CNIL

Decision No. 2011-315 dated 6 October 2011 adopting a standard for delivering privacy seals in matters of training covering the protection of persons with regard to the processing of personal data

The French data protection authority,

Pursuant to Convention No. 108 of the Council of Europe for the protection of persons with regard to the automated processing of personal data;

Pursuant to directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

Pursuant to Act No. 78-17 dated 6 January 1978 (French data protection act) amended relative to the protection of natural persons with regard to the processing of personal data, particularly its articles 11, 3°, (c) and 13;

Pursuant to decree No. 2005-1309 dated 20 October 2005 for the application of the Act dated 6 January 1978 amended by the Act No. 2004-810 dated 6 August 2004;

Pursuant to decision No. 2011-249 dated 8 September 2011 amending article 69 of the internal regulations of the French data protection authority by inserting a chapter IV a entitled "certification procedure";

After having read the report from Mr Jean-François Carrez, commissioner, and heard the comments of Ms Elisabeth ROLIN, government commissioner;

Makes the following comments:

Article 11, 3°, (c) of the Act dated 6 January 1978 amended states that "when requested by professional organisations or institutions of which the members are mainly data controllers, [… the CNIL] delivers a privacy seal to products or procedures intended to protect individuals in respect of processing of personal data, once it has recognised them to be in conformity with the provisions of this [Act dated 6 January 1978 amended]".

The data protection authority considered that requests made by professional organisations or institutions of which the members are mainly data controllers correspond to a requirement from professionals in this sector.

This is why the Data Protection Authority agrees to deliver training privacy seals concerning the protection of persons with regard to the processing of personal data.

Article 53-3 of the Data Protection Authority's internal regulations specifies that *" examination of a privacy seal request is performed based on a standard established by the Data Protection Authority. This standard defines the characteristics that a product or procedure must have in order for*

it to be recognised as compliant with the provisions of the Act dated 6 January 1978 amended. It specifies the procedures for assessing this compliance and, where applicable, the details relative to checks following delivery of the privacy seal".

Consequently, the present decision determines the standard for evaluating training procedures covering the protection of persons with regard to the processing of personal data

Decides that the standard for evaluating privacy seals requests relative to training courses covering the protection of persons with regard to the processing of personal data is shown in the appendix to the present decision, which is published in the "Journal Officiel" of the French Republic.

The Chair

Emmanuel de GIVRY Isabelle FALQUE-PIERROTIN

Delegate Vice-chair

Appendix: STANDARD FOR CERTIFYING TRAINING COURSES

Introduction

A training course is defined as a process intended to produce and develop knowledge, know-how and the behaviour necessary to satisfy requirements (definition taken from the standard ISO 10015 "Quality management – Guidelines for training").

Data Protection training is therefore a process intended to produce and develop knowledge, know-how and behaviour necessary to compliance with the French data protection act. It should be noted that the said process may take place over several days and include several modules which are independent of each other.

The present standard defines the criteria and resources enabling the Data Protection Authority to determine whether the training courses for which a privacy seal is requested actually achieve such an objective.

It includes two parts corresponding to both phases of the evaluation performed by the Data Protection Authority and which cover:

- the training activity (requirements concerning the method, noted "EMxx" in chapter 1);
- the content of the training course, which is composed:
  - of a main module of fundamental knowledge that the training course must at least include in its curriculum to apply for certification (requirements on the content of the main module, noted "ECxx" in chapter 2);
  - supplementary modules, that the training course may also include in its curriculum (requirements on additional content, noted ESxx in chapter 3).

Applicants must demonstrate that they satisfy the requirements of the standard by supplying explanations and evidence. These may take the form of an extract from an internal standard, a description of a method or a procedure, or any other document. To be valid, the proposed demonstration must not merely repeat the content of the requirements to indicate that the training course subject to evaluation is compliant with them, but it must explain how the evaluated training course fulfils them specifically and in detail.

A part of this standard (chapter 1) is an interpretation by the CNIL of the standard NF ISO 29990 (Learning services for non-formal education and training – Basic requirements for service providers, 2010). Only the original and complete text of this standard, as disseminated by AFNOR and available via the Internet site www.afnor.org, has normative value.

Terminology

Learner	Person engaged in a learning process (IS029990).
Knowledge	Acquisition of ability, particularly through training.
Competence	Knowledge, understanding, skill or attitude which is observable and/or measurable, implemented and controlled in a given working situation and in the context of professional and/or personal development. (IS029990)
Party instructing the training course	Organisation or individual providing financial or other support to the learner or manifestly interested in the result of the training. (ISG29990)
Curriculum	Study plan drawn up by the provider of the training service, which describes the objectives to be achieved, the content, the results of the training, the methods of teaching and learning and the evaluation process. (IS029990)
Training	Process intended to produce and develop knowledge, know-how and behaviour necessary to the satisfaction of requirements. (ISO 10015)
Trainer	Person working with learners to help them in their learning. (IS029990)
Training organisation	Organisation of any size or individual providing training services.

