Deliberation 2018-317 of September 20, 2018 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Friday October 12, 2018 certification bodies for the certification of the skills of the Data Protection Officer (DPO) The National Commission for Computing and Liberties,

Having regard to Convention 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 individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 11-I-2° f bis;

Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 6-8;

Having regard to deliberation no. 2018-318 of September 20, 2018 adopting the criteria of the certification reference system for the skills of the data protection officer (DPO); After having heard Mr. Maurice RONAI, auditor, in his report, and Mrs. Nacima BELKACEM, Government Commissioner, in his observations,

Makes the following observations:

In accordance with Article 11-I-2° f bis of Law No. 78-17 as amended, the National Commission for Data Processing and Liberties (hereinafter, the CNIL or the Commission) is competent to approve organizations with a view to issuing certification of the skills of the Data Protection Officer (hereinafter DPO) on the basis of criteria it has adopted.

This deliberation establishes the criteria for the approval of certification bodies for the certification of the skills of natural persons as data protection officer, as referred to in section 4 of chapter IV of Regulation (EU) 2016/679 .

Decided :

The criteria of the reference document appended to this deliberation with a view to the approval by the Commission of bodies in charge of certifying the skills of the data protection officer are approved.

The functioning of this system will be the subject, at the latest within two years of its entry into force, of an evaluation with a view to adapting, if necessary, the requirements of this reference system.

This deliberation will be published in the Official Journal of the French Republic.Appendix REFERENCE FOR THE APPROVAL OF CERTIFICATION BODIES FOR THE CERTIFICATION OF THE SKILLS OF THE DATA PROTECTION OFFICER (DPO)

Category 1. Accreditation Requirement 1.1. The certification body is accredited, for the entire duration of its approval by the CNIL, by an accreditation body member of the IAF (International Accreditation Forum) with regard to the ISO/IEC 17024: 2012 standard Conformity assessment - General requirements for certification bodies carrying out the certification of persons for a particular system of certification of persons.

Requirement 1.2. The certification body develops and implements a system for certifying people for the DPO in accordance with the ISO/IEC 17024: 2012 standard, the requirements set by this reference system as well as the requirements set by the skills certification reference system of the DPO (deliberation n° 2018-318 of September 20, 2018).Category 2. Evaluation of the candidate for certificationRequirement 2.1. The certification body verifies compliance with the prerequisites provided for in category 1 of the DPO's skills certification reference system (deliberation no. 2018-318 of September 20, 2018).

Requirement 2.2. The certification body verifies the candidate's skills and know-how by means of a written test whose characteristics meet the following requirements.

Requirement 2.3. The written test consists of a multiple-choice questionnaire (MCQ) in French comprising at least 100 questions. 30% of the questions in each of the areas are stated in the form of a practical case.

Requirement 2.4. The written test is carried out under conditions guaranteeing pseudonymity during the correction.

Requirement 2.5. The MCQ questions assess skills and know-how with regard to the requirements of category 2 of deliberation no. 2018-318 of September 20, 2018 and cover all the areas of the program appearing in the appendix to this deliberation according to the following distribution :

Area 1. - General data protection regulations and measures taken for compliance: 50% of questions;

Area 2. - Responsibility: 30% of questions;

Area 3. - Technical and organizational measures for data security with regard to risks: 20% of questions.

Requirement 2.6. For each question, 4 answers are proposed, one or more of which are correct.

Requirement 2.7. MCQ questions are regularly updated.

Requirement 2.8. The written test is passed:- if, in total, at least 75% of the answers are correct; and

- if, for each of the three areas, at least 50% of the answers to the questions are correct. Requirement 2.9. The certification bodies allow observers from the Commission to be present during the course of the tests. Category 3. Issue of certification Requirement 3.1. The certification body issues certification to candidates who have passed the written test.

Requirement 3.2. The certification body sends the certified person a certified DPO certificate bearing the wording Data Protection Officer certified in accordance with the CNIL's DPO skills certification reference system.

Requirement 3.3. The certification is valid for 3 years from its issue.

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

Requirement 3.5. The updated register is transmitted to the Commission every 6 months from the issue of the approval.Category 4. Renewal of certificationRequirement 4.1. Renewal of certification is possible before the expiry date of the certificate provided that the certified person: - passes a new written test meeting the requirements of category 2 of this standard; and

- demonstrates that it has professional experience of at least one year, acquired in the course of the last three years, in projects, activities or tasks related to the missions of the DPO with regard to data protection or information security, attested by a third party (employer or client). Category 5. Assessment material Requirement 5.1. The certification body develops and applies its assessment material and the descriptive documentation of its implementation (certification requirements) in order to assess compliance with the criteria of the certification reference system (deliberation n° 2018-318 of September 20, 2018 ).Category 6. Certification CommitteeRequirement 6.1. Accredited certification bodies invite a representative of the Commission to their special arrangements committee.Category 7. Items to be provided with the application for accreditationRequirement 7.1. The certification bodies that request to be approved by the Commission provide it with a file including:- a K-bis extract or equivalent;

- the ISO/IEC 17024: 2012 accreditation certificate in accordance with requirement 1.1 of this deliberation;

- a document that presents the DPO skills certification process; and

- their assessment material (in particular the questions asked and the answers for the written test) and the descriptive documentation of their implementation (certification rules) concerning the certification of the skills of the DPO.Category 8.

