CNIL CERTIFICATION SCHEME OF DPO SKILLS AND KNOWLEDGE

PRESENTATION

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Presentation of the CNIL certification scheme of DPO skills and knowledge

In order to identify the skills and knowledge of the data protection officers (DPOs), the CNIL has adopted a certification scheme in September 2018.

A new task for the CNIL

The French Data Protection Act, as amended by the Act dated 20 June 2018, provides the CNIL with **a new task** as regards the **certification of persons**. The CNIL can now adopt certification criteria and accredit bodies in charge of issuing such certification.

Following a public consultation, and strengthened by its experience in assisting data protection officers (DPOs), the CNIL has adopted a scheme containing:

- **certification criteria** setting out, in particular, the conditions for admissibility of applications and the list of **17 DPO skills and knowledge required to be certified** (see attached document "Certification criteria"); and

- **accreditation criteria** setting out the requirements applicable to certification bodies wishing to be accredited by the CNIL to certify DPO skills and knowledge on the basis of the criteria adopted by the CNIL (see attached document "Accreditation criteria").

Summary of the public consultation

The public consultation on the framework projects has been carried out from 23 May to 22 June 2018. Nearly **200 contributions** have been received from:

- DPOs or future DPOs;
- data controllers and data processors (companies, professional associations, training organisations, associations, law firms and consulting firms);
- certification bodies.

Contributors represent a diverse range of sectors (banking, public sector, health, education, software publishers, transport, distribution, higher education).

Working meetings have also been held between all three French professional data protection officer associations (ADPO, AFCDP and UDPO), IAPP and approximately ten certification bodies.

This consultation has allowed to improve discussions and to find the most appropriate balance between the skills and knowledge that a DPO must have and professionals' expectations (certification bodies, DPOs, controllers, processors).

Certification of natural persons

Certification is not required to practice as a data protection officer, nor is it required to notify the CNIL of the designation of a DPO. Conversely, it is not necessary to be designated as a data protection officer to apply for certification of DPO skills and knowledge.

This is a **voluntary tool** enabling individuals to prove that they have the skills and knowledge of a DPO as required by the GDPR. As a key player in the compliance with the GDPR, the DPO must indeed possess **expert knowledge of data protection law and practices**. The certificate is a vector of trust both for the organisation recruiting such certified persons as well as for clients, suppliers, employees or agents.

The prerequisites to certification are specified in requirement 1 of the certification criteria.

The CNIL does not deliver DPO skills and knowledge certification. The certification bodies, when accredited by the CNIL, will deliver certificates to individuals who meet the prerequisites and pass the written examination. **Certification will therefore be possible only once the CNIL has issued the first accreditations to certification bodies.** Those interested in this

certification will then be able to approach these certification bodies with a view to be certified.

In July 2019, the CNIL has accredited the first certification body on the basis of the accreditation criteria to deliver DPO skills and knowledge certification on the basis of the CNIL's scheme. The list of accredited certification bodies is available here: https://www.cnil.fr/fr/organisme-agrees

Accreditation of certification bodies by the CNIL

Certification bodies **wishing to issue certification for DPO skills and knowledge based on the CNIL's accreditation framework** can submit an application for accreditation to the CNIL (conditions set out in the FAQ). Such application must meet the requirements set out in the accreditation criteria.

In anticipation of a specific accreditation programme on DPO certification established in collaboration with COFRAC, certification bodies who are willing to candidate for CNIL accreditation must first be accredited by an accreditation body pursuant to standard ISO/CEI 17024:2012 (*Conformity assessment - General requirements for bodies operating certification of persons*) in an existing field.

The functioning of this scheme will be subject to an assessment at the latest within a period of two years from its entry into force with a view to adjusting framework requirements where necessary. Any potential changes to the accreditation criteria or to the certification criteria will not affect certifications or accreditations already issued.

This certification scheme may be shared with other European data protection authorities within the EDPB (European Data Protection Board).

CNIL accreditation is only required for bodies wishing to issue DPO skills and knowledge certification **based on the CNIL's scheme**. This means that certification bodies can still certify DPOs on the basis of **their own certification scheme (that has not been approved by the CNIL)** as it is already the case.

Documents: see hereunder p. 8 the translation of the criteria

FAQ

For applicants:

Do I need to be certified to be designated as a DPO?

