Decision No. 2011-316 dated 6 October 2011 adopting a standard for delivering privacy seals in audit procedures 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 audit 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 audit procedures covering the protection of persons with regard to the processing of personal data

Decides that the standard for evaluating privacy seal requests relative to audit procedures 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 Official Journal of the French Republic.

The Chair

Emmanuel de GIVRY Isabelle FALQUE-PIERROTIN

Delegate Vice-chair

Appendix: STANDARD FOR CERTIFYING AUDIT PROCEDURES COVERING THE COMPLIANCE OF PROCESSING

Introduction

A "Data Protection" audit is an audit whose criteria enable judgement of the compliance of processing personal data with the Act No. 78-17 dated 6 January 1978 (French data protection act) amended by the Act No. 2004-801 dated 6 August 2004.

The scope of such an audit concerns the processing of personal data implemented within a defined scope, not only in terms of places, organisational units, activities, processes or time periods covered, but also in terms of types of processing or specific processing.

The audit procedure describes the conduct, management and content of audits, as they are implemented by the applicant. The complete terminology is presented in the following pages.

To this end, the present standard defines the criteria for evaluation:

relating to the manner of conducting an audit (requirements concerning the method, noted "EMxx" in chapter 1);

of the processing of personal data during the audit (requirements on the content, noted "ECxx" in chapter 2).

A part of this standard (chapter 1) has been drawn up by the Data Protection Authority from the requirements of the standard NF ISO 19011 (Guidelines for quality and/or environmental management systems auditing, 2002) and by adapting them to the specific context of "Data Protection" audits. Only the original and complete text of the standard NF ISO 19011, as disseminated by AFNOR and accessible via the Internet site http://www.afnor.org/en, has normative value as an industrial standard.

To be valid, the demonstration by the organisation seeking the privacy seal from the CNIL must not merely repeat the content of the requirements to indicate that the audit procedure subject to evaluation is compliant with them. It must describe how its audit procedure specifically fulfils them by providing explanations and evidence, such as:

- a relevant extract from the internal audit standard,
- examples of questionnaires or interview scenarios used,
- a description of a method or a procedure,
- a description of software for help with decision-making or any other computerised expert system,
- screenshots illustrating IT or organisational checks,
- any other documented element available to auditors applying the audit procedure.

Terminology

Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled (according to NF ISO 19011) NOTE, when two or more audit organisations cooperate to audit a single auditee, we speak of a joint audit.
Auditee	Organisation which is audited. (NF ISO 19011)
Auditor	Person having the competence necessary to perform an audit. (NF ISO 19011)
Audit scope	Scope and limits of an audit. (NF ISO 19011) NOTE The scope generally describes the places, organisational units, activities and processes and the period of time covered.
Party instructing the audit	The organisation or person requesting an audit. (NF ISO 19011) NOTE The instructing party may be the auditee or any other organisation which has the regulatory or contractual right to request an audit.
Competence	Personal qualities and demonstrated ability to apply knowledge and aptitude. (NF ISO 19011)
Audit conclusions	Results of an audit provided by the audit team after having taken into consideration the objectives of the audit and all findings of the audit. (NF ISO 19011)
Audit findings	Results of the evaluation of the audit evidence collected, in relation to the audit criteria. (NF ISO 19011) NOTE The audit findings may indicate compliance or non-compliance with the audit criteria or opportunities for improvement.
Audit criteria	Set of policies, procedures or requirements determined. (NF ISO 19011) NOTE 1 The audit criteria are the reference in relation to which the audit evidence is compared. NOTE 2 In French, the audit criteria are often known as the audit standard.
Audit team	One or more auditors performing an audit, assisted, if necessary, by technical experts. (NF ISO 19011) NOTE 1 An auditor in the audit team is appointed manager of the audit team. NOTE 2 The audit team may include auditors under training.
Technical expert	Person bringing specific expertise or knowledge to the audit team. (NF ISO 19011) NOTE 1 This knowledge or specific expertise is relative to the organisation, the process or the activity to be audited, or it consists of linguistic or cultural assistance.

