*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 31 August 2022 (Status as of 1 September 2023)

*The Swiss Federal Council,*

on the basis of Article 13 paragraph 2 of the Data Protection Act of 25 September 2020[1] (FADP),

*ordains:*

## Section 1 Certification Bodies

### Art. 1 Requirements

[1] Organisations that carry out data protection certifications in accordance with Article 13 FADP (certification bodies) must be accredited. Accreditation is governed by the Accreditation and Designation Ordinance of 17 June 1996[2] (AccDO), unless the present Ordinance provides otherwise.

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

a. the organisational structure and the procedure (management systems) in connection with data processing;

b. products, in particular data processing systems or programs and hardware, as well as services and processes in connection with data processing.

[3] The certification bodies must have established organisational regulations and an established certification procedure (certification programme).

[4] The minimum qualification requirements for the staff who carry out data protection certifications are set out in the Annex. The certification bodies must prove that they have staff who are qualified in accordance with these criteria.

### Art. 2 Accreditation procedure

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

AS **2022** 569

1 SR **235.1**

2 SR **946.512**

**Art. 3** Foreign certification bodies

[1] Foreign certification bodies that wish to operate on Swiss territory must prove that they hold equivalent qualifications, that they meet the requirements of Article 1 paragraphs 3 and 4 and that they have adequate knowledge of Swiss data protection legislation.

[2] The FDPIC shall consult with the SAS before recognising a foreign certification body.

[3] It may place a time limit on recognition and make it subject to additional requirements.

[4] It shall withdraw recognition if essential conditions or requirements are no longer fulfilled.

## Section 2 Subject Matter and Procedure

**Art. 4** Subject matter of certification

[1] The following may be certified:

a. management systems;

b. products, services and processes.

[2] The certification of management systems may cover the entire system, individual parts of the organisational structure or individual, separable procedures.

[3] The certification of products, services and processes may include the following:

a. products that are primarily used for processing personal data or in the use of which personal data is generated;

b. services or processes that are primarily used for processing personal data or that generate personal data.

**Art. 5** Requirements for the certification programme

[1] In the certification programme, the following must be regulated as a minimum:

a. the checking criteria and the resulting requirements that the items to be certified must meet;

b. the details of the procedure, in particular the course of action in the event that irregularities are detected.

[2] When establishing the certification programme, the following must be taken into account:

a. the personal data to be processed;

b. the electronic infrastructure used to process the personal data;

c. the organisational measures in connection with processing the personal data.

[3] The checking criteria must comply with all the principles set out in Article 6 FADP.

[4] The certification programme must meet the standards applicable in accordance with Annex 2 AccDO[3] and other applicable technical standards.

**Art. 6** Requirements for the certification of management systems

[1] The subject matter of the assessment of management systems is in particular:

a. the data protection policy;

b. the documentation on objectives, risks and measures relating to the guarantee of data protection and data security;

c. the organisational and technical arrangements to be made to achieve the goals and the measures laid down, in particular for rectifying any deficiencies detected.

[2] The FDPIC shall issue guidelines on the minimum requirements for the management system. In doing so, it shall take account of the international requirements relating to the construction, operation, monitoring and improvement of such management systems and in particular the following technical standards[4]:

a. SN EN ISO 9001 quality management systems, requirements;

b. SN EN ISO 27001, information technology, IT security procedures, information security management systems, requirements;

c. SN EN ISO/IEC 27701, IT security procedure, extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management, requirements and guidelines.

**Art. 7** Requirements for the certification of products, services and processes

[1] The subject matter of the assessment of products, services and processes is in particular the guarantee:

a. of the confidentiality, integrity, availability and traceability of the personal data being processed;

b. of avoiding the processing of personal data that is not required in view of the purpose of the product, service or process;

c. of transparency of the processing of personal data;

d. of technical measures to support the user in complying with further data protection principles and obligations under data protection law, in particular with the rights of the data subjects.

[2] The FDPIC shall issue guidelines on any further criteria under data protection law according to which the assessment must be carried out.

3 SR **946.512**

4 The standards mentioned may be viewed free of charge or purchased for a fee at the Swiss Association for Standardization (SAS), Sulzerallee 70, 8404 Winterthur; www.snv.ch

**Art. 8** Grant and validity of data protection certification

[1] The certification body shall certify the management system, the product, the service or the process if the requirements under data protection law and under this Ordinance, the guidelines issued by the FDPIC or other equivalent standards are met. Certification may be made subject to additional requirements.

[2] The certification is valid for three years. The certification body must assess each year whether the requirements are still being met.

