NATIONAL COMMISSION

DATA PROTECTION

OPINION/2020/54

I. Order

The Ministry of Foreign Affairs, through the Directorate-General for Foreign Policy, asked the National Data Protection Commission (CNPD) to comment on the draft Cooperation Agreement between the Portuguese Republic and the Tunisian Republic in terms of internal security (hereinafter 'Agreement').

The CNPD issues an opinion within the scope of its attributions, as the national authority to control the processing of personal data, conferred by paragraph 2 of article 30, in conjunction with paragraph 1 of article 43 and paragraph a) and c) of n. 0 1 of article 44, all of Law n. 0 59/2019, of August 8.

The purpose of this Agreement is technical cooperation and exchange in matters of internal security {d. article 1). Areas of technical cooperation are identified in article 2, namely: prevention and fight against crime in general; management of major events; exchange of information between the different security services of the Parties, proximity policing; managing migratory flows and combating irregular migration and trafficking in human beings; road safety and prevention; training and other areas. The exchange will include the modalities defined by the programs referred to in Article 3 (see Article 2(2)).

Pursuant to Article 3 of the Agreement, under the heading "Modes of Cooperation", the Parties agree, inter alia, to exchange knowledge and best practices between security services, exchange and visits of experts, organize meetings and seminars in the territory of both the Parties, organization of training sessions.

Article 3(2) of the Agreement refers to programs whose scope, objective and responsibility for implementation will be defined on a case-by-case basis, by legally competent bodies, upon approval of the governmental areas with competence in the area of cooperation in question, the terms of which cooperation, in accordance with paragraph 3 of the same article, also deferred for proper regulation through the signature of specific agreements or additional protocols.

Under Article 4 of the Agreement, they are designated as competent authorities for the execution and application of the Agreement, without prejudice to the involvement of other public entities with competence in the aforementioned areas of cooperation, for Portugal the Ministry of Internal Administration, and for Tunisia the Ministry of Interior.

The possibility of exchanging personnel or missions of specialists in security, material and logistics is also foreseen, as well as the secondment of liaison officers, with advisory and assistance functions, not exercising powers of public authority.

Article 8 of the Agreement, entitled "Confidential information, documents and personal data", begins by providing that the parties must ensure the confidentiality of information, documents and personal data received, in writing or orally, (.. .), in compliance with international law and applicable domestic law, and the requested Party must notify the requesting Party that the information provided is confidential (see paragraphs 1 and 2).

According to paragraph 3 of article 8, the information received, including personal data, cannot be transferred to third parties, without the prior consent of the requested Party and provided that adequate legal guarantees regarding the protection of personal data are offered, in the terms of international law and applicable domestic law.

As for the mutual protection of classified information, the Parties will seek to conclude an agreement (see paragraph 4 of the same article).

Article 9 of this Agreement, under the heading "Use and transfer of personal data", provides, in its paragraph 1, that, under the terms of international law and applicable domestic law, the processing of data carried out within the scope of this Agreement , respect the principles of purpose, minimization, updating and conservation limitation.

Paragraph 2 of the article regulates the exercise of the rights of the holders, providing that, upon request, access to the data must be given, as well as proceeding with its correction, except when this request can be refused under the terms of international law and international law. applicable internal.

Among the remaining articles of the Agreement (from the 10th to the 15th), its duration of three years, automatically renewable, for equal and successive periods, and the fact that either Party

be able to denounce the Agreement, and its denouncement will not affect the projects or programs in progress (...) and not yet implemented, at the date of its expiry.

II. appreciation

The object of this Agreement, as it relates to matters of internal security, implies its legal assessment in light of Law no. by the competent authorities for the purpose of preventing, detecting, investigating or prosecuting criminal offenses or enforcing criminal sanctions.1

This bilateral agreement provides for the transmission of personal data from Portugal to Tunisia, and is therefore covered by the specific regime for transfers of personal data to third countries, provided for in Chapter V of Law No. need to comply with the remaining legal provisions contained in this diploma.

To that extent, it is necessary to assess, first of all, the adequacy of the level of protection of personal data in the Tunisian Republic, as this will result in the need to insert in the Agreement, as a binding instrument for the Parties, specific data protection rules, which allow address any shortcomings in the third country's domestic law and provide adequate guarantees with regard to the protection of personal data.