	NOTE 2 Within the audit team, a technical expert does not act as an auditor.
Audit plan	Description of the activities and provisions necessary to carry out an audit. (NF ISO 19011)
Audit evidence	Records, statements of fact or other information, which relate to the audit criteria and are verifiable. (NF ISO 19011) NOTE The audit evidence may be qualitative or quantitative.
Audit procedure	Description of all processes of managing audits implemented by the applicant.
Audit programme	Set of one or more audits planned within a given time period and for a given aim. (NF ISO 19011) NOTE An audit programme includes all activities necessary for planning, organising and implementing audits.
Audit report	Document produced by the audit team and presented to the auditee, which provides a complete, concise, accurate and clear record of the audit.

1. Standard for evaluating the method of processing compliance audits

1.1. Requirements relative to the principles to be complied with

EMOI. The applicant 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 audit.

EM02. The audit procedure includes the commitment that the auditors shall respect the principles of ethics, the impartial presentation of results, professional conscience, independence and a systematic approach.

1.2. Requirements relative to all auditors

EM03. The audit procedure ensures that the auditors have professional experience of at least five years.

EM04. The audit procedure ensures that the auditors have followed a training course on the audit methodology (principles, procedures and techniques for auditing, documents relative to the audit, laws, regulations and other relevant requirements applicable for the discipline,…) of at least twenty hours.

EM05. The audit procedure ensures that the auditors have participated in at least two audits, from their initiation to their closure, within the last two years.

EM06. The audit procedure ensures that the auditors have at least twenty days of auditing experience.

EM07. The audit procedure ensures that the auditors continue to improve professionally.

EM08. The audit procedure ensures that the auditors are evaluated according to criteria and methods

defined in the context of each audit and that auditors who do not satisfy these criteria supplement their training or their experience.

1.3. Requirements relative to the managers of the audit team

EM09. The audit procedure ensures that the managers of the audit team have participated in at least three audits, from their initiation to their closure, during the last two years.

EM10. The audit procedure ensures that the managers of the audit team have at least fifteen days of experience as manager of the audit team.

1.4. Requirements relative to "legal" auditors

EM11. The audit procedure ensures that "legal" auditors have obtained at least a Master I degree or equivalent in the legal sector.

EM12. The audit procedure ensures that "legal" auditors have experience of at least two years in the "Data Protection" field (e.g.: counsel, litigation, accomplishment of prior formalities,…).

1.5. Requirements relative to "technical" auditors

EM13. The audit procedure ensures that "technical" auditors have obtained at least a Master I degree or equivalent in the field of IT or information systems.

EM14. The audit procedure ensures that "technical" auditors have undergone training on the standards used in the management of information systems security (regulations, standards, methods, best practices, risk management…) of at least two days.

EM15. The audit procedure ensures that "technical" auditors have undergone training in the Data Protection field.

EM16. The audit procedure ensures that "technical" auditors have followed auditing training on technical security (intrusion, investigation, detection of technical vulnerabilities…) of at least two days.

EM17. The audit procedure ensures that "technical" auditors have experience of at least three years in the field of information systems security.

1.6. Requirements relative to the preparation of audits

EM18. The audit procedure ensures that the responsibilities of each person, the objectives, the scope, the criteria and the conduct of the audit are defined with the instructing party, taking into account any audits that have been carried out before.

EM19. The audit procedure ensures that the feasibility of the audit is studied and that the necessary actions are taken according to this study.

EM20. The audit procedure ensures that the audit team is constituted according to the "legal" and "technical" competencies necessary to achieve the objectives of the audit and in accordance with the principles relative to the auditors.

EM21. The audit procedure specifies the insertion of a specific clause in the contract established between the service-provider and the party instructing the audit in order to ensure the confidentiality of personal data which could, where applicable, be revealed to the service-

provider during the audit.

EM22. The audit procedure ensures that the documentation examined by the auditor is consulted on the premises of the auditee or is anonymised if it is consulted off the premises of the auditee. This principle is written in the confidentiality clause established between the service-provider and the party instructing the audit.

EM23. The audit procedure ensures that the documentation examined by the auditor is appropriate to perform the audit and that the party instructing the audit is informed of this if this is not the case. For it to be appropriate, it includes the criteria and conclusions of any audits previously done, and the internal policies relative to the protection of personal data, within the scope of the audit.

