Deliberation 2020-139 of December 3, 2020 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Thursday February 18, 2021 NOR: CNIL2104899X Deliberation No. 2020-139 of December 3, 2020 adopting the criteria of the personal data protection training providersThe 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 8-I-2°-h;

Having regard to decree n° 2019-536 of May 29, 2019 as amended, taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 74; Mr. Christian KERT, commissioner, in his report, and Mr. Benjamin TOUZANNE, government commissioner, in his observations, Makes the following observations: In accordance with article 8-I-2° h of law n° 78-17 amended, the National Commission for Computing and Liberties (hereafter, the CNIL or the Commission) is competent to develop or approve the criteria of a skills certification reference system certification of people, products, data systems or procedures. This deliberation establishes the criteria of the certification reference system for training providers in the protection of personal data. Decides On the approval of the criteria of the reference document appended to this deliberation for the certification of services training in the protection of personal data. This deliberation and its appendix will be published in the Official Journal of the French Republic. President M.-L. DenisREFERENCE FOR CERTIFICATION OF PERSONAL DATA PROTECTION TRAINING PROVIDERS (December 2020)I. Who is this reference aimed at?This reference constitutes the list of criteria with which a training provider must demonstrate compliance in order to obtain the certification of training provider in the protection of personal data according to the CNIL reference. II. Terminology

Term

Definition

Learner (Recipient)

Person engaged in a learning process (ISO 29993:2017 [1]).

Aptitude

Ability to apply knowledge and use know-how to perform tasks and solve problems (RNQ Guide [2]).

Skill

Proven ability to implement knowledge, skills and personal, social or methodological dispositions in work or study/training situations, for professional or personal development (RNQ Guide).

Training objectives

Statement of skills and competencies, targeted and assessable, which will be acquired during the training (RNQ Guide).

Training Sponsor

Organization or individual that acquires learning services on behalf of learners, provides them with financial or other support, or has a direct interest in the learning outcome (ISO 29993:2017).

Training service provider (Provider)

Organization providing training services outside the framework of formal education, including all the collaborators involved in the provision of the training service (ISO 29993:2017).

Training Service (Training/Service)

Sequence of activities designed to enable learning (ISO 29993:2017)

Former

A person who works with learners to support them in their learning (ISO 29993:2017).

Methods used

Teaching methods and/or means and/or tools used to carry out the service provided (RNQ Guide).

Assessment methods

Means mobilized to measure, using objective criteria, the beneficiary's achievements during and/or at the end of the service (RNQ Guide).

Training Content Designer (Designer)

Person charged by the service provider with designing and adapting the content of the training and the methods used.

Designers of assessment methods (Designer)

Person charged by the service provider with the design of the evaluation methods.(1) ISO/IEC 29993 - Training services

provided outside the framework of formal education - Service requirements.(2) https://travail-emploi .gouv.fr/demarches-ressources-documentaires/documentation-et-publications-officielles/guides/guide-referentiel-national-qualite.III. Reference criteria1. General requirements

C01. The service provider complies with the criteria of the national quality reference system mentioned in article L. 6316-3 of the labor code for its training actions contributing to the development of skills.

When the service provider does not have certification, according to the national quality reference system, currently valid for its training actions contributing to the development of skills, the service provider is able to demonstrate that each requirement of the latter is respected for the data protection training it offers.

C02. When the service provider uses subcontracting or wage portage, it ensures compliance with the criteria of this reference system by the subcontractor or the employee carried out, prior to the first service and then, at regular frequencies established by the provider.

Note: this does not imply an obligation to certify subcontractors.

C03. The service provider defines, implements and updates procedures to demonstrate compliance with data protection rules for the processing that it implements as part of its data protection training activity. personal.

These procedures cover in particular the implementation of data protection measures in the context of data processing carried out for:

- the evaluation of the skills of the speakers and the learners;

- the service provider's communication actions aimed at the public.2. Requirements relating to the information of the public on the training offered

C04. The service provider designs and offers at least one data protection training course that covers all the objectives of the general skills and competences reference set out in appendix 1.

C05. When the service provider offers training that does not cover all of the objectives of the general skills and competences reference set out in appendix 1, it informs the learners and their sponsor of these exclusions and the resulting prerequisites.3. Requirements for identifying training needs and objectives

C06. The service provider defines the objectives of each training course in terms of acquired skills and competencies.

Where applicable, these acquired skills and competencies specify or supplement the reference system in appendix 1.

C07. The service provider defines and implements a procedure to collect and analyze the training needs, in terms of data protection, of learners and their sponsor, with a view to identifying training objectives.

When a training request relates to a pre-existing service, the service provider:

- ensures that the objectives of this training are adapted to the needs of the learners and the sponsor;
- collects their specific needs according to which he can propose to integrate complementary objectives into the training.

Note: this does not imply the obligation to design or adapt a pre-existing service to all the objectives identified during the collection of the need. On the other hand, if the service is not totally adapted to the needs expressed by the learners and their sponsor, the latter must be informed of the objectives which will not be covered by the proposed training.