A. The level of data protection in the Tunisian Republic

In accordance with Article 38(1) of Law No. 59/2019, the transfer of personal data to a third country may be carried out on the basis of an adequacy decision of the European Commission, which determines that that third country or a specific sector of that country ensures an adequate level of protection. However, the Tunisian Republic was not the subject of an adequacy decision, so that, failing that, the international transfer of personal data

1 Law transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

it can only occur if adequate guarantees have been presented with regard to the protection of personal data through a legally binding instrument (cf. subparagraph a) of paragraph 1 of article 39 of the aforementioned law).

This Agreement constitutes a legally binding instrument, and it is therefore necessary to ensure that it meets the appropriate guarantees regarding the protection of personal data. The extent of safeguards to be introduced depends on the level of data protection existing in the third country.

According to the jurisprudence of the Court of Justice of the European Union, it is not required that the third country guarantees a level of protection identical to that guaranteed by the legal order of the Union, but that it effectively guarantees, by virtue of its domestic legislation or its international commitments, a level of protection of fundamental freedoms and rights substantially equivalent to that provided within the Union (see judgment in Schrems, C-362/14, EU:C:2015:650, nos. 73 and 74).

Only in this way will it be possible to ensure that the protection of personal data processed in the Union is not circumvented, extending the necessary protection to the rights and freedoms of individuals. Let's take a look at the main rules of Tunisian domestic law.

Tunisia ratified, on 18/7/2017, the Convention for the Protection of Persons with regard to the automated processing of personal data (Convention No. 108), of the Council of Europe, and its additional protocol (No. 181), having also been a signatory, since 5/24/2019, of the Protocol amending the Convention (No. 223), modernizing it and aligning it with the new European legal framework on the protection of personal data.

It has constitutionally enshrined, in the chapter on rights and freedoms, the protection of private life, the inviolability of the home and the secrecy of correspondence, communications and personal data (cf. Article 24 of the Constitution of the Tunisian Republic of 2014).

As for other legislation, it appears that Tunisia has a law on the protection of personal data, Organic Law 2004-63 of 27 July 2004 (hereinafter “LOPD”), supplemented by Decree No. 2007-3004 , of November 27, 2007, which sets out the conditions and procedures for notification and authorization for the processing of personal data. Decree no. 2007-3003, of 27 November 2007, which sets out the operating modalities

of the national body for the protection of personal data. Indeed, Tunisia has a national supervisory authority - INPDP - responsible for supervising the processing of personal data.2

Analyzing the Tunisian data protection law, it is confirmed that it is applicable to the object of this Agreement, as it includes data processing in the context of public security or national defense, or for criminal proceedings (cf. article 53 of the LOPD).

However, there are several derogations for public entities (cf. articles 54 and 56 of the LOPD), among which, due to its relevance in this case, the absolute denial of the exercise of rights to data subjects stands out: right of access, right of rectification and right of erasure3.

In fact, adherence to Convention 108 and its protocols has not been reflected, in terms of Tunisian domestic legislation, in a full implementation of these international legal instruments, in particular in matters essential to our national law and to European law, such as the rights of data subjects. The right of access is, in itself, a fundamental right, expressly recognized by the Portuguese Constitution (Article 35(1)) and by the Charter of Fundamental Rights of the European Union (Article 8(2)), and cannot therefore be outright denied.

Also with regard to the processing of sensitive data, listed in article 14 of the LOPD, and equivalent to Portuguese and European legislation, there is a total derogation from the safeguards for the processing of this special category of data, when carried out by public entities.

Thus, without the need to analyze here in detail other aspects of Tunisian legislation, there are serious deficiencies in terms of the level of data protection offered, and it is crucial to regulate some matters in the text of the Agreement, otherwise they will not be met. the adequate guarantees legally required.

Indeed, the reference of the Agreement to the applicable national law cannot be accepted in this case, due to the shortcomings of Tunisian law regarding the processing of data by entities

2 http://www.inpdp.nat.tn/

3 With exceptions for the processing of health data by public entities, in which the exercise of certain rights is allowed.

("NATIONAL MISSION

DATA PROTECTION

public. Furthermore, we are dealing with processing of personal data of special sensitivity, taking into account the matter in question, and with a notable impact on the rights and freedoms of individuals.

In short, it is essential that the text of the Agreement contains rules that address the main weaknesses detected in the Tunisian data protection legislation, so that the adequate guarantees for the protection of personal data provided for by Portuguese and Union law are assured.

