COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 15 October 2015 T-PD(2015)14

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD)

OPINION ON THE REQUEST FOR ACCESSION BY TUNISIA

Directorate General of Human Rights and Rule of Law

Introduction

By letter dated 6 July 2015, registered on 3 August 2015 at the Secretariat of the Council of Europe, the Tunisian Minister of Foreign Affairs expressed the Republic of Tunisia's interest in being invited to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention 108") and its Additional Protocol regarding supervisory authorities and transborder data flows.

The Consultative Committee of Convention 108 (T-PD) points out that it invited the Committee of Ministers in 2008 to take note of its recommendation to allow non-member states with data protection legislation in accordance with Convention 108 to accede to this Convention. The Ministers' Deputies took note of this recommendation and agreed to examine every accession request in the light of that recommendation (1031st meeting, 2 July 2008).

Opinion

In accordance with Article 4 of Convention 108, each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in the Convention (Chapter II). Pursuant to Article 3.1 of the Additional Protocol, the Parties shall regard the provisions of Articles 1 and 2 of the Protocol as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

Having examined the Constitution promulgated on 27 January 2014 and the relevant legislation (Institutional Act No. 2004-63 of 27 July 2004 on personal data – hereinafter the "Data Protection Act"), the T-PD notes the following.

1. Object and purpose (Article 1 of Convention 108)

Article 24 of the Constitution provides: "The state protects the right to privacy and the inviolability of the home, and the confidentiality of correspondence, communications, and personal information". Article 1 of the Data Protection Act sets out its object and purpose: "Everyone has the right to the protection of personal data relating to his or her private life as one of the fundamental rights guaranteed by the Constitution. The processing of personal data shall comply with the principles of transparency, fairness and respect for human dignity, in accordance with the provisions of this Act."

While Article 1 of the Data Protection Act is in the spirit of the Convention, it should be noted that Article 1 of Convention 108, the aim of which is to secure for every individual "respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')", is a means of protecting an individual with regard to the processing of personal data other than those "relating only to their private life" and that this limitation in the Tunisian Act should consequently be reviewed.

2. Definitions

a) Personal data (Article 2.a of Convention 108)

Article 4 of the Data Protection Act defines personal data as “any information, whatever its origin or its form, relating to an individual who can be identified either directly or indirectly, with the exception of information relating to public life or considered as such by the law”.

This definition is more detailed than the wording of Convention 108 and corresponds to the definition given in Article 2.a of the Convention, but with the exclusion of a category of information (“relating to public life)” that should in pursuance of Convention 108 fall within the scope of the definition of personal data and accordingly be accorded the corresponding protection (provided there is no conflict with the right to freedom of expression, which, when several conditions are met, authorises a restriction on the right to respect for privacy).

b) Automated data file (Article 2. b of Convention 108)

Article 6 of the Data Protection Act defines the “data file” as “any structured and collated set of personal data that may be consulted in accordance with specific criteria that enable a particular person to be identified”.

This definition is narrower than that of Convention 108, which states that “automated data file means any set of data undergoing automatic processing”. The Data Protection Act uses the concept of “consultation” rather than “processing”.

c) Automated processing (Article 2.c of Convention 108)

Article 6 of the Data Protection Act defines the processing of personal data as consisting of “manual or automated operations carried out by an individual or legal entity, with the aim of obtaining, recording, storing, organising, altering, exploiting, using, sending, distributing, disseminating, destroying or consulting personal data, as well as any operation in relation to the use of databases, indexes, directories, data files or the interconnection thereof”.

The definition of processing in the Data Protection Act corresponds to the one given in Article 2.c of Convention 108 but without emphasising the application of logical and/or arithmetical operations to data, which is covered by the terms data exploitation and use. The Data Protection Act adds to the non-exhaustive list in Convention 108 a number of operations, including manual operations, such as interconnection (which is also defined), indexes and directories.

d) Controller (Article 2.d of Convention 108)

The definition of the controller is provided in Article 6 of the Data Protection Act: “any individual or legal entity that determines the aims and means of the processing of personal data”.

This definition does not expressly mention the public authorities, in contrast to Convention 108, the scope of which covers both the private and the public sector. Section 1 of Chapter V, on

specific processing categories, deals with the processing of personal data by public entities (Article 53 to 61 of the Act) and sets out a system of exceptions.

