

APPLICATION FORM FOR ACCREDITATION AS A DATA PROTECTION AUTHORITY

Application to the Credentials Committee for accreditation as a data protection authority pursuant to the resolutions adopted at the 23rd International Conference of Data Protection and Privacy Commissioners at Paris on 25th September 2001.

Notes:

- (a) Please complete application in French or English.
- (b) Please keep answers brief and to the point.
- (c) Please ensure that all 33 questions are answered
- (d) If you retype the form, please include the numbered questions with your answers. It is possible to avoid such retyping by getting the electronic application form in French or in English upon request by e mail at credentials@privacy.org.nz.

Details of applicant

1. Name and postal address of authority

Data Protection Ombudsman The Office of the Data Protection Ombudsman P.O. Box 315 FIN-00181 HELSINKI Finland

2. Contact person for this application:

(a) Name

Data Protection Ombudsman Reijo Aarnio
--

(b) Email address

Reijo.Aarnio@om.fi

(c) Direct telephone number

+358 9 2511 2301

(d) Fax contact

+358 9 2511 2301

Type of application

3. The application is for accreditation as:

- (a) national Authority YES
- (b) sub-national Authority NO
- (c) Authority within an international, if yes which one..... NO

Description of applicant

4. Description of Authority (e.g. commissioner, commission, board etc)

Data Protection Ombudsman and Data Protection Board.

5. Is the Authority a public body? YES

6. Geographical jurisdiction

Finland

7. Sectoral coverage (i.e. does the applicant's jurisdiction cover the entire public and private sectors? If only part of a sector or if there are significant activities not covered, please specify)

The jurisdiction of the Data Protection Ombudsman and the Data Protection Board covers the entire public and private sectors in Finland.

8. Is the role of the Authority mainly concerned with data protection and privacy?
YES

Legal basis

9. Title of law under which the Authority is constituted

The Authority is constituted under the Act on the Data Protection Board and the Data Protection Ombudsman and its competence is determined in the Personal Data Act.

10. Is this principally a data protection law? YES
The Personal Data Act is principally a data protection law.

11. Status of the law (e.g. statute, regulation, executive order)

The Personal Data Act and the Act on Data Protection Board and Data Protection Ombudsman are acts. The latter is supplemented by a decree on the Data Protection Board and the Data Protection Ombudsman.

12. Which body made the law?

The Parliament of Finland

13. What body has the power to amend or revoke the law?

The Parliament of Finland

Autonomy and independence

14. Who appoints member(s) of the Authority? (Please explain if a different process applies to the presiding member from other Authority members in this question and in subsequent questions.)

The Data Protection Ombudsman and the Data Protection Board are appointed by the Finnish Government. The Secretary of the DPB and the Head of the Office for the DPO are appointed by the Ministry Of Justice. The staff of the Office for the DPO is appointed by the DPO.

15. What process is followed?

The DPO is appointed by the Finnish Government for the five year period without announcing the office open

16. For what term are appointments made?

Data Protection Ombudsman – 5 yrs
The members of the Data Protection Board – 3 yrs

17. Does the law under which the Authority operates explicitly state that it acts independently?

No, but it is stated in the Government's proposal for the Personal Data Act. An explicit statement was considered no to be needed, since the directive has binding effects.

18. May the member(s) be removed before expiry of their term? YES

19. If yes, who may remove members of the Authority before expiry of their term?

The instance that has appointed the authority (ie. the Finnish Government for the DPO)

20. Are there limited reasons specified in the statute, or in another law, providing the permitted grounds for removal?

The reasons for removal are specified in the Act on State Office Holders.

21. What are the grounds for removal?

Serious default of official duties or other especially strong cause.

