COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 27 June 2016 T-PD(2016)17

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

(T-PD)

COMPILATION OF OPINIONS

Directorate General of Human Rights and Rule of Law

INDEX

OPINION ON THE RECOMMENDATION 2067 (2015) OF THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE "Mass surveillance"

1. The Ministers' Deputies agreed at their 1227th meeting (12 May 2015) to communicate to the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) the Recommendation 2067 (2015) on Mass surveillance, for information and possible comments by 12 July 2015.

2. The T-PD welcomes the adoption by the Parliamentary Assembly of the Recommendation 2067 (2015) which emphasises the importance of addressing the issue of surveillance practices that endanger fundamental human rights, including the right to privacy. It further welcomes the work of the Rapporteur.

3. The T-PD notes that, while the Recommendation "invites the Committee of Ministers to make use of the *tools* at its disposal to uphold the fundamental right to privacy in all member and observer States of the Council of Europe" it does not specifically refer to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). The T-PD recalls that the fundamental right to respect for private life is protected under Article 8 of the European Convention on Human rights, as well as under Convention 108 and its Additional Protocol, which is, to date, the only legally binding international instrument protecting individuals with regard to the processing of their personal data, thereby contributing to respect for their human rights and fundamental freedoms, and in particular their right to privacy and the protection of their personal data. The modernisation work of the Convention, which is now at its final stage, should strengthen the effectiveness of this tool at global level.

   In this respect, T-PD invites the Council of Europe to step up its efforts for the promotion of Convention 108, in view of the accession of third countries and in particular those which already Parties to the Convention on Cybercrime.

4. In relation to paragraph 2.1, the T-PD welcomes the call for a recommendation to member states to ensure the protection of privacy in the digital age and Internet safety in the light of the threats posed by the mass surveillance techniques and stands ready to contribute to any future work in the area of its expertise. It highlights, in this respect, the Council of Europe Guide to Human Rights for Internet Users, and its implementation through capacity building and cooperation assistance activities. The Guide states that Internet users must not be subjected to general surveillance or interception measures but may only be subject to legitimate interference which is prescribed by law, such as a criminal investigation. In particular, users should have access to clear and precise information about the relevant law or policy and rights in this regard.

5. The T-PD welcomes the call made to member states in paragraph 2.2 to explore internet security issues related to mass surveillance and intrusion practices. Inviting all institutions and companies that process personal data, to apply the most effective security measures available, upholds the provisions of article 7 of Convention 108, which requires from member states to take appropriate security measures for the protection of personal data according to their vulnerability. Indeed, the processing of personal data engages the responsibility of all users, both in the public and private sector. While the processing of personal data by electronic means may prove to be highly beneficial for users, it may also raise concerns and undermine the position of the persons whose data are being processed.

   Moreover, the text of the modernised Convention, in its article 7.2, contains a specific obligation for the data controller to notify without delay, at least to the competent supervisory authority, the data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

6. The T-PD welcomes the initiative of the Parliamentary Assembly to draw the attention of member states on exploring the threats posed by mass surveillance and intrusion practices, particularly in terms of human rights and fundamental freedoms. The T-PD recalls that, in the absence of any oversight mechanism, the processing of personal data may undermine the enjoyment of other fundamental rights

(the right to privacy, the right to non-discrimination and right to a fair trial) as well as other legitimate interests.

In order to maintain the balance between these various rights, Convention 108 imposes conditions and restrictions on the processing of personal data. While surveillance can be considered as being justified in the current context, this should not result in the *de facto* denial of the fundamental right to privacy for the protection of national security, as being an overriding public interest.

Furthermore, the T-PD recalls that in order to ensure respect for the rights of the persons concerned, Convention 108 and its Additional Protocol provide for the establishment of a national independent supervisory authority, with powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of the domestic law in relation to the protection of personal data. Parties, according to the Convention, further undertake to establish appropriate sanctions and remedies for violations of the provisions of domestic law giving effect to the basic principles of data protection.