Section 2 of the Data Protection Act describes precisely and in considerable detail the obligations of the controller (or, as the case may be, the processor, who is also defined in Article 6).

3. Scope of the data protection system (Article 3 of Convention 108)

The Data Protection Act contains no details of its scope of application.

Having regard to the Convention, the Tunisian legislation, the scope of which appears considerably more limited, should specify and stipulate the scope of the Data Protection Act, which should be identical for processing carried out by both the private and the public sector.

In addition, Article 16 of the Act, relating to the processing of data concerning the employee's work situation, seems to establish a system of exceptions, which should not be the case.

4. Quality of data (Article 5 of Convention 108)

Article 9 of the Data Protection Act sets out the fundamental principles according to which the processing of personal data must be carried out: "The processing of personal data shall be carried out with due respect for human dignity, privacy and public freedoms".

The same Article states that "[t]he processing of personal data, whatever its origin or form, shall not violate the human rights protected by the laws and regulations in force. In all cases, the use of personal data with the aim of breaching the rights or damaging the reputation of individuals shall be prohibited".

Articles 10 and 11 of the Data Protection Act give effect to the fundamental principles of data protection, such as limiting the purposes for which it may be carried out (Article 10: "The collection of personal data shall be carried out exclusively for lawful, specific and explicit purposes"). Moreover, Article 17 contains a strict ban on "providing services to or giving an advantage to persons in return for their consent to the processing of their personal data or the use of their personal data for purposes other than those for which they have been collected".

The Act also mentions conditions relating to quality and proportionality (Article 11): "Personal data shall be processed honestly and within the limits necessary to achieve the purpose for which they have been collected".

Article 11 of the Act also states that the data controller shall ensure that the data are accurate, precise and up-to-date.

Generally speaking, the principles mentioned in Articles 9 to 11 of the Data Protection Act are in line with the provisions of Convention 108. Article 12 provides for an exception for the collection of data "if the processing is essential for particular scientific purposes" (Article 12 in conjunction with Articles 66 to 68). As far as this exclusion is concerned, it is recommended that reference be made to the relevant legislation or that new legislation be passed, if such is not already the

case, specifying and governing these forms of processing. Clear mention should also be made of the legitimate grounds for any processing (law, contract, consent, etc), whereas this is only laid down in the case of subsequent processing operations (Article 12 of the Act).

5. Special categories of data (Article 6 of Convention 108)

Articles 13 and 14 of the Data Protection Act prohibit the processing of data "relating to offences, convictions, criminal prosecutions, sentences, preventive measures and criminal records, as well as data concerning, "directly or indirectly, racial or genetic origin, religious beliefs, political or philosophical views, trade union membership or health".

The Act also provides for exceptions to this prohibition. For example, the data in question may be processed if the data subject has given his or her explicit consent by any means leaving a written record, if these data have clearly entered the public domain or if the processing is necessary for historical or scientific purposes or for the protection of the data subject's vital interests.

Article 15 states that the processing of the data in question is subject to the authorisation of the National Personal Data Protection Authority, with the exception of data relating to health.

Articles 62 to 65 also contain provisions on the processing of health data (Chapter V of the Act, Specific processing categories).

Articles 13, 14 and 15 and Chapter V of the Data Protection Act (Articles 62 to 65 on the processing of health data, and Articles 66 to 68 in connection with scientific research) refer to the fundamental principle of prohibiting the processing of sensitive data, together with the possible exceptions and the generally appropriate safeguards, albeit reduced with regard to health data. These safeguards, provided for in Articles 12 and 14, may, on the whole, be considered to be in compliance with the provisions of Convention 108, with the exception of the processing of data on the sexual lives of the persons concerned, which is not the subject of any specific additional safeguards such as those provided by Article 6 of Convention 108, and with the exception of Chapter V, in which the reduced system of exceptions may prove insufficient. The processing of sensitive data by public entities is not covered by any specific system of protection and therefore fails to meet the requirements of Convention 108.

In addition, at the end of this list of exceptions to the prohibition of processing personal data the Act provides for the possibility of an exception when the data have "clearly entered the public domain or if the processing is necessary for historical or scientific purposes". As far as these eventualities are concerned, it is recommended that they be clarified or that specific legislation be passed, if such is not already the case.

