/ NATIONAL DATA PROTECTION COMMISSION

OPINION/2020/37

I. Order

0 Social Security Institute, I.P. (ISS), submitted to the National Data Protection Commission (hereinafter CNPD), for an opinion, the Protocol to be granted with Instituto de Informática, I.P., and Caixa Geral de Aposentações, I.P. (CGA), governing "the terms under which cooperation, coordination, exchange of information and procedures between the services of the CGA and the signatory social security institutions take place",

The CNPD issues an opinion within the scope of its powers 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) Article 58(3) and Article 36(4), all of Regulation (EU) 2016/679, of 27 April 2016 - General Data 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 (hereinafter, Law of Enforcement) in the domestic legal order.

For this purpose, it is important to bear in mind the purposes of the Protocol, highlighting, in particular, "the fair, quick and effective implementation of social security benefits", the simplification of "the relationship of citizens with the Administration", and the objective of " ensure the control of contributory obligations, guarantee the rigorous attribution of social benefits, as well as promote effectiveness in preventing and combating fraud and contributory evasion".

In order to comply with the provisions of the Protocol, the ISS and the CGA agree to provide their information systems with the necessary functionalities for sharing personal data contained in two structured lists that make up Annexes I and II of the aforementioned Protocol. The Instituto de Informática is technically responsible for the information systems of the ISS and for the communication infrastructure to support those systems, and which “ensures the construction, management and operation of application systems and technological infrastructures in the areas of information and communication technologies”. From

services and bodies under the Ministry of Labour, Solidarity and Social Security', it is as a subcontractor of the ISS that it is a signatory to this protocol.

The sharing of data between the two information systems takes place as follows:

• For the consultation of individualized data in singular situations, the CGA will provide access to its Internet portal to selected and duly authorized ISS users.

• For the remaining data queries between the CGA and ISS information systems, web services1 will be implemented.

II. appreciation

The Protocol in question clarifies, in clause 6, the capacity in which the ISS, the CGA and the Instituto de Informática intervene in it - respectively, responsible for the processing (cf. paragraphs 2) and 7) of article 4 of the GDPR) and subcontractor (cf. Article 4(8) of the GDPR).

Having analyzed the data subject to processing listed in the annex to the Protocol, it is understood that data relating to the health of natural persons are also at stake, so the processing focuses on sensitive data specially protected under the terms of paragraph 1 of article 9. of the GDPR. In fact, in Annex I of the Protocol, it is established that the “List of data to be transmitted by the CGA” includes the “name of the benefit (retirement pension, old age; disability; death; blood price; survival, lifetime monthly allowance, disability allowance, etc--)" and the "type of disability of the subscriberf.

Bearing this in mind and considering that the processing is carried out on a large scale, it can only be concluded, in accordance with Article 35(3)(b) of the GDPR, that the present processing has to be preceded by a data protection impact assessment. This assessment may still be mandatory if it is verified, which was not

Services available via the web.

It is possible to assess, by analyzing the Protocol, the assumptions provided for in subparagraph a) of paragraph 3 of article 35

of the GDPR, as better explained below, in point 4.

This assessment is particularly relevant to assess the risk to the rights of data subjects and to determine the measures to mitigate that risk, in particular, adequate security measures. However, the request does not mention that the necessary impact assessment has been carried out, nor, strictly speaking, do the conclusions of that assessment and the measures that had been defined in that case reflect in the clauses of the Protocol.

The CNPD therefore recommends that this assessment be carried out and that the text of the Protocol be strengthened with the provision of adequate conditions and rules to protect rights and interests in crisis.

In particular, the CNPD then highlights some aspects that are missing from the provisions of the Protocol or that raise doubts as to the adequacy of the solutions outlined therein. 1

1. First of all, it should be noted that in subparagraph a) of paragraph 1 of clause 5.3, it is stated that access to the data stored in the CGA information systems can be carried out by duly selected and authorized ISS employees, through the "consultation of the personal data on the CGA website, electronically and in real time. The Protocol refers, in the same clause and in the same number, to annexes I and II, where the categories of personal data communicated between the two entities are identified.

However, from reading the Protocol it is not clear whether these data refer to the consultation of personal data on the CGA website on the internet.; or to the data transmitted by invocations to the web services, or even to both cases.

In fact, the Protocol is not explicit in relation to the sets of personal data that are made accessible to the ISS employee, nor does it mention the limitations on the set of subscribers or beneficiaries of CGA pensions or benefits, whose information can be consulted through the aforementioned portal.

It is therefore also important, as part of the principle of transparency set out in point a) of paragraph 1 of article 5 of the GDPR,

to define precisely the terms in which the processing of data takes place, in this case, access personal data by employees of a public entity other than the one that holds them.

2. Secondly, with regard to clause 5.a, paragraph 2 states that “the ISS communicates to the CGA the identification of the persons authorized to access the database, with a view to assigning the name and the respective passwords". At this point, the Protocol does not make explicit the criteria used in the selection of these employees, nor the universe of ISS employees to be accredited for accessing the CGA portal on the internet.

