CSNiPD

National Data Protection Commission

OPINION/2021/112

I. Order

1.0 High Commissioner for Migration, I.P (ACM), asked the National Data Protection Commission (CNPD) to issue an opinion on the draft Protocol on the creation of the ConheSer+ Platform, under the responsibility of the ACM, the Foreigners and Borders Service (SEF) and the Social Security Institute, I.P. (ISS), under a co-responsibility regime.

2. The platform is a tool that interrelates information on refugees residing in the systems of the signatory entities, creating a new database. The platform aims to facilitate the articulation of entities through "efficient and real-time operationalization and mapping of this population", with the objective of establishing "a collaborative way of working between the SEF, the ACM and the ISS so that, by aggregating the valences of the three public institutes, the Portuguese State can ensure an adequate reception to refugees in our country, overcoming the normal procedural barriers in silos between the entities and data entered in triplicate between these institutions" enabling, in short, the "integrated management of the process of host".

3. It also intends to "ensure the indicators of case management through the individual registration of applicants and beneficiaries of International protection (scheduled or unscheduled migratory movements), the registration of the life project of each [one] [...] and respective household until the stage of autonomy [...] and also the identification of secondary movements (abandonments, repossessions and take-overs)". The Platform will make it possible to produce statistical data, for monitoring, and indicators of "physical and financial execution of the ACM protocols for managing support [...] with the host entities". The "transfer of data between those responsible for treatment and the Portuguese Council for Refugees (CPR), the Santa Casa de Misericórdia de Lisboa (SCML), as well as civil society entities (host entities)".

4. 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 cj 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, Article 4(2) and Article 6(1)(a), all of Law No. 58/ 2019, of 8 August, which implements the GDPR in the

domestic legal order.

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

II. Analysis

i. Legal condition

5. The Protocol under analysis aims to regulate an information system, embodied in a single information platform for refugees, to support the entities that are responsible for processing the processes of reception and integration of people in need of international protection.

6. In fact, the SEF is the entity responsible for registering and deciding on the acceptance of the analysis of requests for international protection, as well as for guaranteeing reception conditions until the admissibility decision (cf. Law No. 27/2008, of 30 June, with the amendments introduced by Law no. 26/2014, of 5 May), the ACM is responsible for the integration of foreigners residing in Portugal (cf. subparagraphs c) and j) of no. Article 3 of Decree-Law No. 31/2014, of 27 February, Ordinance No. 203/2016, of 25 July, and also the Resolutions of the Council of Ministers No. 12-B/2015 103/2020, of 23 November) and the ISS is responsible for bearing the costs resulting from the attribution of material reception conditions to applicants for international protection who enter or are in national territory, from admission of the request until a final decision on it (cf. article 61, no. 2 of Law no. 27/2008, of 30 June, amended by Law no. 26/2014, of May 5th).

7. Council of Ministers Resolution No. 103/2020, of 23 November, created the Single Operating Group, whose limited formation only includes these three entities, with coordination functions in terms of reception and integration of refugees.

8. None of the diplomas or regulations mentioned above provide for the creation of the new processing of personal data by the ConheSer+ Platform. It is only mentioned that this treatment is provided for in measure 25 of Simplex+2018. However, the

aforementioned measure appears to be an act of a political nature, which, for that very reason, requires legislative intermediation to determine the creation of a processing of personal data and where adequate guarantees of the fundamental rights and interests of the holders of the data must always be provided. Dice.

9. In fact, the personal data being processed include extremely sensitive data, namely those relating to religious and philosophical beliefs, race and ethnicity, health, so, given the purpose, the lawful condition in paragraph b) or in Article 9(2)(g) of the GDPR. In fact, it is not enough for administrative entities with legal competence to process personal data in this context to decide, by protocol, to create a new platform and a new database, centralizing the information so far dispersed through the information systems of these three entities, invoking only a governmental measure, without legislative or even regulatory nature. Especially when they are

special data, as the point e) of paragraph 1 of article 6 of the GDPR is clearly insufficient to justify such treatment.