B. The text of the Agreement

1. First of all, it should be noted that the object of the agreement is quite generic, focusing on the vast area of internal security and combining modalities of technical cooperation, exchange of knowledge and good practices and training, with exchange of personal data. However, as far as the processing of personal data is concerned, the purposes of this processing are not specified, nor exactly what areas of cooperation involve the processing of personal data. This immediately precludes the subsequent analysis regarding the concrete application of the remaining data protection principles, provided for in article 4 of Law No. 59/2019.

2. On the other hand, the categories of personal data to be transferred are not described, which would necessarily depend on the purposes for which they were intended and which would be essential to assess their suitability.

3. Also with regard to the parties involved in the Agreement, there is no mention of the "competent authorities", within the meaning of article 3, paragraph 1, point i), of Law 0 59/2019, responsible for data processing in Portugal who are involved in the transfer of personal data to Tunisia. Likewise, it is not known whether in the third country who will receive the transferred personal data are competent authorities, as required by Article 37(1)(b) of Law No 59/2019. 4

4. The only reference is in Article 4 of the Agreement, indicating as "competent authorities" for the execution and application of the Agreement the respective ministries that oversee the

area of internal security. However, the governmental oversight and respective powers to enforce the Agreement in the respective States cannot be confused with the nature of public "authority" that they do not hold, suggesting the adaptation of the wording.

5. On the other hand, in Article 2(1)(1) and in Article 3(1) of the Agreement, there is a reference to "security services" of the Parties, not understanding whether the cooperation is restricted to these services. However, pursuant to article 25, no. 2, of Law no. 53/2008, of 29 August, last amended by Law no. 21/2019, of 25 February (Internal Security Law) , which determines which security forces and services perform internal security functions4, it appears that, according to the respective organic laws, only the SEF and, although not expressly, the SIS, qualify as “security services” , with the GNR and PSP being qualified as 'security forces'. This is, therefore, a misnomer.

6. In fact, the text is silent on the identification of those responsible for the processing of data covered by the terms of this Agreement, and this discrimination is essential to comply with the principle of transparency, to verify the effective quality of "competent authority", in the light of law, and for supervisory purposes. Assuming that this list is not included in the Articles of the Agreement, it is essential, however, that it be included in an annex to the Agreement, which is an integral part of it, identifying the competent authorities and exactly for what purposes they transfer and receive personal data. .

7. As for the content of Article 8 of the Agreement, which seems to cover information and documents that do not include personal data, it is suggested, for reasons of clarity, rigor and legal certainty, that the processing of personal data be regulated separately from other information that is not contain personal data.

8. On the other hand, the reference to the confidentiality of information, documents and personal data (cf. Article 8(1)) is ambiguous, as it is not clear whether this is classified information or whether there is an imposition of respect for a general principle of confidentiality, embodied, in Law no.

4 These are the National Republican Guard (GNR), the Public Security Police (PSP), the Judiciary Police (PJ), the Foreigners and Borders Service (SEF) and the Security Information Service (SIS).

compliance with obligations regarding the security of treatment (Article 31), in accordance with the principle enshrined in Article 4(f)(2).

9. In fact, also with regard to the security of data processing, subject to international transfers, the Agreement is completely silent, not containing any rule that requires the Parties to adopt appropriate technical and organizational measures, in accordance with the requirements by article 31 of Law No. 59/2019. Furthermore, the means and conditions under which the data are transferred and received must also be added to the Agreement, as an annex.

10. Regarding the rule contained in paragraph 3 of article 8, which correctly subjects the prior authorization of the requested Party to the transfer of data "to third parties" and also on the condition that there are adequate guarantees in terms of data protection, it is suggested that it be added for "third countries or international organisations", as this appears to be intended and not for any third party within the same country. It should also be added that the Party receiving the data is obliged to respect any restrictions to which the personal data are subject.

11. Regarding the communication of data to third parties, it is noted that the Agreement is also silent as to the possibility of the competent Tunisian (or Portuguese) authorities receiving personal data to communicate this data to other entities within the same country. Now, this is a matter of the utmost importance to be regulated in this Agreement. Firstly, personal data must not be subsequently communicated, as a matter of principle, to other entities in the country of destination, except in duly substantiated situations and with knowledge of the requested Party. On the other hand, it must be specifically safeguarded in the Agreement that only competent authorities for the purposes set out in article 1 of Law No. 59/2019 should be recipients of personal data. Indeed, it is necessary to ensure that personal data processed in a context of internal security - for the specific purposes that the Agreement must make explicit - are not further processed for other purposes and by other types of authorities.

