Clk ■ IP%i li%

i)

National Data Protection Commission

OPINION/2021/120

I. Order

1. Caixa Geral de Aposentações asked the National Data Protection Commission (CNPD) to issue an opinion on the draft Protocol on the automated processing of personal data within the scope of the Information System of the Ministry of Education and the Information System Caixa Geral de Aposentações, to be concluded between Caixa Geral de Aposentações (CGA), the Directorate-General for Education and Science Statistics (DGEEC) and the Agency for Administrative Modernity (AMA), as well as the corresponding Impact Study.

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.

II. Analysis

i. Object and processing operations

3. The Protocol under analysis aims to regulate the procedures relating to the exchange of information between the DGCEE and the CGA, regarding "the proof of school status in an educational establishment, for the purposes of recognition and maintenance of the right for the purpose of attributing family benefits and of survivors' pensions and blood price by the CGA".

4. This information exchange is carried out through the Public Administration Interoperability Platform (iAP), managed by AMA.

5. In order to fulfill the purposes of the Protocol, DGEE transmits the following student data to the CGA: NISS PS Holder / Student; Academic year of the School Test / Enrollment; Year of Enrollment (test); Level of Teaching of the School Test /

Enrollment; school performance of the previous academic year; enrollment status; date of the Registration Status, data that, given the intended purposes, seem adequate and not excessive.

6. Since paragraph 3 of Clause Two refers to these data as the "possible responses of the DGEEC", it follows that such information is provided at the request of the CGA.

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

gerai@cnpd.pt

www.cnpd.pt

7. It follows from Clauses Two1 and Three that "CGA, through AMA, I.P. does not provide the DGEEC with any additional information to what it already holds in its information systems, in addition to the control messages and information request from the holder of data, provided for in the communications protocol, so that the CGA obtains the data it needs".

8. This wording needs clarification. Let's see: it is said that, through the AMA, no information will be transmitted by the CGA to the DGEEC beyond what this entity already has. However, it is not clear whether it was intended to exclude the transmission of any other information from the CGA to the DGEEC, whatever the route, or whether there will be the transmission of other information, but not through this route. In that case, it would be necessary to indicate which information is in question. In addition, a "communications protocol" is mentioned, where the information to be transmitted will be provided, which was not attached to the request for an opinion, which prevents the CNPD from commenting on all relevant aspects.

ii. Joint responsibility and rights of data subjects

9. Pursuant to article 2 of Regulatory Decree No. 13/2012, of 20 January, in its current wording, the DGEEC is responsible for creating and ensuring the proper functioning of the Integrated Information System for Education and Science, as well as to globally observe and evaluate the results obtained by the educational and technological systems, in conjunction with other Education and Science services. To this end, it pursues, namely, the following attributions: ensuring the collection, monitoring,

processing, production and dissemination of adequate information, within the framework of the National Statistical System; manage the integrated information and management system for the educational and training offer; design and implement computer applications for managing the information system, namely those that ensure data consistency and certify school applications and, in particular for what is currently important, the MISI system, Escola 360 and the Enrollment Portal, through from which information relevant to the implementation of this Protocol is collected and processed.

10. For its part, CGA is a Public Institute whose mission is "to manage the public social security system in terms of pensions and retirement, retirement, survival and other special nature" (Article 3(1)) . of Decree-Law No. 131/2012, of 25 June).

11. In turn, AMA is the Public Institute responsible for ensuring the operation of the IAP which, pursuant to Article 6(2) of Decree-Law No. 73/2014, 13 of May, constitutes as the preferred means of communication between Public Administration services and bodies.

1 Number 1 of Clause Two refers to 'the situation defined in paragraph a) of Clause One', which, however, does not exist.

12. Under the terms of Clause Six, the CGA and the DGEEC are assumed to be "jointly responsible under Article 26 of the GDPR", with the third party, AMA, being the subcontractor.

