

English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

Ordinance on Data Protection Certification (DPCO)

of 28 September 2007 (Status as of 1 January 2008)

The Swiss Federal Council,

based on Article 11 paragraph 2 of the Federal Act of 19 June 1992¹
on Data Protection (FADP),

ordains:

Section 1: Certification Organisations

Art. 1 Requirements

¹ The organisations that carry out data protection certification in accordance with Article 11 FADP (certification organisations) must be accredited. Accreditation is governed by the Accreditation and Designation Ordinance of 17 June 1996², unless the present Ordinance provides otherwise.

² Separate accreditation is required in each case for the certification of:

- a. the organisation of and procedure for data protection;
- b. products (hardware, software or systems for automated data processing procedures).

³ The certification organisations must have established organisational regulations and an established certification procedure (checking program), in which the following in particular are regulated:

- a. the assessment or checking criteria and the resultant requirements that must be fulfilled by the organisations or products to be certified (assessment and/or checking scheme); and
- b. the details of the procedure, and in particular the course of action in the event that irregularities are detected.

AS 2007 5003

¹ SR 235.1

² SR 946.512

⁴ The minimum requirements for the checking program are governed by the standards and principles applicable in accordance with Annex 2 of the Accreditation and Designation Ordinance of 17 June 1996 and in accordance with Articles 4–6 hereof.

⁵ The minimum qualification requirements for the staff that carry out certification procedures are set out in the Annex.

Art. 2 Accreditation procedure

The Swiss Accreditation Service shall consult the Federal Data Protection and Information Commissioner (the Commissioner) on the accreditation procedure and the follow-up inspection as well as on the suspension or the withdrawal of accreditation.

Art. 3 Foreign certification organisations

¹ The Commissioner, in consultation with the Swiss Accreditation Service, shall recognise foreign certification organisations as being qualified to carry out their activities on Swiss territory provided they are able to prove that they hold an equivalent qualification to that required in Switzerland.

² The certification organisations must in particular provide proof that they fulfil the requirements of Article 1 paragraphs 3 and 4 and that they have adequate knowledge of Swiss data protection legislation.

³ The Commissioner may place a time limit on recognition and make it subject to conditions or requirements. He shall withdraw recognition if essential conditions or requirements are not fulfilled.

Section 2: Subject Matter and Procedure

Art. 4 Certification of organisation and procedure

¹ The following may be certified:

- a. any data processing procedures for which an organisation is responsible;
- b. individual, separately definable data processing procedures.

² The subject matter of the assessment is the data protection management system. This includes in particular:

- a. the data protection policy;
- b. the documentation on objectives and measures relating to the guarantee of data protection and data security;
- c. the organisational and technical measures for the achievement of the goals and measures laid down, and in particular the measures to rectify any irregularities detected.

³ The Commissioner shall issue guidelines on the minimum requirements for the data protection management system. In doing so, he shall take account of international standards relating to the construction, operation, monitoring and improvement of management systems, and in particular the standards ISO 9001:2000 and ISO 27001:2005.

⁴ The exemption from the obligation to register data files in accordance with Article 11a paragraph 5 letter f FADP is only applicable if all data processing procedures that apply to a data file are certified.

Art. 5 Certification of products

¹ Products may be certified if their primary purpose relates to the processing of personal data or their use results in the generation of personal data, and in particular data on the user.

² The subject matter of the assessment is in particular the guarantee inherent to the product:

- a. of the confidentiality, integrity, availability and authenticity of the processed personal data taking account of the purpose of the product;
- b. of the avoidance of the unnecessary generation, storage or other processing of personal data taking account of the purpose of the product;
- c. of the transparency and comprehensibility of the automated processing of personal data that results from the functionality of the product determined by the manufacturer;
- d. of technical measures to support the user in complying with data protection requirements and obligations under data protection law.

³ The Commissioner shall issue guidelines by 1 January 2010 at the latest on which specific data protection criteria must as a minimum be assessed in terms of the product certification procedure.

Art. 6 Grant and validity of certification

¹ The certificate is granted if the certification procedure based on the assessment or checking criteria applied by the certification organisation establishes that the requirements under data protection law as well as the requirements imposed by this Ordinance and the guidelines issued by the Commissioner (Art. 4 para. 3 and 5 para. 3) or any other equivalent standards are fulfilled. Certification may be made subject to conditions or requirements.

² The certification of a data protection management system is valid for three years. The certification organisation must conduct an annual summary review of whether the requirements for certification continue to be fulfilled.

³ The certification of a product is valid for two years. A product must be certified again as soon as any fundamental changes are made thereto.

