The Secretariat provides this compilation of 4 membership accreditation assessments conducted by Canada.

Attached are complete assessments of membership applications submitted by:

1. National Commission of Data Protection of Cape Verde
2. Autorité de Protection de Données à Caractère Personnel of Mali
3. Cybercrime Advisory Council of Nigeria
4. Office of Privacy and Data Protection of the State of Washington, USA

Executive Committee Secretariat

22 August 2016
Review of the Application for Member Status of the National Commission of Data Protection of Cape Verde to the International Conference of Data Protection and Privacy Commissioners

Following an assessment of the application received on 13 July 2016 and other information provided in support, our Office believe that the National Commission of Data Protection of Cape Verde (the NCDP) meet the five requisite criteria to be granted member status.

It is suggested that the Executive Committee put this recommendation to the full membership of the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

Analysis

In accordance with article 5.1 of the Rules and Procedures of the ICDPPC, we are satisfied that the Cape Verde NCDP:

a. Is a public entity, created by an appropriate legal instrument based upon legal traditions of the country or international organization which it belongs to

Cape Verde's Law 133/V/2001 (the “Data Protection Act”) has been in force since 22 January 2001 following its enactment and signature by the President of the Republic and of the National Assembly of Cape Verde. The law delegates a number of functions to the NCDP.

Another law, Law 42/VIII/2013 (the “NCDP Act”), regulates the composition, competence, organization and operation of the NCDP. It establishes the NCDP as an “independent administrative entity which operates within the Assambleia Nacional (National Assembly)”.

b. Has the supervision of the implementation of the legislation on the protection of personal data or privacy as one of its principal regulatory mandates

Article 8 of the NCDP Act establishes the NCDP as "the national authority endowed with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and the fundamental freedoms and guarantees enshrined in the Constitution and the law."

c. Operates under a legislation that is compatible with the principal international instruments dealing with data protection or privacy

The Cape Verde application notes that the NCDP Act implements the Economic Community of West African States (ECOWAS) Supplementary Act A/SA.1/01/10 on Personal Data (the ECOWAS Supplementary Act).

In reading the two Cape Verde Acts alongside the ECOWAS Supplementary Act and the ECOWAS Treaty of 1975, we note the national Acts' compatibility with the international instruments. In addition, the NCDP has taken steps to accede to Council of Europe Convention 108.

d. Has an appropriate range of legal powers to perform its functions

Article 8 of the NCDP Act endows the NCDP with the following powers:

- Investigation: including the power to access data undergoing processing and to collect all the information necessary for the performance of its supervisory duties;
- Order-making: including the power to order the blocking, erasure or destruction of data, or imposing a temporary or permanent ban on the processing of personal data;
- Public education: including providing public opinions before processing is carried out;
- Sanction: including by warnings or publicly censuring a processor that repeatedly fails to comply with data protection laws.

Further, Article 10 gives the NCDP responsibility for a number of functions, such as:

- Approvals: including authorizing or recording the processing and transfer of personal data;
- Compliance: including establishing retention periods and issuing directives;
- Redress: including assessing claims, complaints or applications of private individuals;
- Sanction: including the application of fines;
- Guidance: including the issuance of directives and the assessment of codes of conduct; and
- Advise: including by suggesting to the Assembleia Nacional the measures deemed useful for pursuing its duties and exercising its responsibilities.

Further, Article 6 of the NCDP Act posits that "public and private entities shall cooperate with the NCDP by providing it with all information requested in carrying out its responsibilities" while Article 7 gives NCDP members and staff "the right of access to the computer systems supporting personal data processing."

e. Has appropriate autonomy and independence

As noted above, Article 2 of the NCDP Act establishes the NCDP as an "independent administrative entity which operates within the Assembleia Nacional."
The NCDP is composed of 3 members, elected by the legislature for a once renewable term of six years. The Presidency of the NCDP is assumed by each of its members by alphabetic order respectively for a period of two years. Article 17 provides that NCDP members are "irremovable" except in very limited circumstances, including death, resignation and loss of mandate. Article 18 endows members with a series of guarantees on their job stability and benefits.
The NCDP issues monthly reports to the National Assembly about its deliberations and activities as well as a yearly report that explains legislative, administrative and financial issues evaluated in the exercise of its functions (Article 45).
Review of the Application for Member Status of the Autorité de Protection de Données à Caractère Personnel of Mali to the International Conference of Data Protection and Privacy Commissioners

Following an assessment of the application received on 8 July 2016 and other information provided in support, our Office believes that the Autorité de Protection de Données à Caractère Personnel of Mali (hereinafter the Mali DPA) meets the five requisite criteria to be granted member status.