C08. When the objectives of a training course specifically target a sector of activity, a particular theme or a particular type of data processing operation, the service provider identifies the specific skills necessary for the design, adaptation and implementation of this formation.

Note: the informative list of sectors of activity, specific themes and specific types of data processing operation published by the CNIL can be used for this purpose.

C09. The service provider who decides to design training preparing for a skills certification approved by the CNIL takes into account the criteria of this certification when defining the objectives of the training.4. Training design requirements

C10. The service provider establishes the content of the training and the methods used, which include a theoretical and practical dimension, taking into account the objectives agreed with the learners and their sponsor during the needs analysis phase.

When the service provider designs training whose objectives relate to a specific sector, a particular theme or a particular type of data processing operation, it takes into account the applicable standards published by the CNIL and the European Data Protection Board. .

C11. The service provider develops and documents the methods for evaluating the achievement by learners of the objectives of each training.

In particular, the service provider ensures that the evaluation methods cover all of the objectives of each training course.

C12. The service provider monitors the latest news in terms of data protection, the legislation applicable to data protection and the state of the art in terms of information security.

The service provider regularly identifies the training courses impacted by the new features identified.

C13. The service provider reviews and updates the content of the training according to:

- the changing needs and feedback from learners and their sponsor;

- the result of the learners' assessments;

- news in terms of data protection: guidelines from the European Data Protection Board, guidelines developed by the CNIL, communications and corrective measures from the CNIL, etc. ;

- changes in data protection legislation;

- the development of information security techniques;

- the evolution of threats in terms of information security.

C14. The service provider ensures that the content of the training courses has been updated for less than 3 months at the time of their completion.

C15. When modifying or adapting the objectives of a training course, the service provider ensures that the content of this training course and the evaluation methods remain adequate.

C16. The service provider mobilizes designers who have the skills necessary to achieve the identified objectives, in particular with regard to specific sectors and specific themes or specific types of processing operations.

C17. The service provider ensures that changes to the content of each training course and to the evaluation methods are subject to follow-up, which enables changes to be controlled, for example by version control.

The service provider documents the purpose of the modifications made, the date of application of these modifications and their authors.5. Requirements for preparing and adapting training to learners

C18. When the training request relates to a pre-existing service, the service provider adapts the content of the training to the additional objectives agreed with the learners and their sponsor during the needs analysis phase.

C19. The service provider mobilizes trainers who have the skills necessary to achieve the identified objectives, in particular with regard to specific sectors and specific themes/specific types of processing operations, and taking into account the needs of learners.

When the service provider wishes to call on participants who do not meet the competency criteria for trainers in this reference system (participant outside the criteria), or when the organization is unable to demonstrate compliance with these criteria for

these participants, he ensures that the interventions concerned are assessed by a trainer who meets the skills criteria of this reference system (qualified trainer).

This evaluation aims to analyze the relevance of the intervention for achieving the training objectives, in addition to the interventions carried out by the trainers mobilized for the service. For regular interventions, this assessment is renewed every year.

Note: any use of contractors outside the criteria must be justified by an intervention requiring a specific contractor profile.6. Requirements relating to the conditions for carrying out training

C20. The service provider keeps a list of the data protection training sessions that have been carried out. This list includes in particular the date, the training reference, the names of the speakers and the number of learners who have completed the training.7. Stakeholder competency requirements

C21. The service provider ensures that its staff has the skills required to collect the needs of learners and their sponsor, define the objectives of the training requested and identify specific sectors, specific topics or specific types of processing operations.

C22. The service provider ensures that the designers of the training content, the designers of the evaluation methods and the trainers have professional experience that includes:

- (technical profile) at least 3 years in positions or functions dedicated to the design, or the evaluation or the implementation of measures relating to information security; Where

- (legal profile) at least 3 years in positions or functions dedicated to the analysis, or the evaluation or the implementation of the regulations applicable to the protection of personal data.

When a training course is designed or carried out by a single speaker, the service provider ensures that this speaker has professional experience which makes it possible to justify experience corresponding to both the technical and legal profiles defined by these standards.

The service provider ensures that this professional experience is not older than 2 years at the time of the intervention.

Note: professional experience acquired as a trainee or apprentice is not counted.

C23. The service provider ensures that the designers and trainers justify:

- at least a law degree at master 2 level or equivalent; Where

- at least a master's degree 2 or equivalent in the field of computing, information systems or cybersecurity; Where

- a diploma course relating to the protection of personal data.

Failing to justify one of these diplomas, the designers and trainers must justify under the validation of acquired experience in the context of this reference system:

- full-time professional experience of at least 5 years in positions or functions dedicated to the design, or the evaluation or the implementation of measures relating to information security; Where

- a full-time professional experience of at least 5 years in positions or functions dedicated to the analysis, or the evaluation, or the implementation of the regulations applicable to the protection of personal data personal.