Art. 7 Recognition of foreign data protection certification

The Commissioner in consultation with the Swiss Accreditation Service shall recognise foreign certifications provided a guarantee is given that the requirements of the Swiss legislation are fulfilled.

Art. 8 Notification of the result of the certification procedure

¹ If a certified organisation notifies the Commissioner that it has successfully undergone the certification procedure in accordance with Article 4 in order to be exempted under Article 11a paragraph 5 letter f FADP from the obligation to register its data files, it must submit the following documents on request:

- a. the assessment report;
- b. the certification documents.

² If the certification organisation in the course of its monitoring activities detects substantial changes in conditions for certification, for example relating to the fulfilment of conditions or requirements, the certified organisation must notify the Commissioner of this.

³ The Commissioner shall publish a list of organisations that have been certified and are relieved of the obligation to register their data files (Art. 28 para. 3 of the Ordinance of 14 June 1993³ to the Data Protection Act). In particular, this list provides information on the term of validity of the certification.

Section 3: Sanctions**Art. 9** Suspension and withdrawal of the certification

¹ The certification organisation may suspend or withdraw certification, in particular if it establishes serious irregularities in the course of an inspection (Art. 6 para. 2). A serious irregularity is constituted in particular where:

- a. essential requirements for data protection certification are no longer fulfilled; or
- b. a certificate is being used in a misleading or unlawful manner.

² In the event of any dispute in relation to the suspension or the withdrawal, the assessment and the procedure for the case are governed by the provisions of civil law that are applicable to the contractual relationship between the certification organisation and certified organisation.

³ The certification organisation shall notify the Commissioner of the suspension or the withdrawal the data protection certification provided the Commissioner has been notified of certification in accordance with Article 8 paragraph 1.

³ SR 235.11

Art. 10 Procedure in the case of supervisory measures by the Commissioner

¹ If the Commissioner detects serious irregularities in the supervisory activity in accordance with Article 27 or 29 FADP in the case of a certified organisation, he shall notify the certification organisation thereof.

² The certification organisation shall immediately arrange for the certified organisation to rectify the irregularity within 30 days of receipt of notification from the Commissioner.

³ If the certified organisation fails to rectify the irregularity within this time, the certification organisation shall suspend the certification. If there is no prospect of the lawful position being established or restored within a reasonable time, certification must be withdrawn.

⁴ If within the period in accordance with paragraph 2 the certified organisation fails to rectify the irregularity and the certification organisation does not suspend or withdraw certification, the Commissioner shall issue a recommendation in accordance with Article 27 paragraph 4 or Article 29 paragraph 3 FADP to the certified organisation or to the certification organisation. He may in particular recommend that the certification organisation suspend or withdraw the certification. If he issues the recommendation to the certification organisation, he must notify the Swiss Accreditation Service.

Section 4: Commencement**Art. 11**

This Ordinance comes into force on 1 January 2008.

Annex
(Art. 1 para. 5)

Minimum Qualification Requirements for Staff at Certification Organisations that conduct Certification Procedures

1 Certification of Data Protection Management Systems

The certification organisation must provide proof that its staff who certify data protection management systems when taken together hold the following qualifications:

- knowledge of data protection law: proof is required of a minimum of two years' practical experience in the field of data protection or a successfully completed course of studies at a university or university of applied sciences of a minimum of one year in duration with data protection law as the main subject;
- knowledge of the field of information technology security: proof is required of a minimum of two years' practical experience in the field of information technology security or a successfully completed course of studies at a university or university of applied sciences of a minimum of one year in duration with information technology security as the main subject;
- training as a management systems auditor (in accordance with ISO/IEC-Guide 62 [ISO/IEC 17021:2006]).

The certification organisation must provide proof that it has qualified staff in each of the individual specialist fields. The assessment of data protection management systems by an interdisciplinary team is permitted.

2 Certification of products

The certification organisation must provide proof that its staff who certify products when taken together hold the following qualifications:

- knowledge of data protection law: proof is required of a minimum of two years' practical experience in the field of data protection or a successfully completed course of studies at a university or university of applied sciences of a minimum of one year in duration with data protection law as the main subject;
- knowledge of the field of information technology security: proof is required of a minimum of two years' practical experience in the field of information technology security or a successfully completed course of studies at a university or university of applied sciences of a minimum of one year in duration with information technology security as the main subject;

- specialist knowledge in relation to the product testing (in accordance with ISO/IEC-Guide 65).

The certification organisation must provide proof that it has qualified staff in each of the individual specialist fields. Product testing by an interdisciplinary team is permitted.

