36th International Conference of Data Protection and Privacy Commissioners

Resolution

Accreditation

The Executive Committee proposes that the 36th International Conference of Data Protection and Privacy Commissioners grants accreditation to the authorities listed below for the reasons explained in the Explanatory Note.

1. **Membership**
    a. **Bremen (Germany)** Die Landesbeauftragte für Datenschutz und Informationsfreiheit (The State Commissioner for Data Protection and Freedom of Information, LDI)
    b. **Ghana** Data Protection Commission (GDPC)
    c. **Senegal** La Commission de Protection de Données Personnelles (Commission of Personal Data Protection, CDP)

2. **Observer Status**
    a. **Bermuda** Ministry of Education and Economic Development Department ofE-Commerce
    b. **Japan** Specific Personal Information Protection Commission (SPIPC)
    c. **State of Mexico (Mexico)** Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Transparency, Public Information Access and Personal Data Protection Institute, INFOEM)
    d. **Singapore** Infocomm Development Authority (IDA)
    e. **United States** Commodity Futures Trading Commission (CFTC)

Explanatory Note

This year, the Executive Committee received three applications for accreditation before the deadline of 21 June 2014. The Senegalese Data Protection Commission has applied for membership. The Japan Specific Personal Information Protection Commission and the United States Commodity Futures Trading Commission both applied for observer status. Shortly after the deadline, an application for membership was received from the Ghana Data Protection Commission. Shortly before the Conference, the Executive Committee received observer applications from the Bermuda Ministry of Education and Economic Development Department of E-Commerce and the Singapore Infocomm Development Authority, and a membership application from the State of Mexico Transparency, Public Information Access and Personal Data Protection Institute. Due to time constraints, the Executive Committee will consider the application from the State of Mexico as an observer applicant, deferring full consideration for the 2015 Conference.

Furthermore, the Executive Committee still needed to assess the membership application received in 2013 from the Bremen State Commissioner for Data Protection and Freedom of Information, which was submitted too late to be taken into account for the Warsaw Closed Session.

1. **Applications for Accreditation as Member**

Upon review of the applications received and consideration of the legislative instruments and other documents provided as background information, the Executive Committee recommends that the Bremen State Commissioner for Data Protection and Freedom of Information (Germany), the Ghana Data Protection Commission, and the Senegalese Commission of Personal Data Protection be granted Member status to the Conference. The Executive Committee is satisfied that each of these authorities meets the requisite conditions for accreditation; notably that they:

- are public entities, created by an appropriate legal instrument based upon legal traditions of the country or international organization which they belong to;
- have the supervision of the implementation of the legislation on the protection of personal data or privacy as one of their principal regulatory mandates;
- operate under a legislation that is compatible with the principal international instruments dealing with data protection or privacy;
- have an appropriate range of legal powers to perform their functions; and
- have appropriate autonomy and independence.

2. **Applications for Accreditation as Observer**

The Executive Committee recommends that the Bermuda Ministry of Education and Economic Development Department of E-Commerce, Japan Specific Personal Information Protection Commission, Singapore Infocomm Development Authority, and the United States Commodity Futures Trading Commission be granted Observer status to the conference, insofar as they are

public entities involved in dealing with the protection of personal data. Additionally the Executive Committee recommends that the State of Mexico Transparency, Public Information Access and Personal Data Protection Institute (Mexico) be granted observer status until its membership application can be reviewed for the 2015 Conference.

Background information on the new members and observers

The Bremen State Commissioner for Data Protection and Freedom of Information is a public entity headed by a Commissioner and created by an Act of Parliament of the German State of Bremen through the Data Protection Law, last amended in 2013(Chapter 4). The power to revoke this law also rests with Parliament. The Commissioner is appointed by the Bremen parliament upon nomination by the Senate, for the duration of 8 years. No possibilities to remove the Commissioner from office are foreseen. All personnel required to carry out the tasks of the State Commissioner should be provided.

The Ghana Data Protection Commission is a public entity created by Article 1 of the Ghana Data Protection Act 2012. Its main task is to supervise the implementation of the provisions of the Data Protection Act. The Commission has various supervisory powers and is in a position to enforce the provisions of the law. Additionally the Commission can engage in public education and maintains the data protection register.

The Senegalese Commission of Personal Data Protection is a public entity created by Chapter II of the Senegalese data protection law. The members of the Commission are appointed for renewable terms of four years and may not be removed from office. The Commission has various powers including those related to compliance, approvals, sanctions and guidance.

The Bermuda Ministry of Education and Economic Development Department of E-Commerce is concerned with the technology, e-business and e-commerce agenda Bermuda and its strategic development, ensuring that the appropriate legislative and policy framework is in place for both business and citizens. The Department is currently developing privacy and data protection legislation for Bermuda.

The Singapore Infocomm Development Authority (IDA) promotes the adoption of information and telecommunications technology. As the Chief Information Officer for the Singapore Government, IDA is responsible for master planning, project-managing and implementing various systems and capabilities for the government. The Next Generation Trusted Infrastructure Team in IDA has the responsibility of exploring new technologies in protecting personal data and privacy. The team works in tandem with Personal Data Protection Commission of Singapore on technologies that support data privacy.

The Japan Specific Personal Information Protection Commission (SPIPC) is an independent supervisory authority established on January 1, 2014, under the Number Use Act promulgated on May 31, 2013. The SPIPC is responsible for taking necessary measures in order to ensure the proper handling of Personal Number and other Specific Personal Information (personal information that includes Personal Number). The SPIPC promotes Privacy Impact Assessments (PIAs); publishes guidelines for proper handling of Specific Personal Information; and supervises government agencies, incorporated administrative agencies, and local governments.

The State of Mexico Transparency, Public Information Access and Personal Data Protection Institute (INFOEM) has jurisdiction over personal data protection in the public sector. The INFOEM's functions include compliance, approvals and redress. The INFOEM is constituted under the Transparency and Public Information Access Law of the State of Mexico and municipalities and the Personal Data Protection Law of the State of Mexico.

The United States Commodity Futures Trading Commission (CFTC) is an independent financial supervisory authority within the U.S. executive branch. The CFTC's responsibility includes promoting and enhancing the privacy rights of individuals involved in the financial markets the CFTC supervises. For example, the CFTC has adopted "red flags" rules requiring programs to identify and address the risk of identity theft to protect customers. Additionally, the CFTC adopted a rule regarding the proper disposal of consumer information, requiring reasonable measures to protect against unauthorized access or use of the information.