10. It should be noted that this is a new processing of personal data, which focuses on a wide range of especially vulnerable data subjects and concerns an extensive set of especially sensitive personal data, and which by its nature implies increased risks for these subjects , thus lacking a specific and especially guaranteed legislative framework.

11. Furthermore, both point b) and point g) of Article 9(2) of the GDPR require that the processing be based on Union or Member State law. It is this provision in Portuguese law, and specifically the guarantees to safeguard the increased risks to the rights of data subjects, that is omitted. Thus, there is no legal basis in the GDPR for the intended processing of personal data.

12. Without prejudice to what has just been concluded, the CNPD still appreciates the provisions contained in the Protocol, highlighting the aspects of the regime that must be revisited.

ii. joint responsibility

13. In paragraph 2 of Clause Six of the Protocol, the joint responsibility of the three parties is stated, referring to an "Agreement on Joint Responsibility for the Processing of Personal Data", hereinafter Agreement, which forms an integral part of the Protocol.

14. However, Clause Three defines, under the heading "Specific Obligations of the Grantors" that all entities provide and

receive information, referring to Annex F the breakdown of personal data to be shared, adding that the ACM it is incumbent upon "the management of the platform, ensuring its proper functioning and the attribution of profiles", and SEF is responsible for "ensuring the security of the information and [of] the accommodation of the ConheSer+ Platform".

15. Analyzing the Agreement, with the exception of Clauses 6.a and 9a, which, respectively, determine the existence of a specific address for a single point of contact and regulate the processing of communications regarding the exercise of the holders' rights, it appears that this it is limited to attributing to each party the fulfillment of the obligations foreseen in the RGPD, which does not comply with the provisions of article 26 of the RGPD. Therefore, its densification is recommended.

iii. Impact Assessment on Data Protection

16. The request was accompanied by the Impact Assessment on Data Protection (AIPD), in compliance with the provisions of Article 18(4) of Law No. 43/2004, amended by Law No. 58/ 2019, August 8th.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

I (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

17. Point 4 of the IAPD states that a "brief" risk analysis is carried out, insofar as "the development phase of the computer application has not yet begun". Going through the AIPD this is clear, it is not possible to verify which actual risks exist and which measures may be able to mitigate these risks. In any case, the CNPD cannot, at this stage and with the information available, pronounce on the compliance of data processing with the RGPD.

18. It should be noted that the fact that the development of the application that will support the Platform has not started is not the only element that conditions the risk analysis. Moreover, it is also at the time of defining the means of processing that, by applying the principles set out in Article 25 of the GDPR, it is necessary to decide on the measures capable of protecting the rights of the data subjects.

19. By way of example, the issue of subcontracting is mentioned. The possibility is stated for those responsible for the treatment to be able, whenever justified, to resort to subcontractors, with their obligation to implement all technical and organizational measures appropriate to the protection of the personal data transmitted to them by the responsible in question, in order to ensure the defense of the rights and interests of the respective holders, and always in compliance with the provisions of Articles 28 and 29 of the GDPR.

20. But this reference is generic, limiting itself to repeating the provisions of Article 28(1) of the GDPR and referring to the provisions governing subcontracting.

21. The AIPD says that "the subcontractors involved in this process have not yet been determined. As soon as this is done, they will assume such a position and the contract or other normative act must be signed with each subcontractor, establishing all the aspects stipulated in the Article 28 of the GDPR, namely the duration, scope, purpose, documented treatment instructions, prior authorization where a subcontractor is involved, provision of any documentation proving compliance with the GDPR, immediate notification of any data breach, as well as defined in article 29 of that Regulation".

22. However, since it is not indicated whether there will be subcontracts and which services they will involve, it is not possible to assess the resulting risk. Therefore, the determination of the existence of subcontracts will necessarily have to be subject to a new risk assessment.

