D

National Data Protection Commission

OPINION/2021/24

I. Request

1. The Directorate-General for Education and Science Statistics (DGEEC) 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 data transfer for the purposes of of TRANSPORT PASSES through the Enrollment Portal of the Ministry of Education.

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.

The Protocol under analysis aims to regulate the transfer of data from the Enrollment Portal of the Ministry of Education to TIP - Transportes Intermodais do Porto, ACE, for the purpose of issuing public transport passes to all students who meet the age conditions and belong to municipalities covered by the Porto Metropolitan Area.

3. The General Directorate of School Establishments (DGEstE) is also granted in the Protocol as the entity responsible for verifying the placement of students in the respective schools and groups through the Enrollment Portal.

4. The data to be transferred are communicated through the Enrollment Portal Platform, managed by DGEEC, through a protocol via WebServices.

5. The legal condition for this treatment will be based on the consent of the parents or students when they are of age, which will be collected by DGEEC.

6. Several security measures are indicated with a view to the effective protection of personal data.

7. The period for keeping consent records is 60 days after completion of the purpose. The audit logs, with the records of

consultations via the web service, will be kept for a period of 24 months, as stated in paragraph 8 of clause three.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

8. A Data Protection Impact Assessment (AIPD) was carried out, which accompanies the request for an Opinion. The AIPD describes the purposes and conditions of data processing, as well as the categories of data involved. Several preventive mechanisms are presented that will be applied to the treatment and that involve the pseudonymization of data, encryption and monitoring of accesses.

9. The assessment of the CNPD is limited to the rules that provide for or regulate the processing of personal data.

II. Analysis

10. The protocol in question aims to define the terms of the collaboration between DGEEC, DGEstE and TIS, with a view to producing Andante cards and issuing public transport passes to all children and young people attending compulsory schooling who meet the age conditions and belong to municipalities covered by the Porto Metropolitan Area. For this purpose, it is necessary to transfer personal data from the enrollment portal to the TIP, and the communication of data constitutes a processing of personal data, within the meaning of Article 4(2) of the GDPR. i.

i. Conditions of access to information - Third clause

11. With regard to the conditions of access, the third clause provides that the same is carried out in real time, through electronic data communication between systems of the granting entities, with the use of webServices, specifically implemented in order to protect the supply of Dice. The following data are transferred: name, type of identification document, expiry date of the identification document, date of birth, student's photograph, address, postal code, locality, county, district, level of education, organic unit code, grouping name, school code, school name, school social action level (if beneficiary), indicator if

the process is completed, date of prior consent. In view of the legally established criteria for issuing the school pass, it is considered that the personal data that will be transmitted are necessary and adequate to fulfill the purpose, in compliance with the principle of data minimization, as per subparagraph c) of paragraph 1 of the article 5 of the GDPR.,

12. Access to data requires prior authentication and is only allowed by assigning an application user and a password. The communication of information is carried out through a dedicated circuit between DGEEC and TIP. The granting entities register all information queries carried out in this area, which is marked as positive, and the records are kept for two years for audit purposes.

Prior consent - Fourth Clause

13. It is up to the DGEEC to obtain the unequivocal consent of the parent or of the student if of legal age, for the access and transmission of the aforementioned data, which constitutes a basis for the lawfulness of the treatment under the terms of subparagraph a) of no. 1 of article 6 of the GDPR. The consent mechanism will be implemented and made available by DGEEC on the Enrollment Portal, and the right to withdraw consent may be exercised until the respective card is issued.

14. Decree-Law No. 186/2008, of 19 September, created the school pass or «passe 4 18fg)escola.pt», and Ordinance No. 268-A/2012, of 31 August, amended the conditions for granting the school pass provided for in Ordinance No. 138/2009, of February 3, amended by Ordinance No. 982-A/2009, of September 2, and 34-A/2012, of February 1 , Ordinance 249-A/2018, of September 6, and 353/2019, of October 7. In turn, Decree-Law no. public school transport1. However, these legal provisions are limited to providing as assumptions for the attribution of passe4-18@escola.pt the conditions that students have to fulfill, whose proof is now intended to be expedited.

15. Thus, and in the absence of a law that expressly determines the ways of speeding up the test and verifying the fulfillment of the legal requirements in the specific case for the allocation and maintenance of a school pass, only the consent of the parents or data subjects if they are larger, this processing of personal data is legitimate.

16. In turn, paragraph 5 of Clause Four provides that, in case of need to change the consent according to the will of the student's guardian, or of the student if he is of age, after sending the information by the from the DGEEC for the TIP, must be requested from the TIP. The CNPD recalls that under the terms of paragraph 3 of article 26 of the RGPD, the data subject can

exercise his rights in relation to each of those responsible for the treatment, regardless of what is agreed by the granting entities.

iii. Obligations of those responsible for the treatment - Clause Six

17. Under the terms of the first clause of the Protocol, DGEC and TIP are jointly responsible for the processing, with TIP being the coordinating and operating entity of the ANDANTE System, and responsible for the issuance, management and provisioning of personalized ANDANTE Cards and also «responsible for the Andante Intermodal System, 1

1 Article 36(b) provides that it is the responsibility of the municipal councils to “request public transport service concessionaires for subscription tickets (passes) for the students covered, under the terms to be established by decree of the members of the Government with competence in the matter'.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

the central system that gathers personal data and information about customers, sales and validations of public transport operators'.