1. Standard for evaluating the training activity

1.1. Requirements relative to compliance with the French data protection act by the training organisation

EM0I. The training organisation has set up an approach aiming to ensure that all processes that it uses for all of its activities are compliant with the French data protection act, including the training.

EM02. The training organisation has carried out the prior formalities relative to the processing implemented pursuant to the management of its personnel and all of its activities, including training.

EM03. The training organisation informs, in compliance with the provisions of the French data protection act, the persons concerned by the processing that it implements,

EM04. The training organisation puts in place a procedure intended to manage requests and complaints from the persons whose data it processes.

1.2. Requirements relative to the identification of training requirements

EM05. The training organisation has a procedure for taking into account the requirements of learners and their instructing party when designing the content of the training course and the training process (for example: requirements collection form, market study, meeting to prepare for the organisation of the training course…).

EM06. The training organisation has a procedure for making sure that the training material and methods used are appropriate for reaching the stated objectives (for example: consultation of professionals in data protection, satisfaction survey,…).

EM07. The training organisation has a procedure so that the content of the training course and the training process takes into account the results of the training course (for example: evaluation of learners, analysis of satisfaction questionnaires).

1.3. Requirements relative to the process of designing the training course

EM08. The training organisation must finalise and document a curriculum and the appropriate means of evaluating the training course.

EM09. The training organisation has training methods which meet the objectives and requirements of the curriculum and take into account the requirements of learners.

EM10. The training organisation has procedures intended to review and update the content of the training course, both according to requirements of, and feedback from, learners and their instructing party and according to relevance, evolution of the legislation and development of techniques.

1.4. Requirements related to the competence and evaluation of trainers

EM11. The training organisation makes sure that its personnel and its trainers have the competence required to identify the requirements of learners, design the training course and deliver its content (for example: by interviewing the trainer, by attending a training session,…).

EM12. The training organisation makes sure that the trainers have professional experience of at least five years in the data protection sector.

EM13. The training organisation makes sure that the trainers have carried out at least two training courses during the last two years.

EM14. The organisation makes sure that the trainers have the key competence required and that this is maintained.

EM15. The training organisation sets up systems for evaluating the competence of its personnel and of those taking part. This process is documented.

EM 16. The training organisation has a procedure for requesting feedback from learners on the methods and resources used, and in their effectiveness in producing the agreed results of the training course.

EM17. The training organisation makes sure that the evaluation procedures chosen and implemented provide reliable information on the skills of its personnel and those taking part.

1.5. Requirements relative to the training implementation conditions

EM18. The training organisation informs the learner and their instructing party of the objectives of the training course, its format, the educational instruments used and, where applicable, the criteria used for the evaluation.

EM19. The training organisation informs the learner and their instructing party of prerequisites such as modifications and professional experience necessary to the training.

EM20. The training organisation ensures that the training resources are available and accessible to learners.

2. Reference framework for evaluating the content of the main training module

2.1. Requirements relative to the presentation of principles and definitions

EC01. The training provides understanding and knowledge on the concepts of processing, files, personal data, data controller and recipient.

EC02. The training provides understanding and knowledge of the practical scope of application of the Act.

EC03. The training provides understanding and knowledge of the geographical scope of application of the Act.

2.2. Requirements relative to the presentation of legality conditions for processes

EC04. The training provides understanding and knowledge of the principle of the intended purpose of processes.

EC05. The training provides understanding and knowledge of the principle of relevance and appropriateness of data for the intended purpose.

EC06. The training provides understanding and knowledge of the principle of limited retention of data.

EC07. The training provides understanding and knowledge of the principle relative to the physical and logical security of data, including in a subcontracting context.

EC08. The training provides understanding and knowledge of the concept of consent, its necessity in the context of implementing processing and exceptions to its collection.

EC09. The training provides understanding and knowledge of "sensitive" data and the conditions under which it can be processed.

2.3. Requirements relative to the presentation of the rights of persons with regard to the processing of personal data

EC 10. The training course provides understanding and knowledge of the right to information of the persons concerned by processing and the resulting obligations for the data controller.

EC11. The training course provides understanding and knowledge of the right of persons to object, the procedures for exercising it and the resulting obligations for the data controller.

EC 12. The training course provides understanding and knowledge of the right of access of the persons concerned by processing and the resulting obligations for the data controller.

EC 13. The training course provides understanding and knowledge of the right of rectification and deletion of the persons concerned by processing and the resulting obligations for the data controller.

3, Standard for evaluating the content of additional training modules

3.1. Requirements relative to the presentation of the CNIL and its duties

ES01. The training provides understanding and knowledge of the status and composition of the CNIL.

ES02. The training provides understanding and knowledge of the organisation and services of the Data Protection Authority in its plenary and select forms.

ES03. The training provides understanding and knowledge of the various duties of the CNIL.

3.2. Requirements relative to the presentation of formalities prior to the implementation of processing

ES04. The training course provides understanding and knowledge of the various prior formality regimes.

ES05. The training course provides understanding and knowledge, for the various regimes, of the procedures for accomplishing the formalities with the CNIL and the way in which it examinates them.