13. With regard to data protection, it should be noted that the heading of Clause Five is misleading. In fact, under the heading Rights of Data Subjects, the exercise of any rights is not regulated, rather the agreement of the Parties is established to "communicate expeditiously, namely by e-mail", the requests of data subjects who wish to exercise their rights. So, what it really is about is establishing a duty of collaboration between those responsible for the treatment and the WADA.

14. With regard to the specific obligations of the grantors regarding the processing of data and, more precisely, regarding the safeguarding of the rights of the holders, Clause Ten 2 governs.

15. Thus, in paragraph 1, it is stated that AMA is responsible for collaborating with those responsible in guaranteeing the exercise of the rights of the data subjects, informing those responsible for processing any corrections or situations of erasure of personal data requested by the data subject and ensuring that there is a legal basis for carrying out the processing of data.

16. In turn, number 2 identifies the responsibilities of controllers. Thus, two e-mail addresses are indicated, one from the

DGEEC and the other from the CGA through which the holders or their guardians can request clarification depending on the type of information they want. Thus, through the address dpo@daeec.mec.pt, data subjects can request "clarifications on privacy issues of data processing systems". The address epd@cga.pt will be used to request "clarifications on privacy issues of the data processing systems", however, under the terms of the same clause, any of the grantors may receive such requests.

17. It is not understood, however, the reason why it is established in subparagraph h) of number 2 that the request for rectification of data has to be made in writing to the Directorate-General for Education and Science or the Caixa Geral de Aposentações - according to the respective competences -, without specifying that electronic mail can be the means to be used for this purpose, allowing the interpretation that it cannot be carried out, also, through such means.

18. Nothing is said about the exercise of the right to erase data, information that must be made available to the data subject.

2 It is believed that there is a lapse in the heading Right of Access Guardianship of the Rights of Holders of Personal Data, and the first part should be deleted since the category holders' rights necessarily encompasses the right of access.

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

gerai@cnpd.pt

www.cnpd.pt

19. In the event of suspension or termination of the Protocol, this implies, pursuant to the provisions of Clause Thirteen, the immediate cessation of authorization to access personal data.

20. The duty of confidentiality is established for the duration of the Protocol and even after its termination.

iii. data processing

21. The "form, extent and limits of data interconnection between the various services and bodies of the Public Administration" necessary for the fulfillment of its mission are provided for in Decree-Law No. 309/2007, of 7 September, which, in use of a legislative authorization, in article 2 it lists the databases which contain the data to be related in order for the CGA to fulfill its

mission.

22. It should be noted that the databases mentioned in Clause Two as those that will provide data under this Protocol - Enrollment Portal, Escola 360 and MISI (Coordinating Office of the Information System of the Ministry of Education) -, only the third appears in the list of the decree-law (item j). In fact, this paragraph establishes access by the CGA only to data relating to enrollment, attendance and school performance contained in the MISI database.

23. Thus, as for the others, there is no provision for data processing, so if there is a legal basis for the collection and processing of data under the terms of the respective regime, it does not seem to exist for transmission to the CGA.

24. Article 4(4) of the aforementioned decree-law establishes that "[t]he access by the CGA to data on the school situation of students contained in the MISI databases has the exclusive purpose of allowing the weighing of information relevant to the specific decisions for the attribution of social benefits and the prevention and fight against fraud and contributory evasion, namely for the purposes of attributing family benefits and survivors' pensions and blood price". Hence the exclusive reference also to the same database, excluding the others.

25. The categories of data subject to interconnection are, in the terms of subparagraph g) of paragraph 1 of article 3, the "students' school situation, in terms of attendance and performance, and the content of the registration of non- legalized public, from the MISI databases.

26. Therefore, in the case of a new processing carried out from the Escola 360 and Portal das Matriculas databases, a legal basis must be found for this transfer.