EM24. The audit procedure ensures that the instruments for collecting information that will be used by the audit team (questionnaires, interview guides, analysis software,…) are relevant with regard to the planned checks and that they are proven (preliminary tests have been carried out, prior usage has demonstrated their correctness…).

EM25. The audit procedure ensures that sampling performed (persons questioned, checks carried out, data verified…) is sufficiently representative.

EM26. The audit procedure ensures that the audit plan, the way in which the audit actions will be carried out and the communication circuits are validated with those in charge of the activities within the scope of the audit, and that their questions are handled.

EM27. The audit procedure ensures that the manager of the audit team prepares an audit plan validated by the party instructing the audit. This audit plan includes the objectives of the audit, the criteria of the audit, the reference documents, the scope of the audit, the dates, places, times and duration of the audit on site, the roles and responsibilities, and the availability of appropriate resources and possibly any objections by the auditee. The audit criteria take into account audits previously carried out and internal policies relative to the protection of personal data.

1.7. Requirements relative to the implementation of audits

EM28. The audit procedure ensures that access to and use of personal data requiring specific authorisation is restricted to duly authorised persons in accordance with the law and the regulations. This principle is written in the contract between the service-provider and the party instructing the audit.

EM29. The audit procedure checks that only persons having specific authorisation actually have access to data and can use it.

EM30. The audit procedure ensures that the auditee and, if necessary, the party instructing the audit, is regularly informed of progress and any difficulties encountered.

EM31. The audit procedure ensures that the audit evidence is constituted from a "legal" and "technical" verification of the information that is collected and retained.

EM32. The audit procedure ensures that personal data collected as evidence is either anonymised or can only be consulted on the premises of the auditee, while being retained in such a way is to ensure its confidentiality. This principle is written in the confidentiality clause established between the

service-provider and the party instructing the audit.

EM33. The audit procedure ensures that the findings of the audit are prepared by assessing the compliance of audit evidence in relation to the audit criteria.

EM34. The audit procedure ensures that the audit team prepares the conclusions of the audit based on the findings of the audit.

EM35. The audit procedure ensures that the evidence, findings and conclusions of the audit are presented to the auditee in order to check his/her understanding and have the evidence acknowledged as accurate, and that any divergence of opinion remaining following the discussion is recorded.

1.8. Requirements relative to the finalisation of audits

EM36. The audit procedure ensures that the audit report provides a complete, concise, accurate and clear record of the audit (containing at least: date of the audit report, objectives of the audit, scope of the audit, party instructing the audit, audit team, dates and places of audit activities on site, criteria of the audit, findings of the audit and conclusions of the audit), is issued by the agreed deadline unless a new issue date is fixed, is approved according to the adopted procedure and is distributed to the recipients identified by the party instructing the audit.

EM37. The audit procedure ensures that documents relative to the audit (supplied documentation, audit plan, audit evidence, audit report…) are retained in such a way as to preserve their confidentiality or destroyed in a definitive and secure manner if they are no longer relevant to the outcome of the audit.

2. Standard for evaluating the content of processing compliance audits

2.1. Requirements relative to the knowledge bases used

EC01. The audit procedure is based on a knowledge base compliant with French and community regulations. Recommendations on interpretation at the French and European levels may also be taken into account.

EC02. The audit procedure is based on a knowledge base reflecting the state of the art in information systems security, and has a method for regularly updating it.

2.2. Requirements relative to the audited organisation

EC03. The audit procedure has a method for identifying the organisational structure of the audited organisation, the information systems, the flows of information concerned and the specific legal standards within the scope of the audit.

EC04. The audit procedure assesses the existence and efficiency of the organisation and the documentation for managing the processing of personal data within the scope of the audit.

EC05. In the case where the auditee has a Personal Data Protection Officer (DPO), the audit procedure assesses the resources provided to him/her for carrying out his/her duties and the outcome of this.

2.3. Requirements relative to the identification of processes

EC06. The audit procedure describes a methodological process of listing all processes identified within the scope of the audit.

EC07. The audit procedure contains a process for detecting processes that may not be identified by the data controller within the scope of the audit.

EC08. The audit procedure identifies any use of external service-providers.

EC09. The audit procedure identifies and categorises all personal data used in the processes included within the scope of the audit.

