 58/2019, of 8 August.

4. Regulation (EC) No. 883/2004 of the European Parliament and of the Council, of 29 April 2004, defined the rules for coordinating national social security systems, within the scope of the free movement of persons.

5. In turn, Implementing Regulation (EC) No 987/2009 of the European Parliament and of the Council of 16 September 2009 lays down the modalities for implementing Regulation (EC) No 883/2004. It should be noted that, under the powers conferred by Article 71 of Regulation (EC) No. 883/2004, the Administrative Commission for the Coordination of Social Security Systems, established, through Decision No. 115, of March 18, 2010, some rules to ensure cooperation between competent national authorities regarding the exchange of personal data.

883/2004.

II. Analysis

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

IV

V,

V.-

6. Under the terms of the aforementioned Regulations, the different institutions of the EU Member States are allowed to exchange the information necessary to verify the existence of persons who fulfill the conditions for entitlement to benefits, as well as to calculate and correctly pay of benefits and verification that entitlement to those benefits is maintained.

7. The CNAV, as responsible for the French legal system of pensions for employees and self-employed workers, must verify the existence of the persons to whom the benefits are paid. Furthermore, the mandatory pension schemes delegated to the CNAV, operator of the National System for the Management of Identifiers (SNGI), the mission of requesting information from the institutions of the other EU Member States on whether the persons covered by the respective schemes, residing in those States, are still alive. In fact, Decree No. 2018-390, of 24 May 2018, provides that the SNGI is intended to verify that the insured are still alive.

8. Pursuant to Article 104 of Law No. 2020-1576 of December 14, 2020 and Decree No. 2021-390 of April 2, 2021, concerning the control of the existence of old-age pension holders and other pensions residing outside France, French mandatory pension schemes share the management of information on proof of life, in order to make checks on the existence of the persons concerned more effective.

9. In turn, pursuant to Article L215(1) of the French Social Security Code, Pension Funds and Occupational Health Insurance register and verify the data necessary to determine the pension rights of those insured under the general scheme. , settle and

pay the pensions resulting from these rights.

10. On the other hand, Law No. 4/2007, of 16 January (Basic Social Security Law), in article 25, concerning the relationship with foreign systems, provides that "The State promotes the conclusion of instruments of coordination on social security with the aim of guaranteeing equal treatment to the beneficiaries covered by it who exercise a professional activity or reside in the respective territory with regard to rights and obligations, under the applicable legislation, as well as the protection of acquired rights and in training .» 1

11. Thus, this Convention regulates the electronic exchange of computer files with information on deaths/existence of persons residing in France, who receive a benefit from the ISSJ.P., ISSM.IP-

1 See, in particular, Decree-Law no. 187/2007, of 10 May, concerning the legal regime of protection in the event of old age and disability of the general social security system; Decree-Law No. 322/90, 18/10, of October, concerning the legal protection regime in the event of death of the general social security regime.

RAM and ISSA,IPRA, on the one hand, and, on the other hand, of persons residing in Portugal who receive a benefit from the CNAV and the French mandatory pension schemes.

12. The communication of personal data constitutes a processing of personal data, within the meaning of point 2) of article 4 of the RGPD. Annex 1 of the Convention is dedicated to the protection of personal data.

13. From the analysis of this Annex, it appears that point 2 (responsibility of the parties) refers that the country issuing the data is responsible for transferring these data to the other country. Once the data is received, the country is responsible for its own processing activities. However, under Article 4(7) of the GDPR, the controller is the natural or legal person, public authority, agency or other body that individually or jointly with others determines the purpose and means of processing. It is therefore recommended to reformulate this section in order to accurately use the terms used in the GDPR2, in order to indicate the Portuguese or French granting party as responsible, as the case may be. The same applies to point 3, which refers to data protection officers (DPS) and reference entities in terms of information technology and freedoms Taking into account that those responsible for data processing are public entities, under the terms of point a) of Article 37(1) of the GDPR, they have the duty

to designate an EPD or a data protection delegate, and should therefore be the reference to reference entities in terms of information technology and up-to-date freedom in accordance with the concept provided for in Article 37 of the GDPR, in the French language version ("data protection delegate").