3.3. Requirements relative to the presentation of the control of transfers of data outside the European Union

ES06. The training course provides understanding and knowledge of the principles concerning the transfer of data outside the European Union.

ES07. The training course provides understanding and knowledge of the various means of controlling data transfers.

ES08. The training course provides understanding and knowledge of the prior formalities applicable to a transfer of data outside the European Union.

ES09. The training course provides understanding and knowledge of the obligations of the data controller concerning information to persons concerned by their data being transferred outside the European Union.

3.4. Requirements relative to the presentation of the role of Personal Data Protection Officer

ES 10. The training course provides understanding and knowledge of the status of the officer and the various types of designations.

ES 11. The training course provides understanding and knowledge of the conditions and procedure for designating an officer.

ES 12. The training course provides understanding and knowledge of the conditions under which the list

of processes must be kept by the officer.

ES13. The training course provides understanding and knowledge of the conditions under which the officer handles complaints sent to the data controller.

ES 14. The training course provides understanding and knowledge of the conditions under which the officer must prepare the annual statement of his/her activity.

ES 15. The training course provides understanding and knowledge of the conditions under which the officer alerts the data controller concerning any shortcomings that he/she finds.

ES 16. The training course provides understanding and knowledge of the relationship between the CNIL and the officer.

ES 17. The training course provides understanding and knowledge of the conditions and procedure relative to the end of the officer's assignment.

3.5. Requirements relative to the presentation of the control of processing in the field of health

ESI8. The training course covers the knowledge and determination of the prior formalities regime applicable depending on whether the processing concerns research in the field of health (chapter IX) or the evaluation or analysis of practices or activities concerning treatment and prevention (chapter X).

ES 19. The training course provides understanding and knowledge of the content of the dossier to be presented to the CNIL, whether the processing concerned relates to chapter IX or X of the Act.

ES20. The training course provides understanding and knowledge of the conditions under which the processing of personal data intended for research in the field of health must be implemented to comply with the provisions of the Act.

ES21. The training course provides understanding and knowledge of the cases where the Data Protection Authority may, for medical research processing, adopt reference methodologies.

ES22. The training course provides understanding and knowledge of the rights of persons who participate in medical research and particularly the right to information, with, in certain cases, the collection of their consent, and the resulting obligations for the data controller.

ES23. The training provides understanding and knowledge, for medical research processing, of the cases in which there may be dispensation from the obligation to provide information specified by the Act.

ES24. The training course provides understanding and knowledge of the conditions under which the processing of personal data intended to evaluate or analyse treatment or prevention practices must be implemented to comply with the provisions of the Act.

ES25. The training provides understanding and knowledge of the guarantees that the person in charge of processing must present to the Data Protection Authority for evaluating or analysing treatment and prevention practices.

ES26. The training course provides understanding and knowledge of the security conditions to be implemented to ensure the confidentiality of information handled by the processing in question, whether it relates to chapter IX or X.

3.6. Requirements relative to the presentation of the CNIL's subsequent inspection powers

ES27. The training course provides understanding and knowledge of the various forms of subsequent inspection that may be carried out by the CNIL.

ES28. The training course provides understanding and knowledge of the formalism associated with an inspection procedure.

ES29. The training course provides understanding and knowledge of the practical procedures for exercising an inspection procedure.

ES30. The training course provides understanding and knowledge of the rights and obligations of data controllers and representatives of the CNIL in the context of an inspection procedure.

ES31. The training course provides understanding and knowledge of the follow-up after an inspection.

3.7. Requirements relative to the presentation of the CNIL's power to impose penalties

ES32. The training course provides understanding and knowledge of the various penalty procedures that may be implemented by the CNIL.

ES33. The training course provides understanding and knowledge of the functioning of the Data Protection Authority in its select form and the conduct of a meeting.

ES34. The training course provides understanding and knowledge of the formalism associated with a penalty procedure, the rights and obligations of the data controller in question and procedures for appeal.

ES35. The training course provides understanding and knowledge of the conditions for publication and advertising penalties.

3.8. Requirements relative to the presentation of the criminal provisions associated with non-compliance with the French data protection act

ES36. The training course provides understanding and knowledge of the conditions under which an offence of obstructing action by the CNIL is constituted.

ES37. The training course provides understanding and knowledge of the criminal penalties related to non-compliance with the requirements concerning the fair and legal collection of data.

ES38. The training course provides understanding and knowledge of the criminal penalties relative to breaches of the rights to access, rectification or objection by the person.

ES39. The training course provides understanding and knowledge of the criminal penalties related to non-compliance with requirements relative to the provision of information to persons.

ES40. The training course provides understanding and knowledge of the criminal penalties related to

non-compliance with requirements relative to prior formalities.

ES41. The training course provides understanding and knowledge of the criminal penalties related to non-compliance with requirements relative to data security.

ES42. The training course provides understanding and knowledge of the criminal penalties related to non-compliance with requirements relative to the data retention period.

ES43. The training course provides understanding and knowledge of the criminal penalties related to non-compliance with the intended purpose of processing.

ES44. The training course provides understanding and knowledge of the criminal penalties related to non-compliance with the requirements relative to the processing of sensitive data.