ACCREDITATION FEATURES OF DATA PROTECTION AUTHORITIES ADOPTED ON SEPTEMBER 25, 2001 DURING THE 23RD INTERNATIONAL CONFERENCE OF DATA PROTECTION COMMISSIONERS HELD IN PARIS, 24-26 SEPTEMBER, 2001

This paper establishes a process and criteria for recognising the credentials of data protection authorities for the purposes of the international Conference. It is set out in three parts:

(A) criteria and rules for a credentials committee;
(B) accreditation principles;
(C) addendum to guidelines and procedures for Conference resolutions adopted at the 22nd Conference.

A. CRITERIA AND RULES FOR CREDENTIALS COMMITTEE

1. Credentials committee

There will be a credentials committee ("the committee") to consider applications from data protection authorities ("authorities") that wish to be accredited to participate in the International Conference of Privacy and Data Protection Commissioners ("the Conference"). The committee will keep these criteria and rules, and the accreditation principles, under review and, if warranted, recommend change to the Conference.

2. Membership

The committee is composed of three members.
The initial committee will be selected by participants in the closed session of the 23rd Conference in Paris.
Thereafter members will be selected from participating accredited authorities only. In doing so the participants should have regard to the desirability of diversity in the committee membership between legal systems, geographical areas and size of jurisdiction.
The committee may not contain more than 1 member from the same country at any time.

3. Co-option

To fill vacancies occurring between Conferences the committee may co-opt a member or members (not exceeding 2) from accredited authorities.

4. Applications for accreditation

Any authority that wishes to be accredited must write to the committee explaining its case in terms of the accreditation principles. Applications should be made at least 3 months before the annual Conference.

The committee will offer a recommendation to the Conference in respect of each application received and will propose a resolution to recognise the credentials of each approved authority within a national or sub-national category.

Comment: Authorities would have to meet one of the following criteria, be:

- *A national authority;*
- *An authority operating within a limited sub-national territory (typically a state, province, canton or land in a federal country);*
- *An authority within an international or supranational body.*

The committee may be requested to consider the credentials of authorities having narrower functions than otherwise acceptable for accreditation, typically operating within a specific area of activity (such as medical privacy) or performing just one kind of function (e.g. solely a complaints or advisory body) which may, at the discretion of the host of the Conference, be entitled to attend as observers but without the right to vote.

5. Committee procedure

The Committee may adopt whatever procedure it deems appropriate.

6. Term

The normal term for committee members is 2 years. Co-opted members serve only until the following Conference. No member may serve consecutively for more than 4 years.

7. Costs

Members will bear their own costs.

8. Reviews of accreditation

The committee may, at the request of any accredited authority, review the position of any previously accredited authority and offer a recommendation as to whether that accreditation should be continued.

B. ACCREDITATION PRINCIPLES

Accredited data protection authorities will, by virtue of their broad functions and depth of experience, be the premier experts on the principles and practice of data protection and privacy in their jurisdiction. They will have the clear mandate to promote and protect data protection and privacy across a wide sphere of activity and all the necessary legal powers to carry out the task.

1. Legal basis

The data protection authority must be a public body established on an appropriate legal basis.

Comment: The legal basis upon which an authority is established underpins its independence and ability to perform functions and demonstrates a jurisdiction's commitment to effective protection of personal data. The legal basis should be of the type normally associated with significant public bodies dealing with citizens' rights in that jurisdiction. Typically this will be primary legislation enacted by the legislature, such as a statute, but depending upon local traditions a suitable Executive instrument may be appropriate. The legal basis should be transparent and have sufficient permanence that it cannot be revoked or changed without reference to the legislature.

2. Autonomy and independence

The data protection authority must be guaranteed an appropriate degree of autonomy and independence to perform its functions.

Comment: Autonomy requires that an authority be empowered, both in a legal and practical fashion, to initiate and undertake appropriate action without having to seek others' permission. Independence is important for agencies to be able to operate free from political or governmental interference and to withstand the influence of vested interests. Typical guarantees include:

- *appointment for a fixed term;*
- *removal only for inability to perform the office, neglect of duty, or serious misconduct;*
- *the power to report directly to the head of government or legislature and to speak publicly on matters of concern;*
- *immunity against personal law suit for actions carried out as part of official duties;*
- *power to initiate investigations.*

3. Consistency with international instruments

The law under which the authority operates must be compatible with the principal international instruments dealing with data protection and privacy.

Comment: The principal international instruments are the OECD Guidelines (1980), Council of Europe Convention No 108 (1981), UN Guidelines (1990) the EU Directive (1995), and, as far as they are relevant, the UN Principles relating to the Status and Functioning of National Institutions for the Protection and Promotion of Human Rights (1991).

4. Appropriate functions

The authority must have an appropriate range of functions with the legal powers necessary to perform those functions.

Comment: A data protection authority will have a range of functions in areas such as compliance, supervision, investigation, redress, guidance and public education. An authority must not merely be advisory but must have supervisory powers with legal or administrative consequence.

C. ADDENDUM TO GUIDELINES AND PROCEDURES FOR CONFERENCE RESOLUTIONS

At the 22nd Conference held in Venice in September 2000, commissioners adopted guidelines and procedures for Conference resolutions. The following addendum to the earlier resolution is adopted for future resolutions.

1. At the 24th International Conference the meeting of authorities shall first consider and approve or reject such recommendation as may be made by the Credentials Committee. Thereafter, resolutions may only be proposed and supported by accredited authorities (whether operating at the national or sub-national level).

2. From the 24th International Conference only accredited authorities may vote on any resolution. A resolution can only be adopted when a majority of accredited authorities entitled to vote are present. As far as possible resolutions will be adopted by consensus rather than through a formal vote. When voting is necessary, only one vote may be cast on behalf of any country, and the resolution is adopted by simple majority of the countries present at the Conference. Where more than one delegate from any country is present at the Conference, the vote is to be cast by the national authority that must first consult the sub-national authorities of this country, which have in any case the possibility to make their positions known. If the national authority is not represented, the sub-national authorities of this country that are present at the Conference may agree how the vote is to be cast. Failing agreement the vote is forfeited. Authorities within an international or supranational body which have been duly accredited may attend and participate in meetings but will not be entitled to vote unless the conference has specially decided to grant them voting rights at the time of accreditation.

3. Resolutions proposed by the credentials committee for recognition of data protection authorities are to be circulated in advance of the Conference within the period of time provided in the guidelines and procedures for Conference resolutions adopted on September 29, 2000 in Venice. However in case of urgency the Conference may waive this requirement.