14. It should also be noted that in point 6 of Annex 1 there is a gap in the indication of the articles of the GDPR where the rights of data subjects are foreseen and regulated, since Article 23 of the GDPR does not provide for a right. To that extent, the CNPD recommends reviewing that point 6., to refer to the rights listed in articles 15 to 22 of the RGPD.

15. The data subject to communication are referred to in Article 7 of the Convention, including identification data (single surname, married surname, surname used, if different from previous surnames, first name(s) (s), date of birth, sex, secondary country registration number (if used by country), date and place of birth, affiliation), date of death, postal address, proof-of-life situation identification code and the national identification numbers of the person concerned: Social Security number (NIR) in France and Social Security number (N1SS) in ISS,I.P., ISSM,IP-RAM and ISSA.IPRA. The data being processed are necessary and suitable for the purpose in question in compliance with the principle of data minimization provided for in Article 5(1)(c) of the GDPR.

2 See also the last part of point 6.

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

]

16. Under the terms of Article 7(2) of the Convention, the modalities of data transmission and the structure of the file to be used for exchanging the same are defined in Annex 2 — service provision contract. Here it is mentioned that this information is sent and received using the transfer of text files in a pre-defined format, encrypted with a PGP3 tool. It is further specified that the file transfer is carried out using the FTP protocol.

17. It should be noted that this protocol is not encrypted and, although the PGP mechanism is used, which provides authentication and cryptographic privacy for data communication and, as transfers are carried out via the TESTA4 private network, the risk is relatively low, the security of data transmissions can be enhanced through the use of a secure point-to-point protocol (eg sFTP/SSH). . Therefore, the CNPD recommends reconsidering the solutions found in order to strengthen the security of file transmissions.

18. Point 6.2.3 of the draft of the contract for the provision of services (Annex 2), regarding traceability rules in the management of the exchange of data in the II, I.P., provides that this body maintains a record of sending files with the respective partner institutions (issuer, entry date, date to be taken into account by the application, etc.). However, it does not define the retention period by the II, I.P., which appears to be similar to that defined for the CNAV in point 6.2.1, therefore, three years. It is therefore recommended to explicitly provide for the period of retention of the record of sending files.

19. Note that point 7.3 of Annex 2 states that «Access to this server is done by IP filtering on the private network and the connection is made through login and password». For this purpose, it is recommended to use strong credentials with long, unique, complex passwords with numbers, symbols, uppercase and lowercase letters. It is also important to define whether the Monitoring and Information Security Area (AMESI) will recover the file automatically or manually. If manually, a protocol must be established to ensure the confidentiality of the credential assigned to access the files.

20. It should be noted that the service provision contract (Annex 2) is not defined by the II, I.P., where the request files sent to the CNAV and the respective responses are stored, if they are retained in the encrypted form with the PGP tool and who will have access to the repository, both data in use and data on file, identified in the table in point 2.2.1.3 of the AIPD. Although logical access controls to data are foreseen and identified, within the scope of transfers, they are not identified

J For a simplified explanation of this concept, see https.7/en.wikipedia.org/wiki/Pettv Good Privacv 11 Cf, https://ec.europa.eu/isa2/solution.s/testa en/

controls for the data once retrieved to the destination repository in II, I.P. It is therefore recommended to introduce a new point that addresses these missing aspects.

21. Finally, it should be noted that point 11 of the service provision contract (Annex 2) describes the process of sending data in exceptional situations. One of the mentioned modalities is the use of a transfer tool provided by the CNAV DSI, using the HTTPS protocol. The CNPD reminds you that this protocol must be based on the most recent version of TLS.

III. Conclusion

22. Under the terms and on the grounds set out above, the CNPD recommends:

a) The reformulation of point 2 of Annex 1, in order to use terminology in line with that of the GDPR, in particular with regard to the concept of controller;

b) The re-weighting of point 4 of Annex 2 in order to guarantee greater security in the transfer of files;

c) The definition in point 6.2.3 of Annex 2 of the retention period by the II,I.P. the management record of data exchange with partner institutions; and

d) The introduction of an item in Annex 2 with the missing information identified above, in point 20. Lisbon, August 10, 2022

Maria Cândida Guedes Oliveira (Rapporteur)

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