National Data Protection Commission

OPINION/2022/46

I. Order

1. The Directorate-General for Education and Science Statistics (DGEEC), submitted to the National Data Protection Commission (hereinafter CNPD), for an opinion, the Collaboration Protocol for access to information on the contributory situation of citizens to social security for verification and proof of the absence of debts, for the processing and payment of the "Qualifica Incentive". The grantors of this Protocol are DGEEC, the National Agency for Qualification and Vocational Education, I.P., (ANQEP, I.P.), the Agency for Administrative Modernization, I.P., (AMA), the Social Security Institute, I.P., (ISS) and the Instituto de Informática, I.P., (II, I.P.).

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

3. 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.

4. Decree-Law No. 29-B/202, of 4 May, establishes the governance model for European funds allocated to Portugal! through the Recovery and Resilience Plan, in which the Accelerador Qualifica sub-investment is inscribed, with ANQEP, I.P. the entity designated for its execution.

5. The Accelador Qualifica determines the attribution of a pecuniary incentive to the trainees who complete a school qualification of level 3 or level 4 of the National Qualifications Framework (QNQ), or being holders of the 12th year, the conclusion of a professional qualification of level 4 of the NQF (see article 17 of Ordinance No. 61/2022, of 31 January).

6. In order to fulfill the granting of the monetary incentive within the scope of the "Qualifica Accelerator", it is necessary that the DGEEC, through the SIGO system, confirms that the beneficiary of this incentive has its tax and contributory situation regularized.

7. Access to this SIGO platform, which is freely accessible on the public Internet, through the URL:

https://www.siao.pt/Login.isp. allows you to verify that the authentication mechanism presented is of

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

username and password and allows multiple attempts. In order to avoid brute-force attacks and prevent system intrusion, complementary protection mechanisms should be considered (e.g., two-factor authentication (as mentioned in the EPD alerts in the AIPD document) or a CAPTCHA test).

8. Paragraph 1 of Clause 2.a of the Protocol establishes that "the consultation of personal data is carried out in real time, through electronic communication of data between systems of the grantors, using "webservices" specifically implemented in a to protect the provision 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.

9. In turn, number 3 of clause 2.a of the Protocol refers to accreditation in the respective systems, namely the assignment of an application user and a password. The AIPD identifies, in the EPD alerts, that «in the case of user authentication, the 2FA mechanism should be implemented as soon as possible, for access to data of a set of students, including authentication in a nominal way by them in order to be able to know who used/accessed the personal data». This alert reveals that SIGO does not identify users by name and that credentials may be shared. It also appears that there will be no auditing mechanisms to identify who accessed what data in the system during use.

10. It is noted 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 their 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 managing the respective life cycle, as well as the review of user access rights at regular intervals.

11. It should be noted that paragraph 4 of Clause 2.a provides that the consultation of personal data is carried out through a dedicated circuit between DGEEC and AMA, I.P., and between the latter entity and II, IP. 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.

12. Under the terms of Clause 7.3, DGEEC is solely responsible for obtaining prior consent from data subjects for accessing and transmitting the data being processed. The consent of the beneficiaries is provided for through a declaration of authorization for consultation, under the terms set out in article 4 of Decree-Law no. 114/2007, of 19 April. The declaration of authorization for consultation is expressly provided for in the Term of Acceptance, which is annexed to the Guidance

Technique developed by ANQEP, I.P. and refers to the authorization of the electronic transmission of allusive data that allows the DGEEC to assess the situation of non-debt with the Tax and Social Security Authority.

13. In turn, the Protocol provides that ISS, I.P., DGEEC and ANQEP, I.P. are considered responsible for the processing of personal data, with II, I.P., and AMA, I.P. (cf. Clause 8.a).

14. 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.

15. As for Clause 11.a, on subcontracting, it states that "It is considered delegated to the subcontractor and the choice of further subcontractors, without prejudice to the availability of an updated list with their identification, accompanied by the applicable contractual conditions and the right to opposition". 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 in terms of increasing the number or replacement of other processors, thus giving the controller the opportunity to object to such changes".

16. 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, a since the subcontractor can only carry out further subcontracting if these subcontractors present 'sufficient guarantees that appropriate technical and organizational measures are carried out...'. It is also suggested to replace the reference to the right of opposition by the possibility of opposing, since that expression has its own meaning in the GDPR, corresponding to a right of data subjects under the terms of its article 21.

17. Therefore, it is recommended to correct Clause 11.a and insert concrete references to the obligations of subcontractors set out in paragraphs 2 and 4 of article 28 of the GDPR.

18. 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 submitted before those responsible. However, Articles 16 and 17 of the GDPR grant the data subject the right to obtain from the controller the

Av. D. Carlos 1,134,1o 1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

rectification and erasure of your personal data, with the processor providing assistance to the controller to allow the controller to fulfill its obligation to respond to requests from data subjects. This follows from subparagraph e) of paragraph 3 of article 28 of the RGPD and is contained in subparagraph a) of paragraph 1 of Clause 12 of the Protocol, so that this subparagraph cannot be made autonomous.

19. Finally, a reference to the 10-year period for data retention provided for in clause 14 of the Protocol. The IAPD does not present any justification for this period, so the CNPD is not in a position to comment on compliance with the principle of limitation of conservation provided for in subparagraph e) of paragraph 1 of article 5 of the GDPR

III. Conclusion

20. On the grounds set out above, the CNPD points out the need to consider complementary mechanisms to protect access to the SIGO, as well as the amendment of the aforementioned provisions.

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

i. Clause 8.a in order to contain an express reference to the existence of an agreement between the two controllers that delimits their respective responsibilities for compliance with the GDPR;

ii. From clause 11.a in order to insert concrete references to the obligations of subcontractors set out in paragraphs 2 and 4 of article 28 of the GDPR.

Lisbon, May 31, 2022

\

^ ^ "V... ^

Maria Cândida Guedes de Oliveira (Rapporteur)