CMPO

National Data Protection Commission

OPINION/2022/36

I. Order

I. The Institute of Social Security, I.P. (ISS, IP) requested the National Data Protection Commission (CNPD) to issue an opinion on a protocol that aims to establish the terms and conditions of availability, between this entity and the Work Compensation Fund (FCT), the Work Compensation Guarantee Fund (FGCT), the Institute of Informatics, IP (II.IP), the Institute for Social Security Financial Management, IP (IGFSS, IP), the Institute for the Management of Social Security Capitalization Funds , IP,(iGFCSS,IP) the ISS.IP, the Azores Social Security Institute, IP.RA, (ISSA, 1P.RA) and the Madeira Social Security Institute, IP-RAM (ISSM, IP RAM) information relating to employee identification elements, the employment contract, the employer and all the information necessary for the functioning of the Compensation Funds Portal and its respective functionalities.

2. 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 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.

II. Analysis

3. Law No. 70/2013, of August 30, establishes the legal regimes for the Work Compensation Fund (FCT), the Equivalent Mechanism (ME) and the Work Compensation Guarantee Fund (FGCT), being that paragraphs 4 and 5 of article 18 establish, respectively, that the IGFCSS and the IGFSS, ensure the functioning of the FCT and the FGCT, signing, for this purpose, protocols with the ISS, IP and with the competent social security institutions in the autonomous regions.

5. In turn, paragraph 1 of article 18 of Ordinance no. 294-A/2013, of 30 September, (defines the procedures and elements necessary for the operationalization of the Work Compensation Fund (FCT) and the Work Compensation Guarantee (FGCT)),

provides for the communication and interconnection with Social Security of the data mentioned in articles 4 and 5.

6. Article 356(1)(b) of Law No. 75-B/2020, of 31 December, provides for the establishment of data interconnection, within the scope of the Work Compensation Fund and the Guarantee Fund Compensation, and for this purpose a protocol must be signed establishing the responsibilities of each entity

Av.D. Carlos 1,134.1° 1200-651 Lisbon

I (+351) 213 928 400 F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

intervener, either in the act of transmission or in other treatments to be carried out, to be approved by the member of the Government responsible for the sectoral area and which must define, namely the categories of data subjects and data subject to interconnection, as well as their elements and conditions access, communication and processing of data by these entities, pursuant to paragraphs 2 and 3 of the aforementioned article.

7. Such interconnection is necessary to comply with the provisions of article 51 of law no. 70/2013, of August 30, as well as to comply with the measure registered in the Simplex Program 2019 -"Social Security and Funds 3 em 1“, which aims to create a single communication platform to Social Security, the Work Compensation Fund (FCT) and the Work Compensation Guarantee Fund (FGCT) of the elements relating to the conclusion, amendment and termination of employment contracts .

8. Thus, the present protocol aims to regulate the availability between the various granting entities of information regarding the worker's identification elements, the employment contract of the employer and all the information necessary for the functioning of the Compensation Funds Portal and the respective functionalities.

9. The communication of personal data constitutes a processing of personal data, within the meaning of paragraph 2) of article 4 of the RGPD.

10. There is a legitimate basis for this processing of personal data under Article 6(1)(c) of the GDPR.

11. The data subject to communication are referred to in Annex I to this protocol, which details the data to be transmitted by the Social Security to the FCT (identification elements of the worker and the employer), and the data to be transmitted by the

FCT to the Social Security (information necessary for debt delivery and collection).

12. Among the worker's identification data are those provided for in article 4 of Ordinance No. 294-A/2Q13 of 30 September (full name, NISS and civil and tax identification numbers) to which the data " email address' and 'profiles'. As for the latter, since it is not clear what type of information is included therein, it is not possible to assess their relevance and necessity, so it is recommended to reconsider their treatment, in compliance with the principle of data minimization provided for in subparagraph c) of n. Article 5(1) of the GDPR.

13. IGFSS, IP, ISS, I.P, ISSA, IP-RA and ISSM, IP-RAM, FCT and FGCT1 are considered responsible for data processing, with II, I.P. as a subcontractor. We are therefore dealing with a case of joint liability, provided for in Article 26 of the GDPR.

1 It should be noted that, certainly by mistake, recital b) of the recitals states that "ISS, I.P., ÍSSA, IP-RA and ISSM, IP-RAM intervene in this protocol because it is the public legal person that... is responsable"

14. Under the terms of clause three, II, IP, as responsible for the Social Security Information System and the Fund Support Information System, performs electronic communication of data between the systems of the granting entities through an electronic interoperability process. Access to information is carried out through electronic data communication between the systems of the granting entities, «with the use of services specifically implemented in order to protect the supply of data». However, the text does not explain how such communication is carried out, so its densification is suggested (referring, for example, to whether it takes place over an IPSec tunnel, with authentication).

15. In turn, paragraph 3 of the same Clause provides that II, I.P. shall also carry out the access logs within the scope of this protocol, keeping this log for a period of two years. It should be noted that this record must identify the date and time of access, as well as who triggered the request (in case of manual intervention). In the event of a search, the record must identify its parameters and the number of results obtained and, in the case of simple submission, the number of records transmitted.

16. It should be noted that Clause Six of the Protocol provides in paragraph g) which constitutes the processor's obligation "According to the will expressed by the Data Controllers, to return or delete all Personal Data subject to processing after

completion of the provision of services due to exhaustion of purpose , as well as all existing copies, unless their conservation is required by national/European legislation requirements.* It is recommended that this provision be deleted, which is limited to transposing Article 28(g) of the R6PD, without concretely regulate the situation under analysis.

16. Among the obligations of those responsible for data processing, point d) of Clause eight provides that they are responsible for guaranteeing, together with the Processor, the exercise, by the Data Subjects, of the rights of information, access, rectification , erasure, opposition and limitation of treatment, without, however, defining the procedure to be adopted in case the holders exercise their rights. Therefore, it is suggested that this clause be reformulated in order to regulate the procedures in question.

17. Finally, the CNPD recommends the densification of Clause 9 regarding security and privacy measures, defining the existence of a profile to access data (and a limit on the number of users with that profile); the existence of logs of requests and access to data with identification of who triggered these procedures as described in point 15 and, also, the use of secure channels for data transmission. As a note, it should also be noted that the text of the Protocol does not specify the support for the information to be transmitted.

III. Conclusion

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

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

a) The re-weighting of the worker's identification data contained in Annex I;

b) The reformulation of the third clause in order to explain the way in which the communication between the systems of the granting entities is carried out;

c) The reformulation of paragraph 3 of Clause 3, concerning access records, in the terms described in point 15;

d) The elimination of Clause Six of the Protocol;

e) The introduction of a new paragraph in Clause eight regulating the procedure to be adopted in relation to the exercise of the

rights of data subjects;

f) The densification of Clause 9 regarding security measures, the clause having to expressly provide for the existence of a profile to access the data, the existence of logs of requests and accesses with identification of who triggered these procedures, the use of secure channels for the transmission of data as well as the explanation of the support of the information to be transmitted.

Lisbon, April 28, 2022

Maria Cândida Guedes Oliveira (Rapporteur)