EC 10. The audit procedure characterises the responsibility of the audited organisation with regard to processing within the scope of the audit, notably determining whether the organisation is data controller or subcontractor according to the meaning of the French data protection act.

EC 11. The audit procedure determines the national data protection law applicable to each process coming within the scope of the audit.

EC 12. The audit procedure contains a methodological approach to listing the prior formalities or elements written in the register of the Personal Data Protection Officer, if applicable, for checking their comprehensiveness and accuracy.

2.4. Requirements relative to the assessment of the legality of processes

EC13. The audit procedure can obtain an exact description of the purposes of the processes included in the scope of the audit.

EC 14. The audit procedure assesses the legal basis of each process included in the scope of the audit.

EC 15. The audit procedure includes a specific approach for determining whether the personal data used in the processing included within the scope of the audit is relevant, appropriate and not excessive with regard to the identified purposes.

EC 16. The audit procedure checks whether the personal data used is all necessary with regard to the intended purpose and whether some of it could be partially or totally anonymised, while still allowing the intended purpose to be achieved.

EC 17. The audit procedure checks the quality of the method for collecting personal data from the persons concerned, notably to assess its fair and legal character.

EC18. The audit procedure ensures that processes assigned to service-providers are the subject of a service-provision contract.

EC 19. The audit procedure ensures that contracts for the provision of services contain provisions relative to security measures and clear instructions given by the data controller to its service-provider.

EC20. The audit procedure has a method for identifying flows of data outside the European Union.

EC21. The audit procedure checks the existence and compliance of legal instructions governing transfers outside the European Union.

2.5. Requirements relative to the examination of persons accessing data

EC22. The audit procedure has a method for listing and categorising all persons who, due to their functions, are responsible for processing personal data which is included in the scope of the audit.

EC23. The audit procedure checks the authorisation policy applied to each person having legitimate access to identified data, with regard to the principle of limiting access to those who require it.

2.6. Requirements relative to the analysis of retention periods

EC24. The audit procedure includes a specific approach for listing retention periods for personal data that is used.

EC25. The audit procedure includes a specific approach for determining whether the retention periods are appropriate.

EC26. The audit procedure specifies relevant checks on the information systems by "technical" auditors in order to check whether the retention periods applied are compliant with the specified periods.

EC27. The audit procedure specifies checks to verify that the data is actually deleted upon expiration of the retention period.

EC28. The audit procedure also examines the policy on archiving personal data, if applicable, with regard to the recommendations of the CNIL in the matter.

2.7. Requirements relative to the examination of security

EC29. The audit procedure analyses and assesses the approach used by the data controllers for ensuring the confidentiality, integrity and availability of personal data coming within the scope of the audit.

EC30. The audit procedure includes a specific approach for identifying the main risks that processes within the scope of the audit cause in relation to the liberties and privacy of the persons concerned in case of a breach of security of the personal data, taking into account any subcontractors. This approach can estimate these risks in terms of seriousness and probability.

EC31. The audit procedure includes a specific approach to identifying the security measures used and for evaluating their relevance in relation to identified and estimated risks, particularly for managing security incidents related to private data.

EC32. The audit procedure can determine whether the security measures identified are correctly implemented and based on appropriate checks carried out on information systems, done by "technical" auditors.

2.8. Requirements relative to the examination of respect for the rights of persons

EC33. The audit procedure checks that the persons concerned have the right of access, rectification and, where applicable, the right of objection.

EC34. The audit procedure checks that the rights of persons can be exercised effectively and within reasonable deadlines.

EC35. The audit procedure checks that the persons have correct, accessible and clear information on their rights, and on other information specified by the Act.

2.9. Requirements relative to the examination of specific processes

EC36. The audit procedure determines the legal regime governing processing within the scope of the audit and examines compliance with the relevant specific provisions concerning the protection of personal data, notably:

- the use of sensitive data;
- processing concerning genetic data, processing concerning offences, exclusion processes, interconnections, processing using the social security number, processing concerning assessment of social difficulties of persons, biometric processes,
- processes related to health (research and evaluation of practices);
- processes for the purposes of journalism and literary and artistic expression;
- processes implementing a process of anonymisation; processes implemented by the State.