No, certification is not required to practice as a data protection officer.

Is certification of DPO skills and knowledge open to legal entities?

No, certification of DPO skills and knowledge by the CNIL is only open to individuals.

What are the advantages of certification of DPO skills and knowledge by the CNIL?

This certification enables individuals to prove that they have the skills and knowledge required of a DPO as provided by the GDPR. It is also a vector of trust both for the body recruiting such certified persons as well as for clients, suppliers, employees or agents.

Which prerequisites must be met to take the certification examination?

To be able to take the written examination, the applicant must meet one of the following prerequisites:

- provide proof of at least 2 years of professional experience in projects, activities or tasks related to DPO missions as regards personal data protection; or
- provide proof of at least 2 years of professional experience and at least 35 hours of training course in the field of personal data protection dispensed by a training body.

What does the examination consist of?

The examination consists of a MCQ (multiple-choice questionnaire) of at least 100 questions, 30% of which are set out in the form of practical cases. Questions relate to 3 fields (detailed in the appendix to the accreditation criteria) and aim to assess the 17 skills and knowledge listed in the certification criteria (for example, ability to identify the legal basis of a processing or to establish and implement staff training and awareness programmes on data protection to staff).

The examination is passed if at least 75% of answers are correct (with 50% correct answers in each field).

How long is my certification of DPO skills and knowledge valid?

Certification is valid for 3 years from issuance.

How can I renew my certification?

After the 3-year validity period, renewal is possible provided that applicants pass a new written examination in the same format as the initial examination and that they are able to demonstrate at least one year of professional experience in projects, activities or tasks in relation to DPO missions.

For certification bodies applying for CNIL accreditation:

How can certification bodies be accredited from the CNIL?

Certification bodies wishing to be accredited must provide the CNIL with an application file containing:
- a K-bis extract or equivalent;
- the ISO/IEC 17024:2012 accreditation certificate;
- a document presenting the process for DPO skills and knowledge certification; and
- their assessment material (including the questions and answers for the written examination) and the documents describing their implementation (certification rules) relating to the certification of DPO skills and knowledge.

The CNIL will be particularly attentive to the questions/answers provided and may make any comments on them.

For any questions from certification bodies, contact us

Once accredited, what exchanges take place between certification bodies and the CNIL?

Accredited certification bodies provide the CNIL with:

- any change in the status of their accreditation such as the suspension or withdrawal of their ISO/IEC 17024:2012 accreditation, without delay;

- every 6 months as from issuance of the accreditation, the written examination's success rates as well as the updated register of certified persons, including their names, first names, date of issuance of the certification and date of expiry.

- an annual activity report on the DPO skills and knowledge certification including the complaints and claims made against the certification body relating to this certification, as well as any difficulty encountered in the application of the scheme.

Furthermore, accredited certification bodies must be able to demonstrate at any time, at the CNIL's request, compliance with the scheme requirements.

What should I do if my organisation is not accredited under standard ISO/IEC 17024:2012?

Organisations that are not accredited under standard ISO/IEC 17024:2012 are asked to contact COFRAC to apply for an initial accreditation in the field of DPO skills and knowledge certification. This programme will be created in collaboration with the CNIL.

To find out more:

Link to the CNIL website on DPOs

Guidelines on DPOs (EDPB)

Deliberation no. 2018-317 of 20 September 2018 adopting the criteria for the accreditation of certification bodies for the certification of data protection officer (DPO) skills and knowledge

The Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority),

Having regard to Treaty no. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Having regard to Act no. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties, particularly Article 11-I-2° f bis);

Having regard to Decree no. 2005-1309 of 20 October 2005, amended, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties, particularly Article 6-8;

Having regard to deliberation no. 2018-318 of 20 September 2018 adopting the criteria for the certification of data protection officer (DPO) skills and knowledge;

Having heard the report of Mr. Maurice RONAI, commissioner, and the observations of Mrs. Nacima BELKACEM, government commissioner,

Makes the following observations:

In accordance with Article 11-I-2° f bis) of Act no. 78-17, amended, the Commission Nationale de l'Informatique et des Libertés (hereinafter the CNIL or the Commission) is competent to accredit bodies in order to certify the skills and knowledge of data protection officers (hereinafter 'DPO') on the basis of criteria that it has adopted.