12. One cannot fail to point out that Portugal is obliged to comply with a wide range of European Union legal instruments, which impose clear restrictions on the communication of personal data to third countries (e.g. transfer of data relating to applicants for international protection).

13. As for paragraph 1 of article 9 of the Agreement, this is limited to reproducing some of the general principles applicable to data processing and contained in article 4 of Law No. 59/2019. However, it refers to the terms of International Law (which one?) and to the applicable domestic law, which, as analyzed in point II.A. of this Opinion, has some crucial shortcomings. In fact, the Agreement should reflect the application of these principles, in specific rules appropriate to the specific context and taking into account the processing of personal data in question. It is not intended here to regulate the processing of data in the country of origin, but the conditions under which they will be used in the country of destination.

14. Therefore, it is immediately suggested to change the order of the heading to "Transfer and use of personal data". In this article, the specific rules for the transfer and subsequent use of personal data within the framework of this Agreement should be introduced, some of which have already been stated in this Opinion as being indispensable, namely regarding the prohibition of the use of the data for other purposes and of being processed by entities that are not competent for the explicit purposes that must be set out in this Agreement and that are not. An obligation on the requested Party to notify the receiving Party of the data must also be added whenever the personal data need to be rectified or must be erased, or subject to other restrictions, and consequently the obligation of the receiving Party to comply with this notification must be provided. The Agreement must also provide that prior authorizations for further data transfers are given in writing, and the requesting Party must also justify its request in writing.

15. With regard to possible restrictions on the processing of personal data, Portugal must guarantee reinforced protection for special categories of data (sensitive data), in accordance with the requirements of article 6 of Law No. 59/2019, as the Tunisian data protection legislation completely derogates public entities from complying with the special regime for sensitive data (cf. article 54 of the LOPD). Therefore, it would be necessary to introduce a rule in the Agreement that safeguards the processing of sensitive data that may be transferred to Tunisia. If it is impossible to insert this safeguard, Portugal must not transfer sensitive data, under penalty of violating national and European law.

16. With regard to Article 9(2), which provides for the right of access and the right of rectification, the reference to the

applicable domestic law is not acceptable, as in

Tunisia these rights are not even recognized and admitted when public entities are at stake, as explained above. It is not a question of derogations from the rights of holders, as exists in Portuguese legislation, considering the specificity of the police context, in which rights can be partially or totally derogated, through justifications provided for by law, with the possibility of their correctness being verified. by the supervisory authority, but a denial of prior exercise of any right.

17. However, this situation is unacceptable, in the Portuguese constitutional framework and in the light of Union law, so the guarantee of the exercise of the holders' rights, including the right to erasure due to illegality of the treatment, must be registered under the terms of the Agreement , without reference to national legislation.

18. Finally, it should be noted that the Agreement must contain a rule on administrative or judicial remedies for data subjects, which must be guaranteed in relation to any processing of personal data resulting from this Agreement.

III. Conclusion

On the grounds set out above, the CNPD understands that:

1. It is essential that the text of the Agreement contains rules that address the main weaknesses detected in the Tunisian data protection legislation, so that the adequate guarantees of protection of personal data provided for by Portuguese and Union law are assured.

2. The explicit purposes of the processing of personal data covered by the Agreement must be specified and the categories of personal data associated with them must be indicated;

3. The list of competent authorities, within the meaning of Law no. 59/2019, responsible for the processing of transferred personal data must be included in the annex to the Agreement, forming an integral part of it;

NATIONAL COMMISSION

ut rDATA ROTECTION

4. The rules on the processing of personal data must be regulated separately from those concerning other information or documents that do not contain personal data;

5. The Agreement must contain obligations related to the security of the processing of personal data, and the effective means and conditions under which international data transfers take place must be described in an annex to the Agreement, forming an integral part of it.

6. Articles 8 and 9 of the Agreement should be reviewed in the light of the observations made between paragraphs 10 to 14 of point II.A of the Opinion.

7. Specific rules must be introduced to ensure enhanced protection of sensitive data and to guarantee the exercise of the rights of data subjects, and the reference to the applicable domestic law must be removed, since the legislation of the Tunisian Republic, in this matter, does not offer any protection or allow the exercise of rights.

8. Finally, the Agreement must contain a rule regarding administrative or judicial remedies for data subjects, which must be guaranteed in relation to any processing of personal data resulting from this Agreement.

Approved at the plenary meeting of May 21, 2020

Filipa Calvão (President)

Filipa

Calvão

Digitally signed by Filipa Calvão Data: 2020.05.21 15:05:01 +01'00'