It is suggested that the Executive Committee put this recommendation to the full membership of the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

Analysis

In accordance with article 5.1 of the Rules and Procedures of the ICDPPC, we are satisfied that the Mali DPA:

a. Is a public entity, created by an appropriate legal instrument based upon legal traditions of the country or international organization which it belongs to

Mali's Act No. 2013-015 on the Protection of Personal Data (the "Act") was passed by the National Assembly on May 9, 2013. Article 20 of the Act establishes the Mali DPA as the independent administrative authority charged with the protection of personal data.

b. Has the supervision of the implementation of the legislation on the protection of personal data or privacy as one of its principal regulatory mandates

The Mali DPA has as its mission "ensuring the protection of personal data and participating in the regulation of the Sector" (article 31).

c. Operates under a legislation that is compatible with the principal international instruments dealing with data protection or privacy

The Mali DPA's application says it does not implement any international instrument dealing with data protection or privacy, nor any other general or specific international instrument. That said, the Act appears inspired by international and European standards of data protection and follows the principles of the community law adopted by the member states of the Economic Community of West African States (ECOWAS), including Mali. Mali is a signatory of ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection and the Act uses the same language and structure as that Supplementary Act.


c. Has an appropriate range of legal powers to perform its functions

Article 31 of the Act gives the Mali DPA the mission to ensure the protection of personal data and provides it with legal powers, including:

- Guidance: the Mali DPA sets the norms for the collection, use and retention of personal data, and it can provide its opinion on any bill or decree concerning the protection of personal data;
- Supervision: the Mali DPA provides the prior authorization for the processing of personal data and authorizes data transfers;
- Public Education: the Mali DPA informs and advises data controllers and the public on their rights and obligations;
- Compliance: the Mali DPA ensures that processing practices are in conformity with privacy rights and can conduct the necessary reviews on said practices;
- Redress: the Mali DPA has the power to receive complaints regarding the implementation of data processing practices;
- Sanction: the Mali DPA can impose administrative and pecuniary sanctions in case of breach of obligations; and
- Advise: the Mali DPA can ask the Government to make legal changes necessary to strengthen the protection of personal data.

Article 34 also provides the Mali DPA with the power to investigate complaints related to its mission.

e. Has appropriate autonomy and independence

Article 20 of the Act provides that the Mali DPA is an "independent administrative authority." The Mali DPA is composed of 15 members, appointed by different branches of government and civil society for a non-renewable seven year mandate.

Once appointed, members cannot concurrently hold another government position or be board members of a public or private entity (article 22).

The 15 members elect the five members that will compose its board—a president, two vice-presidents and two rapporteurs (article 30). There are no provisions in the Act for the removal of members and their remuneration is set by Cabinet Decree, on advice of the Prime Minister (article 28).

Further ensuring the Mali DPA's independence, article 27 of the Act states no authority may order or prescribe, either directly or indirectly, the members of the Mali DPA. The budget is part of the
State budget and must be sufficient to carry out the Mali DPA's functions; it is administered by the President of the Mali DPA (article 28).

In addition, article 32 gives the Mali DPA the capacity to prepare and define Mali's position in international negotiations related to the protection of personal data and represent Mali before international and regional organisations in this domain.

Articles 36, 37 and 38 provide additional measures of autonomy and independence to the Mali DPA including: the power to report directly to the Prime Minister on a yearly basis and publish its report; the non-opposability of its actions; the obligation of public and private sector actors to facilitate its work; and immunity against personal lawsuits for actions carried out as part of official duties.
Review of the Application for Member Status of the Cybercrime Advisory Council of Nigeria to the International Conference of Data Protection and Privacy Commissioners

Following an assessment of the application received on 17 July 2016 and other information provided in support, our Office believes that the Cybercrime Advisory Council of Nigeria (hereinafter the Council) does not meet the requisite criteria to be granted member status.

It is suggested that the Executive Committee offer the Council to attend the Marrakech Conference as an Observer and that this recommendation be put to the full membership of the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

Analysis

In accordance with article 5.1 of the Rules and Procedures of the ICDPPC, we are satisfied that the Council:

f. Is a public entity, created by an appropriate legal instrument based upon legal traditions of the country or international organization which it belongs to

The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 of Nigeria (the "Act") establishes the legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. Section 42 of the Act establishes the Cybercrime Advisory Council.

We are not, however, satisfied that the Council:

g. Has the supervision of the implementation of the legislation on the protection of personal data or privacy as one of its principal regulatory mandates

The Council is the body established to provide recommendations to the Executive on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria, as well as to formulate and provide general policy guidelines for the implementation of the Act. Although the Act's objectives include the protection of privacy rights, neither privacy nor data protection figure prominently in the Act's provisions or in the Council's jurisdiction.