This deliberation sets out the criteria for the accreditation of certification bodies for DPO skills and knowledge certification, as provided for in section 4 of Chapter IV of Regulation (EU) 2016/679.

Decides

The accreditation criteria appended to this deliberation for accreditation, by the Commission, of bodies in charge of certifying the DPO skills and knowledge are approved.

Within a period of two years at the latest as from the entry into force of this mechanism, its functioning will be subject to an assessment with a view to adapting, where necessary, the requirements of this scheme.

This deliberation shall be published in the Official Journal of the French Republic.

ACCREDITATION CRITERIA OF CERTIFICATION BODIES FOR THE CERTIFICATION OF DATA PROTECTION OFFICER (DPO) SKILLS AND KNOWLEDGE

Category 1. Accreditation

Requirement 1.1 The certification body is accredited, for the duration of its accreditation by the CNIL, by an accreditation body that is a member of the IAF (*International Accreditation Forum*) under standard ISO/IEC 17024:2012 "*Conformity assessment – General requirements for bodies operating certification of persons*" for a specific certification scheme for persons.

Requirement 1.2 The certification body develops and implements a certification scheme for persons for the DPO that complies with standard ISO/IEC 17024:2012, with the requirements set out in this scheme and with the certification criteria of DPO skills and knowledge (deliberation no. 2018-318 of 20 September 2018).

Category 2. Assessing certification candidates

Requirement 2.1 The certification body ensures that the prerequisites provided for in category 1 of the certification criteria of DPO skills and knowledge (deliberation no. 2018-318 of 20 September 2018) are met.

Requirement 2.2 The certification body verifies the skills and knowledge of the candidate through a written examination, the characteristics of which meet the following requirements.

Requirement 2.3 The written examination is comprised of a multiple choice questionnaire (MCQ), in French, containing at least 100 questions. 30% of questions in each field are set out in the form of practical cases.

Requirement 2.4 The written examination is carried out under conditions that ensure pseudonymity during corrections.

Requirement 2.5 The questions contained in the MCQ assess skills and knowledge relating to the requirements of category 2 of deliberation no. 2018-318 of 20 September 2018 and cover all of the fields of the programme appended to this deliberation with the following breakdown:

- **Field 1 – General regulation on data protection and compliance measures**: 50% of questions;
- **Field 2 – Accountability**: 30% of questions;
- **Field 3 – Technical and organisational measures for data security in light of risks**: 20% of questions.

Requirement 2.6 For each question, 4 possible answers are provided, of which one or several is/are correct.

Requirement 2.7 The questions contained in the MCQ are updated on a regular basis.

Requirement 2.8 The written examination is passed:

- if, in total, at least 75% of answers are correct; and
- if, in each field, at least 50% of answers to questions are correct.

Requirement 2.9 Certification bodies allow Commission observers to be present during examinations.

Category 3. Issuing of certification

Requirement 3.1 The certification body issues certification to candidates having passed the written examination.

Requirement 3.2 The certification body sends the certified person a certified DPO certificate containing the title "*Certified Data Protection Officer in accordance with the CNIL's certification scheme of DPO skills and knowledge*".

Requirement 3.3 Certification is valid for 3 years as from issuance.

Requirement 3.4 The certification body maintains an up-to-date register of certified persons. The register contains, for each certified person, their surname and first names, the date of issuance of the certification, the date of expiry and the status of the certification (issued, suspended, withdrawn, renewed).

Requirement 3.5 The updated register is sent to the Commission every 6 months as from issuance of the accreditation.

Category 4. Renewal of certification

Requirement 4.1 Certification may be renewed prior to the certificate expiry date provided that the certified person:

- passes a new written examination meeting the requirements of category 2 of these criteria; and
- demonstrates that he/she has at least one year of professional experience, acquired within the last three years, in projects, activities or tasks in relation to DPO missions as regards data protection or information security, attested to by a third party (employer or client).

Category 5. Assessment material

Requirement 5.1 The certification body develops and uses its own assessment material and the documents describing its implementation (certification requirements) to assess compliance with the certification criteria (deliberation no. 2018-318 of 20 September 2018).

Category 6. Certification committee

Requirement 6.1 Accredited certification bodies invite a representative of the Commission to their committee for the specific certification scheme.