18. Operationally, the DGEEC is responsible for managing the integrated information and management system for the educational and training offer, while the DGEstE is responsible for verifying the placement of students in the respective schools and groupings. Thus, paragraph 3 of Clause 1 stipulates that the DGEstE is also considered jointly responsible for the processing, in relation to the DGEEC.

19. Thus, we are dealing with a case of joint liability, 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. In this way, the latter should define the respective responsibilities for compliance with the RGPD, namely with regard to the exercise of the rights of data subjects and

the respective duties to provide the information referred to in Articles 13 and 14, and reflect the functions and respective relationships of joint controllers in relation to data subjects (cf. Article 26(2) of the GDPR). Furthermore, the division of responsibilities must cover other obligations of controllers such as those relating to compliance with the principles of data protection, legal basis, security measures, obligation to notify personal data breaches, use of subcontractors, contacts with data subjects and the Control Authority2. 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 GDPR.

iv. subcontracting

20. It should be noted that Clause 7, relating to subcontracting, is limited to establishing the need for prior authorization for subcontracting and to complying with the provisions of Article 29 of the GDPR. It is understood that the clause is too vague and therefore it is recommended to include references to the obligations of subcontractors set out in paragraphs 2 to 4 of article 28 of the GDPR.

v. Right of access and information of data subjects - Clause eight

21. Here it can be seen that the body of the Clause is more comprehensive than its title, since it enshrines the responsibility of each person responsible for ensuring the effective exercise of the rights of data subjects, as well as the information duties referred to in the articles 13th and 14th of the GDPR. In fact, the rights of

2 See Guidelines on Owners and Subcontractors available at https://edDb.europa.eu/guidelines-relevant-controllers-and-processors en.

Data subjects are not limited to the right of access, including the right to rectification and erasure, limitation of treatment, portability and right of opposition. It is therefore suggested to change the heading to "data subjects' rights"

saw. Security and Privacy Measures - Clause Nine

22. As for security measures, point 3 of Clause 9 of the Protocol stipulates that, within the scope of collection, the grantors draw up a nominative list of employees authorized to access personal data in accordance with their function, in compliance

with the principle of data and principle minimization

the need to know enshrined in Article 5(1)(c) of the GDPR.

23. It is foreseen the use of a unique, distinct and exclusive identifier for use in this webservice that guarantees the identification of a single registration process, allowing TIS to later make the invocation again for reprocessing of registration previously transferred, indicating in the request that same identifier.

24. DGGE provides TIS with a specific service account for authentication in the system. The sending of the password for that account to TIS will be carried out separately from the information about the user to the person and telephone number previously established. The transfer of information will be carried out in a dedicated and secure circuit, with the two entities committing to record all queries and other access to information in tog files, also encrypted.

25. A Data Protection Impact Assessment was carried out, which accompanies the request for an Opinion, having classified the set of operations carried out on personal data subject to this Protocol as having a medium level of risk. As for the harmful effect, this was considered significant by virtue of the treatment of the Social School Level, given staff considered to be of a highly personal nature, taking into account the significant risk of stigmatization and discrimination in children and young people.

26. Additionally, the risk of identification of the holder, through the name, number and type of identification document was considered as maximum. To mitigate these risks that jeopardize the rights and freedoms of holders (belonging to especially vulnerable categories of holders) various technical and organizational measures will be implemented, described in the AIPD, highlighting, among them, the generation of random numbers in the variable that contains the unique identifier from the registration process number; the pseudonymization of test data used in the various development environments; encryption in data communication using the TLS 1.25 protocol; encryption in the storage of information in

production and audit log table; the elaboration of a nominal access list (ACL mechanisms); awareness-raising actions on data protection and GDPR, both at DGEEC and TIS.

27. Note that in the section "Global assessment for an acceptable AIPD", page 13, it is mentioned that the information is generically anonymized, through encryption techniques in the database, where the logs and communication channel encryption, as proposed including log storage and transmission channels (i.e. communication and storage encryption). However, the reference to the anonymization of information is not correct, since, on the one hand, the pseudonymization technique, listed in the AIPD as one of the measures to mitigate the risk for holders, is not considered an anonymization technique, since it "only makes it difficult the possibility of matching a dataset to the original identity of a data subject3'. On the other hand, if the information were in fact anonymized, it would be impossible to use it for the data processing described in the protocol.

28. After analyzing the Protocol and the IAPD, it is considered that the technical and organizational measures proposed to mitigate the risks identified in the IAPD, to be implemented under the Protocol, are acceptable and adequate to ensure the security of personal data and privacy .

III. Conclusion

29. With the introduction of the changes identified above, the CNPD believes that there are no impediments to the conclusion of the Protocol for the exchange of personal data between the General Directorate of Education and Science Statistics (DGEEC) and Transportes Intermodais do Porto, ACE (TIP) .

Approved at the plenary session of February 23, 2021

Filipa Calvão (President)

3 As provided in Opinion 05/2014 on anonymization techniques of the Article 29 Data Protection Working Group, accessible at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files /2014/wp216_en.pdf