22. Does the Authority possess the following powers (briefly describe and give statutory references)

(e) to initiate an investigation with seeking provision YES

details: The DPO and DPB shall follow the legislation on privacy and data protection and initiate provisions if needed. (Sections 2(2) and 5(2) of the Act on the DPB and the DPO)

- (f) to report to the head of State, head of Government or legislature YES

details: The authority concerned shall reserve the DPO an opportunity to be heard in connection with the drafting of legislative or administrative reforms relating to the protection of personal rights of freedoms in the processing pf personal data. (Section 41 of the Personal Data Act)

- (g) make public statements YES

details: The DPO shall make public statements concerning his sphere of authority (Section 5(3)of the Act on the DPB and the DPO).

23. Does the Authority (and its staff) have immunity from legal suit for actions performed in the course of their duties?

No.

24. Applicants may list any other measures set out in the statute or in other laws which guarantee the Authority's independence (for example if the law provides specifically that the Authority's finances are protected).

-

Consistency with international instruments

25. Does the Authority explicitly implement any international instrument (for example if the law under which the Authority operates specifies that it implements such international instrument)? YES

If "yes", which of the following does it principally implement?

- | | | |
|-----|--|-----|
| (a) | OECD Guidelines (1980) | YES |
| (b) | (i) Council of Europe Convention No 108 (1981) | YES |
| | (ii) Council of Europe Additional Protocol (8 November 2001) | YES |
| (c) | UN Guidelines (1990) | YES |
| (d) | EU Directive (1995) | YES |

26. Does the law instead, or additionally, implement any general or specific international instrument? (If so, list the international body and the instrument)

No.

27. Have significant questions been raised about the extent to which the law is consistent with the international instruments which are claimed to be implement in answer to questions 25 and 26? (Applicants should supply further information to assist the Committee including a description of any measures under way to address these inconsistencies.)

No.

Appropriate functions

28. Does the Authority possess functions in any of the following areas (briefly describe and give statutory references):

- (a) compliance (e.g. audit, inspection) YES

details: The DPO and the DPB have the right of access to personal data which are being processed as well as information necessary for the supervision of the legality of the processing of personal data. (Section 39 of the Personal Data Act)

- (b) approvals (e.g. prior-checking, notification) YES

details: The controllers have to notify the DPO of automated data processing of personal data in circumstances defined by the act by sending a description of the file. Also transfer of personal data to a third country has to be notified in certain cases. (Section 36)

- (c) redress for individuals (e.g. complaints, conciliation enforcement) YES

details: The DPO shall decide matter brought to his attention by data subjects concerning realisation of the right of access or rectification of an error. The DPO may order a controller to realise the right of access of the data subject or to rectify an error. (Section 40)

- (d) sanctions available to Authority (for example, prosecution and enforcement) YES

details: Where necessary, the DPO may refer the matter to be dealt with by the DPB or report it for prosecution. The DPB may prohibit unlawful processing of personal data, compel the person to remedy an instance of unlawful conduct or neglect or order the operation pertaining to the file to be ceased. The DPO and the DPB also have the right to impose a threat of a fine. (Sections 40, 44 and 46)

- (e) guidance (e.g. compliance advice) YES

details: The DPO provides direction and guidance on the processing of personal data (Section 38)

- (f) public education YES

details: The DPO promotes good processing practice and issues directions and guidelines. (Section 40)

- (g) policy advice for government YES

details: The authority concerned shall reserve the DPO an opportunity to be heard in connection with the drafting of legislative or administrative reforms relating to the protection of personal rights of freedoms in the processing of personal data. (Section 41)

- (h) studies or research (e.g. into developing technologies, privacy issues) YES

details: The DPO eg. assists controllers in drafting sectoral codes of conduct. (Section 42) and may issue more detailed guidelines on how personal data is to be secured against unlawful processing (Section 40)

Additional comments

29. Applicants are invited to offer any further comments that they wish.

Other materials

30. List any attachments which will accompany the application as an electronic attachment or to follow by post.

Personal Data Act and its amendment are sent with the application as an electronic attachment.