In this context, the T-PD supports the call of the Parliamentary Assembly in paragraph 2.3, for the creation of an "intelligence codex" addressed to the intelligence services of all participating States and other third countries, which would define the principles of cooperation for the fight against terrorism and organised crime. Such an initiative regulating and defining clear and concrete rules is more than necessary in order to avoid any attempt of abuse. The T-PD is disposed and available to contribute in any future work if requested.

7. Finally, it is recalled that the T-PD addressed a letter to the chair of the Ministries' Deputies in December 2013, denouncing the use of mass surveillance techniques and suggesting that a line of action based on Convention 108 be defined in the field.

OPINION ON THE REQUEST FOR ACCESSION BY CAPE VERDE

Introduction

By letter dated 8 February 2016, registered on 18 February 2016 at the Secretariat of the Council of Europe, the Ministry of Foreign Affairs of the Republic of Cape Verde expressed the interest of the Republic of Cape Verde to be invited to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention 108").

The Consultative Committee of Convention 108 (T-PD) recalls that the Committee of Ministers took note in 2008 of the T-PD's 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 relevant articles of the Constitution of the Republic of Cape Verde promulgated on 25 September 1992 (hereinafter the "Constitution"), as well as the relevant legislation (Act No. 133/V of 22 January 2001 on personal data – hereinafter the "Data Protection Act" and Act No. 42/VIII of 17 September 2013 – hereinafter the "Supervisory Act"), the T-PD notes the following[1]:

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

a) Automatic processing of personal data

Article 41 of the Constitution protects the rights to private life, personal identity, the development of personality and civil capacity. Articles 43 and 44 furthermore prescribe the inviolability of home, correspondence and communications. Article 45 establishes the right to personal data protection for both computerised and manual files. Article 2.1 of the Data Protection Act reaffirms the constitutional provisions for the protection of individuals with regard to automatic or manual processing of personal data.

b) Data protection regardless the individual's nationality or residence

Article 1 of the Data Protection Act which prescribes that the Act "establishes the general legal framework on the protection of individuals with regard to the processing of personal data", with no distinction of nationality or residence, corresponds to Article 1 of Convention 108.

The T-PD notes the use of the term 'citizen' in Article 4 of the Data Protection Act and seeks reassurance of the fact that this term was not used with the intention of excluding non-nationals from the protection of the Act as the objective of Article 4 is to set out the general principles applicable to a processing.

[1] On the basis of the English versions as translated and shared by the Cape Verdean authorities.

2. Definitions

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

Article 5.1.a of the Data Protection Act defines personal data as “any information of any type/nature and irrespective of the medium involved, including sound and image relating to an identified or identifiable person, «data subject»”.

This definition is more detailed than the wording of Convention 108, giving concrete examples of two types of personal data (sound and image). The concept of personal data of the Data Protection Act is essentially the same as the definition given in Article 2.a of the Convention, referring to an “identified or identifiable person”.

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

Article 5.1.c of the Data Protection Act defines the “data file” as “any structured set of personal data which are accessible according to determined criteria, whether centralised, decentralised or dispersed on a functional or geographical basis”.

This definition is narrower than that of Convention 108, which states that “automated data file means any set of data undergoing automatic processing” with no requirement regarding the structured nature of the file.

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

Article 5.1.b of the Data Protection Act defines the processing of personal data as “any operation or set of operations which is performed upon personal data, whether wholly or partly, with or without automated means, such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, erasure or destruction”.

The definition of data processing in the Data Protection Act is in the spirit of Convention 108 since it should be read in conjunction with its aforementioned object and purpose by which automatic processing data is within the scope of the Act (item 1.a of this Opinion).

The concept of data processing in the Data Protection Act does not emphasise the application of logical and/or arithmetical operations to data, which is however covered by the fairly general terms “any operation or set of operations”. The Data Protection Act adds to the non-exhaustive list in Convention 108 a number of operations, such as alteration, erasure and retrieval.