27. However, the hypothesis of an updated interpretation of the conditions defined in the aforementioned legal diploma is not excluded, if the other databases or information systems indicated in this protocol have been created after the entry into force of this legal diploma, which allows the extension of the formula «Enrollment, attendance and performance in schools and in legalized non-public educational establishments, based in the Information System Coordinating Office of the Ministry of Education (MISI), to other information systems that contain the relevant and necessary personal data for the legally delimited

purpose.

28. In any case, since the information transmitted by the DGEEC to the CGA is already available in the Portal das Matriculas, Escola 360 and MISI systems, with the legal basis of this collection being ensured, it will now be necessary to guarantee the information to the holders or their representatives in relation to this new treatment.

iv. Conditions of access to information and Security and Privacy Guarantees

29. Clause Four explains that data sharing is carried out using WebServices capable of guaranteeing data protection and carried out through a dedicated circuit between the entities.

30. As conditions for access to information, prior authentication mechanisms are foreseen before the granting entities. Furthermore, the accreditation of users is carried out by assigning an application user and a password. A nominative list of employees authorized to access personal data will be drawn up in accordance with their function.

31. All consultations carried out are subject to records kept for a period of two years for audit purposes.

32. As for Security measures, Clause Eleven provides that the data communicated under the Protocol may only be used for the purposes provided for therein, being kept for the period strictly necessary to pursue the purpose provided for in this Protocol, which is not indicated.

33. It is generally determined that "organizational and technological security standards must be adopted that guarantee the protection of confidentiality and data integrity.

34. As an example of the technical measures to be adopted, the following are particularly relevant:

The. regarding the means of communication between the entities - protection of communication by Virtual Private NetWork (VPN) and data encryption through the TLS v1.2 security protocol.

3v.

B. as for access control - nominal access control both in access to the corporate network of the grantors and to the content of the database with the content of the WebService, as well as access restrictions by functional competence.

35. The Impact Assessment on Data Protection prepared and which was also submitted to the CNPD for consideration, considered that the level of risk for the holders' personal data is low, provided that the security and mitigation measures provided are complied with.

36. In fact, in general terms, the Draft Protocol enshrines good practices in the implementation of information sharing systems. The use of a cryptographic protocol protects information in transit between entities and the authentication mechanism and respective nominal credentials strengthen the system, promoting the ability to mitigate security incidents.

37. The necessary monitoring is guaranteed, through the establishment of access restrictions by functional competence and a system of event records, strengthened by a policy of conservation of these records for an acceptable period of 2 years.

38. However, it cannot be overstated to recommend that the personal and non-transferable nature of the access credentials to be granted to users indicated by the grantors be emphasized, as well as the strengthening of policies for the management of access privileges to personal data, in order to ensure that the information transmitted between the grantors is framed in the protocol to be signed.

39. Furthermore, it is recommended that the events of access to information to be recorded be carefully defined, in order to guarantee a more effective prevention of incidents, as well as the mitigation of their effects, if they occur.

40. Likewise, it is suggested to carry out training actions in order to train the interlocutors indicated by the grantors to operate the planned sharing mechanisms, in accordance with the Protocol and other existing internal policies and procedures, as well as raising awareness for the most common errors and potentially liable to lead to personal data breaches.

41. On the other hand, it would be desirable to implement audit procedures with the objective of reviewing, confirming and maintaining compliance with the policies and procedures established in the light of the Protocol and the regular review of information security measures and policies, in order to print improvements whenever necessary.

III. Conclusion

42. On the grounds set out above, the CNPD believes that the existence of a legal basis for the transfer of data from the Escola 360 platform and the Enrollment Platform to aCGA should be verified.

43. Safeguarding this issue, the CNPD considers that, in general, the Protocol enshrines adequate system security and risk mitigation measures and recommends that the measures referred to in points 38 to 41 be considered.

Lisbon, September 10, 2021

Ana PauTa~ , v tora)

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpcl.pt

www.cnpd.pt