

## I. Order

1. The Social Security Institute, I.P., submitted to the National Data Protection Commission (hereinafter CNPD), for an opinion, the Collaboration Protocol for access to information regarding the contributory situation in Social Security within the scope of the State Suppliers Portal. The grantors of this Protocol are the Institute of Public Markets, Real Estate and Construction, I.P., (IMPIC), the Agency for Administrative Modernization, I.P., (AMA), the Institute of Social Security, I.P., (ISS) and the Institute of Informatics, I.P., (II, I.P.).

2. The application is accompanied by the Impact Assessment on Data Protection (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 Article 58(3)(b) and Article 36(4), all of Regulation (EU) 2016/679, of 27 April 2016 - General Protection Regulation (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 enforces the GDPR in the domestic legal order.

## II. Analysis

4. Decree-Law No. 72/2018, of 12 September, created the State Suppliers Portal (Portal), which aims, through the use of digital means, to simplify and streamline the procedures for verifying and proving the inexistence of impediments to public procurement provided for in the Public Contracts Code (CPP), approved by Decree-Law no. of Social Security for the purposes of payments in the contractual execution phase, pursuant to paragraph 2 of article 1 of Decree-Law No. 72/2018, of 12 September.

5. The Portal aggregates information about the supplier, with the express consent of the same, namely with regard to information about their contributory status with Social Security, under the terms of subparagraph b) of paragraph 3 of article 1, of the Decree-Law No. 72/2008, of September 12.

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PAR/2021/128

6. The CNPD has already commented on the Draft Decree-Law that created the State Suppliers Portal and established the respective legal regime, in Opinion No. 30/2018 of 2 July 2018<sup>1</sup>.

7. Pursuant to article 16 of Decree-Law No. 72/2018, of 12 September, IMPIC must establish the conditions and specifications of the data and information to be transmitted to the Portal, through protocols to be signed with public entities holders of the data, with the management companies of electronic public procurement platforms and with the management entities of other platforms of the State that intend to establish an interconnection with the Portal.

8. The Protocol under analysis aims to establish the terms and conditions for the availability of information regarding the contributory situation of economic agents, as State suppliers, by means of express consent, on the National Portal of State Suppliers, under the terms and for the purposes set out in Decree-Law No. 72/2018, of September 12.

9. Thus, in accordance with paragraph 2 of Clause 2.a, the Protocol defines the conditions of access to the Interoperability Platform by IMPIC for the provision of information through the National Portal of State Suppliers.

10. Paragraph 3 of Clause 2.a of the Protocol establishes that «access to information is carried out in real time, through electronic data communication between systems of the grantors, with the use of "webservices" specifically implemented in order to protect the supply of data.» Therefore, it is recommended that all communications be encrypted, using the HTTPS protocol, using Transport Layer Security (TLS), in its most recent version.

11. In turn, paragraph 5 of Clause 2.a of the Protocol refers to accreditation in the respective systems, namely the assignment of an application user and a password. Note that the IAPD identifies, in point 2.3.2, the risk of sharing credentials or abuse of privileges.

12. It is noted, however, that both the Protocol and the AIPD are silent on the existence of a credential management policy and maintenance of an updated list of users, by each of the grantors in the respective systems. Therefore, the CNPD recommends

the introduction of an item that defines the allocation of access credentials in a controlled manner through a formal process of

1 Available at <https://www.cnDd.nt/decisoes/historico-de-decisoes/?vear=2Q18&tvoe=4&ent=>

PAR/2021/128

two

National Data Protection Commission

management of the respective life cycle, as well as the review of user access rights at regular intervals.

13. It should be noted that paragraph 6 of Clause 2.a provides that 'the communication of information is carried out through a dedicated circuit between IMPIC and AMA and, between the latter entity and II, IP'. From reading the initial table of point "2.3.1 Assessment of security controls" of the IAPD, network security appears as an acceptable risk. However, the IAPD only concerns communications to/from the II.I.P. not referring to communications made between AMA and IMPIC. The CNPD recommends that the Protocol include how the secure communication that supports the Web Services is carried out, specifically aspects such as the configuration of a VPN, secure data encryption and communication protocols.