31. If law under which the Authority operates is accessible on the Internet, please give the reference

URL: www.tietosuoja.fi/1560.htm (The Personal Data Act and its amendment)

32. If a recent annual report of the Authority (or a similar recent publication outlining typical activities) is available on the Internet, please give the reference

URL: The DPO's Year in Review 2000 is available at www.tietosuoja.fi

Research use

33. With the consent of applicants, the Committee proposes to make copies of the applications available to appropriate researchers approved by the Committee to facilitate a study on data protection. Please indicate whether you agree to this use:

- I agree to this application being released to a researcher YES

Making the application

The application should be emailed to the credentials committee at credentials@privacy.org.nz

If sent as an email attachment it should be in M/S Word.

If unable to email the application, it should be posted to:

Credentials Committee
C/- Privacy Commissioner
P O Box 466
Auckland
New Zealand

The Committee needs access to a copy of the law under which the Authority is constituted. This need not be supplied in hard copy if it is available on the Internet and listed at question 31. If the law itself is not in English or French, it will be useful to supply an English or French summary or translation if one exists.

Use of information

The information in this form will be used for processing the application and will be disclosed to members of the committee and their staff (being the commissioners from New Zealand, France and the United Kingdom) and future committees. It may be also disclosed also to the Data Protection Authorities which participate to the international conference and approved researchers. Any personal data contained in the form is available for access and correction in accordance with the applicable data protection laws of current and future committees. In the first instance it is subject to the New Zealand Privacy Act 1993.

ACCREDITATION OF DATA PROTECTION AUTHORITY
CHECKLIST FOR THE CREDENTIALS SUB-GROUP

1 Name of Authority

Data Protection Ombudsman, Finland

2 Does the authority have clear and wide ranging data protection functions covering a broad area of economic activity (eg not just an advising body or a body operating in a narrow field such as medical privacy)?

Yes

Notes

The application is for the DP Ombudsman and it seems appropriate to grant accreditation in that name. However, the application does speak also of the DP Ombudsman and the DP Board. The DPO has clear and wide ranging data protection functions but the Finnish law allocates some powers to the DP Board.

It seems correct to say that the Finish authority included both institutions. The accreditation can be granted to the Ombudsman who is in relation with the board

3 Legal Basis.

Is the authority a public body established on an appropriate legal basis (eg by statute or regulation)?

Yes

Notes

4 Autonomy and Independence?

Is the authority guaranteed an appropriate degree of autonomy and independence to perform its functions (eg the power to make public statements and protection from removal from office)?

Yes

Notes

5 Consistency with International Instruments.
Is the law under which the authority operates compatible with at least one of the international instruments dealing with data protection and privacy (eg EU Directive, OECD Guidelines, Council of Europe Convention)?

Yes

Notes
While EU Directive would appear to be principal instrument, claimed implementation also of OECD, CoE and UN instruments.

6 Appropriate Functions.
Does the authority have an appropriate range of functions with the legal powers necessary to perform those functions (eg the power to receive and investigate complaints from individuals without seeking permission)?

Yes

Notes
Some functions performed by DP Board constituted under same law.

7 Does the Sub-group recommend accreditation?

Yes

Notes

8 If accreditation is recommended what is the accreditation as?

Not applicable

Notes

9 If accreditation is as an authority within an international/supranational body does the recommendation include voting rights?

Not applicable

Notes

10 If accreditation is not recommended does the Sub Group recommend that accreditation is refused or is more information needed before a decision can be made?

Not applicable

Notes

11 If accreditation is not recommended and the application is from an authority with narrow functions does the Sub Group recommend that, at the discretion of the conference host, observer status is granted?

Notes

Not applicable

If more information is required what is this:

Signed on behalf of the Sub-group:

Blair Stewart

Date: **22 May 2002**

Marie Georges

Date: 9 juillet 2002

Date:

Note: 2 signatures required for recommendations for accreditation.
3 signatures required for recommendations for refusal