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

The definition of controller is provided in Article 5.1.d of the Data Protection Act: “the person or group, public authority, service or any other entity/body that alone or jointly with others determine(s) the purposes [and[2]] the means for the processing of personal data.”

This definition of the controller corresponds to the one of article 2.d of Convention 108, adding the notion of joint controllership to it.

[2] The English version of the law received refers to ‘the purposes or the means’ while the original linguistic version of the law reads as follows: “as finalidades e os meios”.

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

The definitions under Article 5.1 of the Data Protection Act of "controller" and "processor" refer to public authorities implying the application of the Act to public sector processing, which is furthermore confirmed by Article 2.6 relating to the application of the Act"to the processing of personal data regarding public safety, national defense and State security without prejudice to special rules in instruments of international law to which Cape Verde is bound and specific laws pertinent to the respective sectors".

This scope of application is in accordance with Article 3.1 of Convention 108.

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

a) Obtained and processed fairly and lawfully (Article 5.a of Convention 108)

In compliance with Article 5.a of Convention 108, Article 4 of the Data Protection Act sets out the fundamental principle according to which the processing of personal data must be carried out: " […] transparently and in strict respect for privacy and for other fundamental rights, freedoms and guarantees of the citizen".

Article 6.1.a. of the Data Protection Act furthermore provides that personal data must be: "processed lawfully and with respect for the principle of good faith".

b) Purpose limitation and minimisation of data (Article 5.b and 5.c of Convention 108)

In compliance with Convention 108 Article 6.b of the Data Protection Act states that personal data shall be: "collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".

Article 6.c of the Act provides that the personal data shall be: "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

c) Accuracy and storage of data (Article 5.d and 5.e of Convention 108)

Article 6.d of the Data Protection Act prescribes that personal data shall be: "accurate and, where necessary, kept up to date, and adequate measures must be taken to ensure that data which are inaccurate or incomplete are erased or rectified having regard to the purposes for which they were collected or for which they are further processed."

Article 6.e of the Act provides that personal data must be: "kept in a form that permits identification of their subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed".

The aforementioned provisions of the Data Protection Act give effect to the requirements of Convention 108, as inaccurate data should be rectified and data that is no longer needed should be erased or anonymised.

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

Article 45.2 of the Constitution prescribes that

"The use of computer means to register and process identified individual data related to political, philosophical or ideological convictions, religious beliefs, political or trade union affiliation or private life shall be prohibited, except:

a) by the expressed consent of the holder/data subject;
b) by authorisation provided by law, with assurance of non-discrimination;
c) for data processing of non-identifiable individual statistics purposes."

Article 8 of the Data Protection Act furthermore prohibits the processing of "sensitive data", that is: "data revealing philosophical, ideological or political beliefs or penalty, religion, political party or trade union affiliation, racial or ethnic origin, privacy, health and sex life, including genetic data".

Article 8 also provides for several exceptions to this general prohibition and sensitive data may according to this derogatory regime be processed in various cases such as, for instance,: a) if the data subject [has given his or her explicit][3] consent, with the guarantee of non-discrimination and with adequate [security measures][4] ; b) with foreseen legal authorisation with the guarantee of non-discrimination and with the adequate [security measures] ; c) when the purpose of data processing are purely statistical, not individually identifiable with the adequate [security measures]; d) if the data have manifestly been made public by the data subject; e) for the protection of the data subject's vital interests; f) if data relating to the health and sexual life as well as genetic data is necessary for preventive medicine, medical diagnosis, the provision of medical care or treatments, etc.

The Data Protection Act thus requires in several cases that adequate security measures be put in place, as further developed under Article 16 of the Data Protection Act which prescribes the adoption of special security measures for the processing of sensitive data, such as for instance a strict access control, control of transmission, control of use, etc.

Such legal requirements comply with Article 6 of Convention 108.

6. Data security (Article 7 of Convention 108)

Complying with Article 7 of Convention 108, Section III of Chapter II the Data Protection Act, from Article 15 to Article 18, establishes data security obligations for data controllers. In particular, Article 15.1 of the Act states that the controller "must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular when the processing involves the transmission of data over a network and against all other unlawful forms of processing".