6. Data security (Article 7 of Convention 108)

In accordance with Articles 18 to 21 of the Data Protection Act, the data controller (and the processor, under Article 20) must implement appropriate technical and structural measures to ensure the security of personal data against accidental or unauthorised destruction, accidental

loss, unauthorised access, alteration or dissemination, as provided for by Article 7 of Convention 108.

Articles 18 to 21 of the Data Protection Act comply with the requirements of Article 7 of Convention 108.

7. Right to information (Article 8.a of Convention 108)

Article 31 sets out the information that must be notified to data subjects before their personal data are processed.

"- the nature of the personal data covered by the processing;

- the purposes of the processing of the personal data;

- whether replies to the questions are compulsory or optional;

- the consequences of any failure to reply;

- the name of the individual or legal entity in receipt of the data or the name and address of the individual or legal entity that has right of access;

- the surname and first name or the company name of the data controller and, where applicable, the name and address of the data controller's representative;

- their right of access to the data relating to them;

- their right to withdraw their consent to the processing at any time;

- their right to object to the processing of their personal data;

- the period of storage of personal data;

- a summary of the steps taken to guarantee the security of personal data;

- the country to which the data controller may intend to transfer the personal data.

The notification must be made by registered letter with acknowledgement of receipt or by any other means leaving a written record at least one month prior to the date scheduled for the processing of personal data."

The wording of these provisions complies with the requirements of Article 7 of Convention 108.

8. Additional safeguards for the data subject (Article 8.b to d of Convention 108)

The Data Protection Act provides for the right to object (Articles 42 and 43), the right of access (Articles 32 to 41), the right to rectification (Article 40, and data controller's obligation in Article 21) and the right of deletion (Article 45).

a) Right of access:

Article 32 states that "the right of access shall be understood as the right of the data subject to consult all the personal data relating to him or her as well as the right to correct, complement, rectify, update, modify, clarify or delete the data where they prove inaccurate or ambiguous or where the processing of such data is prohibited. The right of access shall also cover the right to obtain an accurate copy of the personal data in clear language and in an intelligible form where the data are processed by automated means".

Article 34 provides that the right of access may be exercised "by the data subject, his or her heirs or guardian". While it may appear normal that this right be exercised by a legal representative in certain circumstances, care should be taken to ensure that the rights of data subjects are safeguarded.

It should be noted that this right is not always applicable where data are processed by public entities.

b) Right to object:

In accordance with Article 42 of the Data Protection Act, any data subject "has the right to object to the processing of personal data related to him or her […], except where the processing is provided for by law or is required by the nature of the obligation. Furthermore, the data subject […] (has) the right to object to these data […] being communicated to third parties in order to enable them to be exploited for promotional purposes".

c) Right of rectification and deletion:

- Rectification

Article 40 provides that "[t]he data subject may request that personal data relating to them be rectified, supplemented, modified, clarified, updated and deleted where they prove inaccurate, incomplete or ambiguous or to ask for the data to be destroyed where their collection or use is in breach of this Act".

The Act also provides for the possibility for data subjects to "request, free of charge, […] a copy of the personal data and to indicate what action has not been carried out in respect of these data".

- Deletion

Article 45 provides that "personal data shall be destroyed as soon as the specified storage period has expired".

d) Right of appeal

Article 38 provides that "if the data controller or the sub-contractor [*processor*] refuses to allow the data subject to consult his or her personal data or postpones access to these data or refuses to issue a copy of these data, the data subject, his or her heirs or guardian may apply to the [National Personal Data Protection] Authority within one month of the refusal."

The T-PD notes that a number of matters could be clarified: 1) the criteria applicable for determining the existence (or otherwise) of a fee for exercising the right of access; 2) the current amount of the fee, in order for an assessment to be made as to whether it satisfies the criterion laid down in Convention 108 ("without excessive […] expense"); 3) whether this fee is reimbursed to the data subject if the data are imprecise or the processing is unlawful; 4) the Act says nothing about the deadlines by which the data controller must comply with the request. This needs to be clarified in order for an assessment to be made as to whether the deadline satisfies the criterion laid down in Article.8 b of Convention 108 (access to these data must be obtained "without excessive delay").

Overall, the additional safeguards meet the requirements of Convention 108.

9. Exceptions and restrictions (Article 9 of Convention 108)

Chapter V of the Data Protection Act sets out a system of exceptions where processing is carried out by public entities "in connection with public security, national defence or criminal prosecutions or where the said processing proves necessary" for carrying out public service duties in pursuance of the laws in force.