The CGA and ISS information systems integrate and process a wide range of personal data, some of which correspond to the special categories of data provided for in Article 9(1) of the GDPR (e.g., relating to health), at that adequate technical and organizational measures must be foreseen and applied to guarantee compliance with the principles of integrity and confidentiality, enshrined in Article 5(1)(f) of the GDPR, and as a way of guaranteeing the auditability of the system and data processing operations. .

3. Also with regard to clause 5.a, more specifically in paragraph 5, it is established that "electronic data communication between systems can be carried out through a VPN circuit between the H and the CGA".

It turns out that the Protocol does not expressly determine that the communication of personal data between the ISS and CGA must always be carried out through secure channels. This omission seems incomprehensible, given the principles of integrity and confidentiality, already invoked here, and from which the controller is obliged to adopt the appropriate technical or organizational measures to guarantee the security of the treatment, namely the confidentiality of the data. .

4. It is also important to point out that the Protocol does not make reference to the way in which the information of a specific subscriber or beneficiary of CGA pensions or benefits, or of an ISS beneficiary becomes eligible for sharing between the entities in

cause. Moreover, it does not follow from the Protocol whether the selection is case-by-case, manual and subject to the discretion of the employees of the signatory parties, or whether it results in the systematic and automated application of an algorithm in the databases. And this is an aspect of the treatment that should be explained and regulated in the Protocol, also because the risks and risk-mitigating measures are of different nature in one case and another.

In the first case, the selection must be accompanied by rigorous access audit records and the definition of an alarm policy, as generally follows from the principles of integrity and confidentiality, and specifically from subparagraph d) of paragraph 1 of article 32. ° of the GDPR. In the second case, the selection, as the result of a systematic and automated procedure, implies carrying out an impact assessment on data protection, as follows from Article 35(3)(a) of the GDPR, which should have accompanied the present request for an opinion - if it had been prepared, a fact that the CNPD is not aware of.

5. Finally, it is important to comply with the rules for the conservation of personal data. In paragraph 7 of clause 5.a, it is agreed that "the data transmitted under the Protocol are kept for the period strictly necessary to fulfill the purposes foreseen, without prejudice to the established legal deadlines".

It so happens that the Protocol does not define a specific time interval, nor any criteria underlying the time delimitation of data retention.

Given that the nature of the processing of personal data carried out by the ISS and the CGA presupposes the monitoring of cases that can be extended over time, the deadline for the erasure of the data, or for the periodic review of the same, should be specified, ensuring so that information systems do not retain data for a period longer than that justified by the purposes pursued, as required by Article 5(1)(e) of the GDPR.

In addition, there are also no rules on updating the stored data, which were obtained by invoking the web services, an obligation that stems from the principle of accuracy set out in Article 5(1)(d) of the GDPR.

III. Conclusion

Considering the universe of data subjects covered by the processing of data object of the Protocol, as well as the sensitive or special nature of some of the categories of personal data shared between public entities, the CNPD underlines that this Protocol should have been preceded by the evaluation of impact on data protection, under the terms set out in point b) and perhaps in point a) of paragraph 3 of article 35 of the GDPR, a fact that is not mentioned in the request submitted, nor is it reflected in the provisions of the Protocol .

The CNPD therefore recommends that this assessment be carried out and that the text of the Protocol be strengthened with the provision of adequate conditions and rules to protect rights and interests in crisis.

In particular, and on the grounds set out above, the CNPD recommends:

1. Clarification, in clause 5.a, no. 1, point a), of the Protocol, of the terms and scope of access to personal data held by the CGA by ISS employees, in compliance with the principle of transparency of data processing ;

2. The specification of the criteria underlying the access profiles to the CGA portal on the Internet, in terms that allow checking compliance with the principles of integrity and confidentiality of the treatment, as well as guaranteeing the auditability of access;

3. The introduction in the text of the Protocol of a provision that imposes or foresees the adoption of adequate security measures to guarantee confidentiality in the transmission of data between the ISS information systems and the CGA, in accordance with the principles of integrity and confidentiality ;

4. The specification of the form or procedure that makes it possible to identify the subscribers or beneficiaries of CGA pensions or benefits or the ISS beneficiaries who are eligible for the sharing of the respective data between the entities in question, providing for the appropriate measures to guarantee the auditability and the

mitigation of risks to the rights of holders, especially if this results from the systematic and automated application of an algorithm in the databases;

5. The introduction in the Protocol of provisions to foresee the maximum periods for the conservation of personal data, as well as rules on the updating of data, in compliance with the principles of limitation of retention and accuracy.

Lisbon, March 30, 2020

Filipa Calvão (President, who reported)

Av. D. CARLOS I, 134 - Io I 1200-651 LISBON I WWW.CNPD.pt I TEL: +351 213 928 400 | FAX: +351 213 976 832