COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 29 April 2016 T-PD(2016)03

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 CAPE VERDE

Directorate General of Human Rights and Rule of Law

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.

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

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.

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.

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”.

[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”.

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.

[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".

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 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.