Elements to be provided in a manner regularly or at the request of the CommissionRequirement 8.1. Accredited certification bodies shall forward to the Commission: - without delay, any modification of their accreditation status such as the suspension or withdrawal of ISO/IEC 17024: 2012 accreditation;

- an annual activity report on the certification of the skills of the DPO including the complaints and claims against the certification body in the context of the certification of the skills of the DPO as well as any difficulty encountered in the application of the criteria certification of DPO skills adopted in deliberation no. 2018-318 of September 20, 2018;

- every 6 months from the issue of the approval, the statistics of success of the written test as well as the updated register of the DPO certified persons including the surnames, first names, the date of issue of the certification and the date of expiration.Requirement 8.2. Approved certification bodies are in a position, at the request of the Commission, to demonstrate at any time compliance with the requirements:- of this reference system, and in particular of requirement 1.2; and

- the DPO skills certification reference system (deliberation no. 2018-318 of September 20, 2018).Appendix

Program of the written assessment (domains)Area 1. - General data protection regulations and measures taken for compliance (50% of questions)1.1. European regulation and French law on data protection - fundamentals:

1.1.1. Scope.

1.1.2. Definitions and concepts.

1.1.3. Organizations subject to regulatory obligations.

1.2. European regulations and French law on data protection - principles:

1.2.1. Lawfulness of processing.

1.2.2. Loyalty and transparency.

1.2.3. Purpose Limitation.

1.2.4. Data minimization.

1.2.5. Data Accuracy.

1.2.6. Limited data retention.

1.2.7. Integrity, confidentiality of data.

1.3. European regulations and French law on data protection - validity of the processing:

1.3.1. Legal bases for processing.

1.3.2. Consent.

1.3.3. Consent of minors.

1.3.4. Special categories of personal data.

1.3.5. Data relating to criminal convictions and offences.

1.4. Rights of data subjects:

1.4.1. Transparency and information.

1.4.2. Access, rectification and erasure (right to be forgotten).

1.4.3. Opposition.

1.4.4. Automated individual decisions.

1.4.5. Portability.

1.4.6. Restriction of processing.

1.4.7. Limitation of rights.

1.5. Measures taken for compliance:

1.5.1. Data protection policies or procedures

1.5.2. Qualification of data processing actors: controllers, joint controllers, subcontractors

1.5.3. Formalization of relations (subcontractor contract, agreement between joint controllers).

1.5.4. Codes of conduct and certifications.

1.6. Data Protection Officer (DPO):

1.6.1. Designation and end of mission.

1.6.2. Professional qualities, specialized knowledge and ability to accomplish its missions.

1.6.3. Function of the DPO (means, resources, positioning, independence, confidentiality, absence of conflict of interest, training).

1.6.4. Missions of the DPO and role of the DPO in terms of audits.

1.6.5. DPO relations with data subjects and management of requests to exercise rights.

1.6.6. Cooperation of the DPO with the supervisory authority.

1.6.7. Personal qualities, teamwork, management, communication, pedagogy.

1.7. Transfers of data outside the European Union:

1.7.1. Suitability decision.

1.7.2. Appropriate safeguards.

1.7.3. Binding Corporate Rules.

1.7.4. Derogations.

1.7.5. Authorization of the supervisory authority.

1.7.6. Temporary suspension.

1.7.7. Contract clauses.

1.8. Supervisory authorities:

1.8.1. Status.

1.8.2. Powers.

1.8.3. Penalty regime.

1.8.4. European Data Protection Board.

1.8.5. Legal remedies.

1.8.6. Right to repair.

1.9. Doctrine and jurisprudence:

1.9.1. G29 guidelines.

1.9.2. Opinions, guidelines and recommendations of the European Data Protection Board.

1.9.3. French and European case law. Area 2. - Liability

(30% of questions)2.1. Data Protection Impact Assessment (DPIA).

2.2. Data protection by design and by default.

2.3. Register of processing activities (controller) and register of categories of processing activities (processor).

2.4. Personal data breaches, notification of breaches and communication to the data subject.Area 3. - Technical and organizational measures for data security with regard to risks

(20% of questions)3.1. Pseudonymization and encryption of personal data.

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

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

I. Falque-Pierrotin