Category 7. Elements to provide with the application for accreditation

Requirement 7.1 Certification bodies requesting accreditation from the Commission submit a file comprised of:

- a K-bis extract or equivalent;
- the ISO/IEC 17024:2012 accreditation certificate in accordance with requirement 1.1 of this deliberation;
- a document presenting the process for DPO skills and knowledge certification; and

- their assessment material (including the questions asked and replies given for the written examination) and the documents describing their implementation (certification rules) concerning the DPO skills and knowledge certification.

Category 8. Elements to provide on a regular basis or at the Commission's request

Requirement 8.1 Accredited certification bodies are to provide the Commission with:

- without delay, any change in the status of their accreditation such as the suspension or withdrawal of their ISO/IEC 17024:2012 accreditation;

- an annual activity report on the DPO skills and knowledge certification including the complaints and claims made against the certification body relating to this certification as well as any difficulties encountered in the application of certification criteria adopted in deliberation no. 2018-318 of 20 September 2018;

- every 6 months as from issuance of the accreditation, the success rates for the written examination and the updated register of certified DPOs, including their names, first names, date of issuance of the certification and date of expiry.

Requirement 8.2 Accredited certification bodies are able to demonstrate, at any time, at the Commission's request, compliance with the requirements:

- of these criteria, and in particular requirement 1.2; and

- of the certification criteria (deliberation no. 2018-318 of 20 September 2018).

Appendix: Written assessment programme (fields)

Field 1 – General regulation on data protection and compliance measures

(50% of questions)

1.1 European Regulation and French Data Protection Act – fundamentals

1.1.1 Scope of application
1.1.2 Definitions and notions
1.1.3 Organisations subject to regulatory obligations

1.2 European Regulation and French Data Protection Act – principles

1.2.1 Lawfulness of processing
1.2.2 Fairness and transparency
1.2.3 Purpose limitation
1.2.4 Data minimisation
1.2.5 Accuracy of data
1.2.6 Storage limitation
1.2.7 Data integrity and confidentiality

1.3 European Regulation and French Data Protection Act – validity of processing

1.3.1 Legal basis for processing
1.3.2 Consent
1.3.3 Consent of underaged persons
1.3.4 Special categories of personal data
1.3.5 Data relating to criminal convictions and offences

1.4 Data subject's rights

1.4.1 Transparency and information
1.4.2 Access, rectification and erasure (right to be forgotten)
1.4.3 Right to object
1.4.4 Automated individual decision-making
1.4.5 Portability
1.4.6 Restrictions to processing
1.4.7 Restrictions to rights

1.5 Compliance measures

1.5.1 Data protection policies or procedures
1.5.2 Qualification of data processing actors: data controllers, joint controllers, data processors
1.5.3 Formalisation of relationships (processing agreements, agreements between joint controllers)
1.5.4 Codes of conduct and certification

1.6 Data protection officer (DPO)

1.6.1 Appointment and dismissal
1.6.2 Professional skills, specialised knowledge and ability to complete his/her tasks
1.6.3 Role of the DPO (means, resources, position, independence, confidentiality, absence of conflicts of interest, training)
1.6.4 DPO tasks and role of the DPO regarding audits
1.6.5 Relationships between the DPO and data subjects and management of requests to exercise rights
1.6.6 Cooperation between the DPO and the supervisory authority
1.6.7 Personal skills, team work, management, communication, pedagogy

1.7 Transfer of data outside the European Union

1.7.1 Adequacy decision
1.7.2 Appropriate safeguards
1.7.3 Binding corporate rules

1.7.4 Derogations
1.7.5 Authorisation of the supervisory authority
1.7.6 Temporary suspension
1.7.7 Contractual clauses

1.8 Supervisory Authorities
1.8.1 Status
1.8.2 Powers
1.8.3 Penalty system
1.8.4 European Data Protection Board
1.8.5 Judicial remedies
1.8.6 Right to compensation

1.9 Doctrine and case law
1.9.1 WP29 guidelines
1.9.2 Opinion, European Data Protection Board guidelines and recommendations
1.9.3 French and European case law

Field 2 - Accountability
(30% of questions)

2.1 Data protection impact assessment (DPIA)

2.2 Data protection by design and by default

2.3 Record of processing activities (data controller) and record of of categories of processing activities (data processor)

2.4 Personal data breaches, notification of breaches and communication to data subjects.

Field 3 – Technical and organisational measures for data security in light of risks
(20% of questions)