Article 15.2 furthermore specifies that the implementation of security measures must be made having regard to "the state of the art and the cost of their implementation" and that "such measures shall ensure an adequate level of security appropriate to the risks represented by the processing and the nature of the data to be protected."

7. Additional safeguards for the data subject (Article 8 of Convention 108)

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

Article 11.1 of the Data Protection Act lays down the obligation to inform the data subject of a series of specific information which are more detailed than the ones prescribed in Article 8.a of Convention 108. It should be noted that Article 11.4 of the Data Protection Act provides an exception to the right to information where the data subjects are aware that their personal data are circulating on an open access network without security measures.

Article 14.5 furthermore limits the right to information for national security, crime prevention and investigation, in cases of processing of data for "statistical, historical and scientific research purposes", where the provision

[3] The English version of the law received refers to 'if the data subject expressed consent' while the original linguistic version of the law reads as follows: "Mediante consentimento expresso do titular".
[4] The English version of the law received refers to 'the adequate measure of assurance' while the original linguistic version of the law reads as follows: "medidas de segurança adequadas".

of the information would be impossible or involve disproportionate efforts or where the obtaining of the data is laid down by law.

Finally, according to Article 14.6, the obligation to provide information is not applicable to processing "carried out solely for journalistic purposes or the purpose of artistic or literary expression".

b) Right of access (Article 8.b of Convention 108)

In compliance with Article 8.b of Convention 108, Article 12.1 of the Data Protection Act states that the data subject has the right to obtain from the controller, without constraints, at reasonable intervals and without excessive delay or expense a series of information which go beyond the requirements of Convention 108.

Furthermore, Article 12.2 of the Data Protection Act provides for the possibility to exercise the right of access through the intermediary of the Supervisory Authority with regard to some specific categories of sensitive data.

The right of access is furthermore safeguarded by Article 45 of the Cape Verdean Constitution.

c) Right of rectification and deletion (Article 8.c of Convention 108):

According to Article 12.1.d of the Data Protection Act the data subjects have the right to obtain the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the law
The provisions of the Data Protection Act regarding the right of rectification and deletion comply with Article 8.c of Convention 108.

d) Right to a remedy (Article 8.d of Convention 108)

Pursuant to Article 30 of the Data Protection Act, the data subjects may refer, without prejudice to their right to submit a complaint to the Supervisory Authority, to a judicial remedy for any breach of their rights guaranteed by the Act.

8. Exceptions, restrictions (Article 9 of Convention 108)

Article 2.6 of the Data Protection Act states that it applies to "the processing of personal data regarding public safety, national defence and State security without prejudice to special rules in instruments of international law to which Cape Verde is bound and specific laws pertinent to the respective sectors".

No specific Chapter of the Data Protection Act sets out a system of exceptions or restrictions but several dispersed provisions provide derogations from specific basic principles and rights of personal data protection, such as regarding the length of conservation of data (Article 6.2), prohibition of the processing of sensitive data (Articles 8.1.c and 8.5), right to information (Articles 11.5 and 11.6), right of access (Articles 12.4 and 12.6), transborder data flows (article 20.3). Overall, such limitations are prescribed for reasons of national security, the prevention and investigation of crime, for historical and scientific research, artistic or literature expression, freedom of expression and information or journalistic activities.

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

In compliance with Article 10 of Convention 108, Section II of Chapter VI of the Data Protection Act prescribes a wide range of sanctions in cases of violation of the Act, such as monetary fines (Articles 33, 34) and criminal penalties.

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

a) Adequate Level of Protection

Article 19.1 of the Data Protection Act provides that transfers abroad may only take place where an adequate level of data protection is guaranteed, with Article 19.2 providing for criteria of assessment of the adequacy of the level of protection.

Article 19.3 of the Data Protection Act furthermore assigns to the National Commission of Personal Data Protection (Supervisory Authority) the competence to decide if a foreign country provides an adequate level of protection.