14. According to paragraph 8 of Clause 2.a «Access to data by public contracting entities or contracting entities requires their prior authentication in the National Portal of State Suppliers, under the responsibility of IMPIC, I.P., and must be The Citizen's Card (CC) or the Mobile Digital Key (CMD) is used for this purpose'. Note that the same is reiterated in point i) of Clause 6.a. However, paragraph a) of paragraph 3 of article 5 of Decree-Law no. 72/2018, of 12 September, provides that the authentication and identity verification mechanism for access to the Portal is, for contracting authorities, the authentication system of the BASE Portal. Thus, it is observed that the Protocol does not comply with the provisions of Decree-Law no.

15.14. In turn, the Protocol provides that ISS, I.P., and IMPIC are considered responsible for the processing of personal data, with II, I.P., and AMA being subcontractors (see Clause 8.a).

15. From the analysis of the Protocol, it appears that we are dealing with 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. of the data. The CNPD therefore suggests that the content of the Clause 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.

17. As for Clause 11,a, on subcontracting, it states that "Subcontractors may, whenever they deem it necessary, subcontract

any entity for the pursuit of processing-related activities". 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 to the

Av. D. Carlos 1,134.1º

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpcl.pt

www.cnpd.pt

PAR/2021/128

2v,

increase in the number or replacement of other processors, thus giving the controller the opportunity to object to such changes".

18. It is understood, therefore, that the wording of Clause 11.a 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, as since the subcontractor can only carry out further subcontracting if these subcontractors present "sufficient guarantees of carrying out appropriate technical and organizational measures...", and the open provision of subcontracting by any entity cannot be accepted.

19. Therefore, it is recommended that Clause 11,a be corrected and that references to subcontractors' obligations set out in Article 28(2) and 4 of the GDPR be inserted therein.

20. Clause 12.a provides, in subparagraph b) of paragraph 1, that subcontractors are responsible for informing those responsible for processing any corrections or situations of erasure of personal data that occur as a result of a request from the data subjects. Here too, Articles 16 and 17 of the GDPR grant the data subject the right to obtain from the data controller the rectification and erasure of their personal data, so this provision must be revised, in order not to distort the obligation that on those responsible for the treatment falls to guarantee the rights of the holders.

21. Also with regard to Clause 12.a, subparagraph c) provides that it is incumbent upon the II, I.P., to ensure that there is a legitimate basis for the processing of personal data under the terms of article 6 or article 9 of the GDPR. However, the

competence to verify the conditions of legitimacy of the treatment rests with those responsible for the treatment, so the attribution to the processor of the task of verifying the existence of valid consent of the State suppliers for each consultation carried out may distort the legal imputation of responsibility for any non-compliance of such an obligation. Therefore, the CNPD recommends amending the text of Clause 12.a, so as not to contradict the provisions of Article 5(2) of the GDPR.

22. Finally, a note regarding the IAPD sent: point 1.2 mentions that, among other elements, the methodology is based on the Guidelines of the Working Group of article 29 (WP29-Guidelines)<sup>2</sup>. However, when comparing the IAPD with Annex 2 of the document with the aforementioned Guidelines, which contains the criteria for an acceptable IAPD, one of the elements listed is missing, specifically "the assets on which personal data depend (equipment computer, computer program, networks, people, paper or paper transmission channels) are identified;".

<sup>2</sup> (WP29-Guidelines) ARTICLE29 - Item (europa.eu)

PAR/2021/128

3

W

CNPD

National Data Protection Commission

### III. Conclusion

23. With the changes identified above, the introduction of which the CNPD recommends, it is understood that there are no impediments to the conclusion of the Collaboration Protocol for access to information regarding the contributory situation in Social Security within the scope of the State Suppliers Portal.

24. In particular, the need for revision is highlighted:

- i. Clause 6.a and no. 8 of Clause 2.a, for manifest violation of Decree-Law no. 72/2018;
- ii. Of Clauses 8.a, 11.a and 12.a, under penalty of non-compliance with the delimitation of responsibility for the treatment and imputation of obligations established in the RGPD.

Approved at the meeting of December 21, 2021

Filipa Calvão (President)

Av. D. Carlos 1,134.1º

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

[geral@cnpd.pt](mailto:geral@cnpd.pt)

[www.cnpd.pt](http://www.cnpd.pt)