3.1 Pseudonymisation and encryption of personal data

3.2 Measures to ensure the confidentiality, integrity and resilience of processing systems and services

3.3 Measures to restore the availability and access to data in the event of a physical or technical incident

Deliberation no. 2018-318 of 20 September 2018 adopting the criteria for the certification of data protection officer (DPO) skills and knowledge

The Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority),

Having regard to Treaty no. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Having regard to Act no. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties, particularly Article 11-I-2° f bis);

Having regard to Decree no. 2005-1309 of 20 October 2005, amended, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties, particularly Article 6-8;

Having regard to deliberation no. 2018-317 of 20 September 2018 adopting the accreditation criteria of certification bodies for the certification of data protection officer (DPO) skills and knowledge;

Having heard the report of Mr. Maurice RONAI, commissioner, and the observations of Mrs. Nacima BELKACEM, government commissioner,

Makes the following observations:

Pursuant to Article 11-I-2° f bis) of Act no. 78-17, amended, the Commission Nationale de l'Informatique et des Libertés (hereinafter the CNIL or the Commission) is competent to establish or approve the criteria for the certification scheme of skills and knowledge of individuals.

This deliberation sets out the certification criteria of the "data protection officer" category, as provided for in Section 4 of Chapter IV of Regulation (EU) 2016/679.

Decides

The certification criteria appended to this deliberation in view of the certification of data protection officer skills and knowledge by accredited bodies by the Commission are approved.

Within a period of two years at the latest as from the entry into force of this mechanism, its functioning will be subject to an assessment with a view to adapting, where necessary, the requirements of this scheme.

This deliberation shall be published in the Official Journal of the French Republic.

CERTIFICATION CRITERIA FOR DATA PROTECTION OFFICER (DPO) SKILLS AND KNOWLEDGE

Category 1. Prerequisites for certification candidates

Requirement 1.1 In order to access the assessment phase, the candidate must meet one of the following prerequisites:

- provide proof of **at least two years of professional experience** in projects, activities or tasks related to DPO missions as regards personal data protection; or

- provide proof of **at least two years of professional experience** and at least a **training course of at least 35 hours** on personal data protection dispensed by a training body.

Category 2. Skills and knowledge

Requirement 2.1 The candidate shall have knowledge and understanding of the principles of lawfulness of processing, of purpose limitation, of data minimisation, of data accuracy, of storage limitation, of integrity, confidentiality and accountability.

Requirement 2.2 The candidate is able to identify the legal basis of a processing.

Requirement 2.3 The candidate is able to determine which measures are appropriate and which information content should be provided to data subjects.

Requirement 2.4 The candidate is able to establish procedures to receive and manage requests to exercise rights made by data subjects.

Requirement 2.5 The candidate has knowledge of the legal framework relating to subcontracting of personal data processing.

Requirement 2.6 The candidate is able to identify the existence of data transfers outside of the European Union and to determine which legal transfer instruments are likely to be used.

Requirement 2.7 The candidate is able to develop and implement a policy or internal rules on data protection.

Requirement 2.8 The candidate is able to organise and take part in data protection audits.

Requirement 2.9 The candidate is aware of the content of the record of processing activities, the record of categories of processing activities, and of the documentation on data breaches and the documentation necessary to prove compliance with data protection regulations.

Requirement 2.10 The candidate is able to identify data protection measures by design and by default that are suited to the risks and the nature of processing operations.

Requirement 2.11 The candidate is able to take part in identifying security measures that are suited to the risks and the nature of the processing operations.

Requirement 2.12 The candidate is able to identify personal data breaches requiring notification to the supervisory authority and those requiring communication to the data subjects.

Requirement 2.13 The candidate is able to determine whether or not it is necessary to perform a data protection impact assessment (DPIA) and is able to monitor its performance.

Requirement 2.14 The candidate is able to provide advice on data protection impact assessment (in particular on the methodology, on any possible outsourcing, on the technical and organisational measures to adopt).

Requirement 2.15 The candidate is able to oversee relations with supervisory authorities, by answering their requests and by facilitating their action (in particular, through the handling of complaints and investigations).

Requirement 2.16 The candidate is able to establish, implement and provide training and awareness programmes on data protection to staff and to governing bodies.

Requirement 2.17 The candidate is able to ensure the traceability of his/her actions, particularly through monitoring tools or annual reports.