Note: with regard to the skills of designers and trainers, the criteria of professional experience (C22), training or validation of acquired experience (C23), teaching experience (C24) and maintenance of knowledge (C25) are cumulative: the service provider must be able to demonstrate that these criteria are individually respected for each of these stakeholders.

C24. The service provider ensures that designers and trainers:

- have designed or run a diploma course; Where

- have designed or facilitated training carried out by a service provider certified according to this standard (or labeled by the CNIL); Where

- are subject to an assessment of their pedagogical skills during their first intervention in the context of data protection training.

C25. The service provider ensures that designers and trainers maintain their knowledge of data protection.

C26. The service provider sets the criteria making it possible to identify the skills of the designers and trainers in the field of personal data protection in the specific sectors, for the particular themes or the particular types of processing operations for which it wishes to meet the needs of training.8. Requirements relating to the collection of assessments and the consideration of complaints

C27. The service provider defines and implements a procedure to collect and process learner feedback on the resources mobilized (documentary and human) as well as on the ability of the training to meet their needs and the identified objectives.

C28. The service provider defines and implements a procedure intended to collect and process complaints concerning the training activity in the protection of personal data.

The service provider acknowledges receipt of complaints. It responds to applicants and keeps complainants informed of the conclusion of the processing of their complaint within a maximum period of 2 months from the date of receipt of their dispatch

and informs them, during this period, of the progress of the processing. of their request or complaint.

When the processing of the complaint is complex, this period may be extended. In this case, the service provider informs the complainant of the additional period at the end of which a response will be sent to him and of the reasons which justify this additional period. It informs the complainant of this extension within one month of receipt of the complaint.

C29. The service provider appoints a person responsible for acting as a contact point for the CNIL on questions relating to the certification.IV. - Appendix 1: General repository of skills and competencies1. Data protection, its key concepts and its actors

AC01. The training allows you to know and understand the concepts of:

- Personal data;
- Special categories of personal data;
- Data relating to criminal convictions and offences;
- Processing of personal data;
- File ;
- Data controller;
- Subcontracting ;
- Recipient ;
- Authorized third party;
- Rights of persons;
- Profiling;
- Anonymization;
- Pseudonymization;
- Authentication;
- Authorization;
- Logging;
- Archiving;
- Encryption.

AC02. The training makes it possible to identify the processing of personal data.

AC03. The training makes it possible to know and understand the principles allowing to qualify the parties involved in a processing operation (data controllers, joint controllers, subcontractors, recipients).

AC04. The training makes it possible to know and understand the different missions of the supervisory authorities and the European Data Protection Board.

AC05. The training allows you to know and understand the material and territorial scope of the European data protection regulation.

AC06. The training allows you to know and understand the relationship between the texts relating to data protection and other sources of law.

AC07. The training provides knowledge and understanding of the principles applicable to data transfers outside the European Union and the European Economic Area (EEA).

AC08. The training makes it possible to identify the existence of transfers outside the European Union and to know the various legal instruments making it possible to supervise them.2. The principles of data protection

AC09. The training makes it possible to know and understand the conditions of lawfulness of a processing.

AC10. The training allows you to know and understand the conditions applicable to consent.

AC11. The training makes it possible to know and understand the purpose principle and to identify a diversion of purposes.

AC12. The training allows you to know and understand the principle of proportionality and relevance of data.

AC13. The training makes it possible to know and understand the conditions applicable to the processing of specific categories of data.

AC14. The training provides knowledge and understanding of the principle of data retention.

AC15. The training makes it possible to know and understand the principles of data security and confidentiality and makes it possible to qualify a security incident as a breach of personal data.

AC16. The training makes it possible to know and understand the principle of transparency of information and communications with the persons concerned by processing.

AC17. The training makes it possible to know and understand the rights available to the persons concerned as well as their methods of exercise:

- the right of access;

- the right of rectification;

- the right to erasure;

- the right to restriction of processing;

- the right to portability;

- the right of opposition.

AC18. The training provides knowledge and understanding of the principle of data accuracy.3. The responsibilities of the actors

AC19. The training allows you to know and understand the principle of responsibility (accountability) and the organizational measures, internal rules and compliance tools to ensure and demonstrate that the rules relating to data protection are respected.

AC20. The training identifies data protection measures by design and by default.

AC21. The training makes it possible to know and understand the obligations incumbent on data controllers and the principle of joint responsibility.

AC22. The training makes it possible to know and understand the obligations incumbent on subcontractors.4. DPO and compliance tools

AC23. The training allows you to know and understand the methodology of impact analysis relating to data protection.

AC24. The training makes it possible to know and understand the functions and missions of the data protection officer.

AC25. The training provides an understanding of the contents of the register of processing activities (controller), the register of categories of processing activities (processor) and the register of data breaches.

AC26. The training makes it possible to know and understand the guarantees provided by codes of conduct and certification mechanisms when they are approved by an authority or by the European Data Protection Board.5. Standby Sources

AC27. The training provides knowledge of the means to learn about current events and case law in the field of data protection.

AC28. The training provides knowledge of the means to learn about the state of the art in information security.