These provisions do not impose substantial restrictions on the free circulation of data and the requirement of an adequate level of protection is compliant with Article 2.1 of the Additional Protocol.

b) Derogation from the principle of an adequate level of protection (Article 2.2 of the Additional Protocol)

Article 20 of the Data Protection Act provides for derogations to the principle of Article 19. Such derogations fully correspond to the requirements of Article 2.2 of the Additional Protocol, such as for instance, the possibility to authorise a transfer where such a transfer is based on the unambiguous consent of the data subject or corresponds to a particular situation listed in Article 20 (e.g. necessary for the performance of a contract or necessary for important reasons of public interest), or where adequate safeguards, notably resulting from appropriate contractual clauses, are provided.

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

a) Establishment of a Supervisory authority and powers

The Supervisory Act has amended Chapter IV of the Data Protection Act in order to establish the “National Commission of Personal Data Protection” (NCPDP), which is the supervisory body responsible for the oversight of personal data protection and monitoring, assessing and controlling data processing operations pursuant to Article 21 of the Data Protection Act.

Articles 8 to 12 of the Supervisory Act prescribe the duties and responsibilities of the NCPDP.

Among others powers, the Supervisory Authority is able to impose monetary penalties, mandatory destruction and erasure of data as well as to hear claims lodged by any data subject.

Moreover, the NCPDP has powers of investigation, judicial intervention as well as a consultative competence in the preparation of legal provisions relating to data protection.

b) Independence of the Supervisory Authority (Article 1.3 of the Additional Protocol)

Articles 13 to 25 deal with the organisation and mandate of the members and Articles 26 to 33 with the functioning of the NCPDP with a view to securing the independence of the authority.

The provisions of the Supervisory Act clarify the independence of the National Commission of Personal Data Protection.

Article 3 of the Supervisory Act on the legal regime of the NCPDP defines it as an independent regulatory authority.

Articles 17 and 18 of the Supervisory Act provide the conditions of irremovability of the members of the NCPDP.

Article 21 of the Supervisory Act prescribes that the members must exercise their functions with impartiality, independence and rigor.

c) Possibility of lodging an appeal to a court (Article 1.4 of the Additional Protocol)

Article 46.3 of the Supervisory Act provides for judicial remedies required by Article 1.4 of the Additional Protocol.

Additional considerations

It should be noted that:

- Article 2 specifies that the processing of personal data for video surveillance purposes (and others ways of recording sounds and images) is covered by the Data Protection Act;

- There are a number of additional definitions, such as: third party, beneficiary, consent, interconnection, and processor in Article 5 of the Data Protection Act;

- Article 9 regulates data processing for criminal registers, investigations, prosecution, and public security in general, ensuring that the personal data protection provisions are enforceable in this field, as the competence of the NCPDP, with possible limitations where prescribed by law and in accordance with the "principle of necessity";

- Article 10 requires an authorisation of the Supervisory Authority for any data interconnection. Article 23 provides that any data processing must be previously notified to the Supervisory Authority. Finally, Article 24 establishes the "prior checking" procedure requiring the prior authorisation by the Supervisory Authority for specific data processing operations, such as for credit evaluation and sensitive data processing.

Conclusion

In light of the above, the T-PD considers, notwithstanding pending clarifications on points 1.b) (Article 4 of the Data Protection Act) and 2.b) (definition of "data file") of the present Opinion, that the Cape Verdean relevant legislation complies with the principles giving effect to Convention 108 and to its Additional Protocol and recommends that the Committee of Ministers invites the Republic of Cape Verde to accede to both instruments.

The T-PD furthermore notes with interest that the request of Cape Verde to be invited to accede to Convention 108 was expressed together with the request to be invited to accede to the Convention on Cybercrime of the Council Europe (CETS No.185) and underlines the importance of accession to Convention 108 by State Parties to the Convention on Cybercrime and by candidates for future accession.

OPINION ON THE REQUEST FOR ACCESSION BY TUNISIA

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.