This system of exceptions seems too broad insofar as no qualifying details are provided with regard to the actual purpose of the processing and as there are no additional safeguards for the processing of sensitive data.

The T-PD believes it necessary to clarify the compatibility between freedom of expression and the protection of privacy in order to comply with the principle laid down in Article 9.2.b of Convention 108.

10. Sanctions and remedies (Article 10 of Convention 108)

The Data Protection Act (Articles 86 to 103) specifies the penalties applicable to breaches of the Act. These provisions meet the requirements of Article 10 of Convention 108.

11. Transborder data flows (Article 12 of Convention 108 and Article 2 of the Additional Protocol)

Article 51 of the Data Protection Act provides: "The transfer to another country of personal data […] may not take place except where that country ensures an adequate level of protection, which is to be assessed in the light of the nature of the data to be transferred, the purposes of the processing, the period scheduled for the processing, the country to which the data are to be transferred and the requisite precautions taken to ensure data security". Such transfer is also subject to compliance with the conditions laid down by the Data Protection Act.

In addition, Article 50 of the Act prohibits, in a general way, "communicating or transferring personal data abroad where such communication or transfer may endanger public security or harm Tunisia's vital interests".

Overall, these provisions meet the criteria set out in Convention 108 and the Additional Protocol.

Article 52 of the Act also provides that "[i]n all cases, the authorisation of the [National Personal Data Protection] Authority shall be required for the transfer of personal data abroad".

12. Supervisory authority (Article 1 of the Additional Protocol)

Article 75 of the Data Protection Act establishes the National Personal Data Protection Authority, which is the supervisory body responsible for ensuring compliance with the principles applying to the processing of personal data. Decree No. 2007-3003 of 27 November 2007 lays down the Authority's operating procedures.

The same Article provides that this institution is financially independent as its budget is part of that of the ministry with responsibility for human rights.

These provisions are in conformity with Article 1.1 of the Additional Protocol to the Convention.

Furthermore, Article 79 provides guarantees of impartiality with regard to the Authority's internal functioning: "It is prohibited for the President of the Authority and its members to hold any direct or indirect interest in any firm involved in the processing of personal data, whether automated or manual".

With regard to guarantees of institutional independence and in order to be fully compliant with Article 1.3 of the Additional Protocol, which stipulates that "[t]he supervisory authorities shall exercise their functions in complete independence", Tunisian legislation should clearly establish the Authority's independence and clarify its legal status, as well as the conditions relating to the renewal or dismissal of the members of the Authority.

Article 77 establishes the Authority's powers of investigation, authorisation and intervention as well as its duty "to inform the public prosecutor in the relevant jurisdiction about any offences that have come to its notice in the course of its work".

These provisions are in line with Article 1.2.a of the Additional Protocol.

Article 76 gives the National Personal Data Protection Authority the power to receive complaints in connection with the Data Protection Act. However, the Act does not state whether this remedy is open to all persons concerned or whether it is limited, and whether persons outside the country could also file a complaint or not. In order to ensure the conformity of this provision with the Additional Protocol, which requires that the supervisory authority "shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data", Tunisian legislation should clarify the arrangements for this referral.

Article 82 provides for the possibility of lodging an appeal to a court (the Tunis Court of Appeal and the Court of Cassation) against the Authority's decisions.

Overall, these provisions meet the requirements of Convention 108 and the Additional Protocol (Article.1.4).

Additional considerations

It should be noted that:

- There are a number of additional definitions of notions such as: third party, beneficiary, communication, interconnection, and processor.

- There are additional obligations concerning the preliminary procedures for processing personal data (Article 7, which provides that “any operation for processing personal data must be previously notified to the National Authority [...] at its head office”).

- Article 22 contains additional conditions to be met by the controller. The Committee questions the applicability and consequences of the condition relating to the Tunisian nationality of the controller.

- Articles 69 to 74 govern the processing of personal data for video surveillance purposes.

Conclusion

In the light of the foregoing, the T-PD considers that the Tunisian Data Protection Act generally heads towards the principles giving effect to Convention 108 and its Additional Protocol, although several modifications are necessary to bring it into full conformity, and recommends that the Committee of Ministers invites the Republic of Tunisia to accede to both instruments, once it has complied with the observations set out above.