**Art. 9** Recognition of foreign data protection certification

The FDPIC in consultation with the SAS shall recognise foreign certifications provided it is guaranteed that the requirements of the Swiss legislation are fulfilled.

**Art. 10** Exemption from the obligation to conduct a data protection impact assessment

A private controller may only dispense with conducting a data protection impact assessment in accordance with Article 22 paragraph 5 FADP if the certification covers the processing that would have to be assessed in the data protection impact assessment.

## Section 3 Sanctions

**Art. 11** Suspension and withdrawal of certification

[1] The certification body may suspend or withdraw certification, in particular if it establishes serious deficiencies in the course of an inspection. A serious shortcoming 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 suspension or withdrawal, the assessment and the procedure for the case are governed by the provisions of civil law applicable to the contractual relationship between the certification body and the manufacturer of the data processing systems or programs, the controller or the processor who has obtained certification.

**Art. 12** Procedure in the case of supervisory measures by the FDPIC

[1] If the FDPIC establishes serious deficiencies in relation to a manufacturer of data processing systems or programs, a controller or a processor that has been certified, it shall notify the certification body.

[2] The certification body shall immediately request the manufacturer of the data processing systems or programs, the controller or the processor to rectify the deficiency within 30 days of the certification body being notified by the FDPIC.

[3] If the deficiency is not rectified within 30 days, the certification body 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 the deficiency is not rectified within the deadline under paragraph 2 and if the certification body has not suspended or withdrawn certification, the FDPIC shall take a measure under Article 51 paragraph 1 FADP. It may in particular order that certification be suspended or withdrawn. If it issues the order to the certification body, it must notify the SAS.

## Section 4 Final Provisions

### Art. 13 Repeal of another enactment

The Ordinance on Data Protection Certification of 28 September 2007[5] is repealed.

### Art. 14 Commencement

This Ordinance comes into force on 1 September 2023.

5 AS **2007** 5003; **2010** 949; **2016** 3447

*Annex*
(Art. 1 para. 4)

# Minimum Qualification Requirements for Staff

## 1 Certification of management systems

The staff who certify management systems must when taken together hold the following qualifications:

- knowledge of the field of data protection law: a minimum of two years' practical experience in the field of data protection or a successfully completed course of studies of a minimum of one year in duration at a university or university of applied sciences with data protection law as the main subject;
- knowledge of the field of information security: a minimum of two years' practical experience in the field of information security or a successfully completed course of studies of a minimum of one year in duration at a university or university of applied sciences with information security as the main subject;
- knowledge of developments in data protection law and in information security;
- training as a management systems auditor which meets the internationally specified requirements of the following standards[6] in particular:
  - SN EN ISO/IEC 17021-1, conformity assessments, requirements for bodies providing audit and certification of management systems, Part 1: Requirements,
  - SN EN ISO/IEC 17021-3, conformity assessment, requirements for bodies providing audit and certification of management systems, Part 3: Competence requirements for auditing and certification of quality management systems, and
  - SN EN ISO/IEC 27006, Information technology, security techniques, requirements for bodies providing audit and certification of information security management systems.

The certification body must have qualified staff for the individual fields. The assessment of management systems by an interdisciplinary team is permitted.

6 The standards mentioned may be viewed free of charge or purchased for a fee at the Swiss Association for Standardization (SAS), Sulzerallee 70, 8404 Winterthur; www.snv.ch

## 2 Certification of products, services and processes

The staff who certify products, services or processes must when taken together hold the following qualifications:

- knowledge of the field of data protection law: a minimum of two years' practical experience in the field of data protection or a successfully completed course of studies of a minimum of one year in duration at a university or university of applied sciences with data protection law as the main subject;
- knowledge of the field of information security: a minimum of two years' practical experience in the field of information security or a successfully completed course of studies of a minimum of one year in duration at a university or university of applied sciences with information security as the main subject;
- knowledge of developments in data protection law and in information security;
- specialist knowledge relating to the certification of products, services or processes that meets the requirements for certification programmes and FDPIC's guidelines as well as the internationally specified requirements, in particular in accordance with the applicable technical standards and the standard «SN EN ISO/IEC 17065[7], Conformity assessment, requirements for bodies certifying products, processes and services».

The certification body must have qualified staff for the individual fields. The assessment of products, services and processes by an interdisciplinary team is permitted.

7 The standards mentioned may be viewed free of charge or purchased for a fee at the Swiss Association for Standardization (SAS), Sulzerallee 70, 8404 Winterthur; www.snv.ch