In our opinion, the protection of personal data and privacy do not constitute one of the Council's principal regulatory mandates

h. Operates under a legislation that is compatible with the principal international instruments dealing with data protection or privacy

The Council's application notes that it implements the Economic Community of West African States (ECOWAS) Supplementary Act A/SA.1/01/10 on Personal Data (the ECOWAS Supplementary
We observe, however, that most elements of that Supplementary Act are absent from the Act and data protection and privacy do not form a central or important component of the Act.

**i. Has an appropriate range of legal powers to perform its functions**

Article 43 specifies the functions and powers of the Council. These include the formulation of policy, the provision of advice and recommendations on issues related to cybersecurity and computer related offences. The Council, as its name suggests is advisory in nature and not a privacy or data protection authority in the sense stipulated in the ICDPPC Rules and Procedures.

**j. Has appropriate autonomy and independence**

The Council is comprised of 29 representatives from numerous public Ministries and Agencies and some civil society and non-governmental representatives. The Act does not specify how representatives from the Ministries and Agencies are appointed, but it does stipulate that they cease to hold office if "the President is satisfied that it is not in the public interest for the person to continue in office as a member of the Council." Meetings of the Council are convened and presided by the National Security Adviser. These provisions point to a lack of appropriate autonomy and independence on the part of the Council.

All this said, in its application the Council observes that it "is engaging with stakeholders to harmonise the various draft bills on data protection for presentation to the National Assembly for enactment." When and if such legislation is in force, the body overseeing its implementation – provided it has an appropriate range of legal powers and appropriate autonomy and independence – should consider membership in the ICDPPC.

Review of the Application for Member Status of the Office of Privacy and Data Protection of the State of Washington (USA) to the International Conference of Data Protection and Privacy Commissioners

Following an assessment of the application received on 4 August 2016 and other information provided in support, our Office believes that the Office of Privacy and Data Protection of the State of Washington, USA (the OPDP) does not meet the requisite criteria to be granted member status. Nevertheless, on the basis of the analysis below, it is suggested that the Executive Committee offer the OPDP Observer Status for three years and that this recommendation be put to the full membership of the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

Analysis

In accordance with article 5.1 of the Rules and Procedures of the ICDPPC, we are satisfied that the Office of Privacy and Data Protection of the State of Washington:

k. Is a public entity, created by an appropriate legal instrument based upon legal traditions of the country or international organization which it belongs to

The Office of Privacy and Data Protection was created by Substitute House Bill 2875 – an Act Relating to establishing the office of data privacy (the “Data Privacy Act”) – which passed both chambers of the Washington State legislature and has been in effect since June 9, 2016. The OPDP is created “within the office of the state chief information officer.”

l. Has appropriate autonomy and independence

The Chief Privacy Officer (CPO) of the State of Washington is appointed by the state’s Chief Information Officer in consultation with the Governor. There is no term limit for the CPO, who is a full time state employee. The CPO can only be removed “for cause” under local law. The OPDP has the power to advise government branches and agencies, but it is unclear whether this involves issuing public reports beyond those relating to its performance (Section 2 (5) of the Data Protection Act. The OPDP is quite young, but has already spoken publicly on matters of concern, which speaks positively to its ability to act autonomously and independently.

We are not, however, satisfied that the OPDP:

m. Has the supervision of the implementation of the legislation on the protection of personal data or privacy as one of its principal regulatory mandates

CPO Alex Alben’s thoughts on the encryption battle of Apple and the FBI.
Section 2 of the Data Privacy Act states that the OPDP's purpose "is to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection." As such, the OPDP has an advisory role, and not a supervisory one, in terms of data privacy and data protection in the State of Washington.

Operates under a legislation that is compatible with the principal international instruments dealing with data protection or privacy. The OPDP application notes that the Data Privacy Act does not implement any international instrument dealing with data protection or privacy, but notes call for the Chief Privacy Officer for Washington State to coordinate with international bodies regarding the state privacy law.

The Data Privacy Act prescribes the duties of the OPDP and its administrative reporting obligations to the State of Washington legislature. It does not set out privacy principles or rules, failing to lay a basis for comparing its compatibility with international data protection or privacy instruments.

Section 2 (3) of the Data Protection Act lays out the OPDP's duties, which include:

- Conducting an annual privacy review;
- Conducting annual privacy training for state agencies and employees;
- Articulating privacy principles and best practices;
- Coordinating data protection in cooperation with the agencies; and
- Participating in the review of major state agency projects involving personally identifiable information.

Section 2 (4) also gives the OPDP duties in terms of being a resource for state employees and the public on data privacy and protection by developing and promoting best practices and having an educational role.

The OPDP does not have powers related to compliance, investigation, redress or any other supervisory powers with legal or administrative consequence.