23. As for the possibility of transferring personal data outside the European Union, there seems to be a contradiction between the IAPD, where it is stated that they are not provided for, and the Agreement, since Clause 11,a, deals with "Transfers of data outside the European Economic Area".

24. Little is mentioned about the technology to be used to implement the platform, with only a brief reference in the section that addresses malicious software, where it is indicated that access can be made through less secure networks and that browsers will be updated for this purpose.

25. It is therefore understood that this is a web application accessed by users via browser. Strictly speaking, nothing is known about the communication infrastructure, whether on an internal network with dedicated access or available on the internet,

nothing is said about the security of information transport between the customer and the ConheSER+ platform, nor the means used to communicate with the external entities.

26. Nothing is mentioned regarding the security infrastructure, namely if it exists and if illicit access and other attacks are prevented.

27. Also regarding the interoperability between the systems, it is mentioned that the entities intend it to be carried out through the Interoperability services of the Public Administration, made available by AMA, IP. Nothing is detailed on this matter and none of the documents sent adds any information on the matter.

28. Likewise, nothing is indicated regarding the technology used for the database managed by the Platform, nor the infrastructure that implements it, nor the communication of the application component with the data repository, nor the administration policy of that repository and access control, nor, with the necessary rigor, in relation to the backup policy.

29. It is hereby declared that, in addition to nominal accesses to the ConheSER+ Platform, access via the web service will be made available. It has as authentication credentials a username and password, unique to all invocations. It is not specified which set of operations this web service makes available or which entities are capable of invoking it. From reading the documents, one can only speculate that it can be used for the automatic loading of information from the SEF to the ConheSER+ platform, at the beginning of the process, and in the return of information to the SEF systems. Furthermore, these automated operations referred to in the annexes are not known in detail.

30. Still regarding the web service, it is not known whether the functionalities it makes available go beyond the competences of the different entities when they access ConheSER+. It would be important to clarify whether the web service will have capabilities that can be invoked by the entities' systems, thus circumventing the limitations that the platform imposes on users' direct access.

31. Nothing is mentioned about the transfer of data to external entities, such as, for example, the Portuguese Council for Refugees, Santa Casa da Misericórdia de Lisboa and the various entities of

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

host. Nothing is indicated about the data that are sent, nor about the security measures adopted in the transport of information, nor about the technology used. Nor is it mentioned how communication is triggered.

32. The IAPD identifies the risk of illegitimate access that makes consultation, alteration or deletion operations possible. As potential sources of this risk, the sharing of credentials between employees and identity theft are pointed out, and as a mitigation measure it is proposed "that users are duly and regularly informed of good hygiene and safety practices", together with the definition of strong passwords, as well as mechanisms for blocking the session However, given the sensitivity of the information processed, the measures indicated are clearly insufficient, requiring the use of multi-factor authentication mechanisms.

33. References to audit records are not sufficiently detailed. It is indicated that the operations of accessing, creating and editing records, and exporting data, will be logged. Nothing else is mentioned regarding the content of these audit logs, apart from mentioning that they identify the user and the date/time of the change.

III. Conclusion

34. On the grounds set out above, the CNPD considers that the Protocol concerns the processing of personal data that is not based on lawfulness and cannot, therefore, under penalty of violating Article 9 of the GDPR, be carried out.

35. Nevertheless, the CNPD points out above the provisions of the Protocol that need to be reformulated and densified and the aspects of the treatment that need to be evaluated and specifically recommends that:

The. The Agreement on Joint Responsibility for the Processing of Personal Data is reviewed in order to establish the responsibilities of each jointly responsible person, in compliance with Article 26 of the GDPR;

B. The means of processing are clearly defined and a new IAPD is carried out, so that mitigating measures capable of guaranteeing the fundamental rights and interests of the holders of personal data are foreseen.

Lisbon, August 26, 2021

lipa Calvão (President who reported)