PRIVACY SEALS

ON

PRIVACY GOVERNANCE PROCEDURES

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

RÉPUBLIQUE FRANÇAISE

SUMMARY

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

Commission Nationale de l'Informatique et des Libertés

DELIBERATION NO. 2014-500 OF 11 DECEMBER 2014 ON THE ADOPTION OF A STANDARD FOR THE DELIVERANCE OF PRIVACY SEALS ON PRIVACY GOVERNANCE PROCEDURES.

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

Having regard to the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

Having regard to the amended Act No. 78-17 of 6 January 1978 on Information Technology, and Data Files and Civil Liberties, and notably Articles 11(3°, *c*) and 13;

Having regard to the Act No. 2014-344 of 17 March 2014 on consumption;

Having regard to the amended Decree No. 2005-1309 of 20 October 2005 enacted for the application of Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties;

Having regard to the Deliberation No. 2013-175 of 4 July 2013 on the adoption of an internal regulation of the Commission Nationale de l'Informatique et des Libertés, notably Articles 33 *et seq*;

After having heard Mr. Jean-François Carrez, Commissioner, on his report, and Mr. Jean-Alexandre Silvy, State Commissioner, on his observations;

Has adopted the following observations:

Article 11(3°) and (3°)(c) of the amended French Data Protection Act of 6 January 1978 states that "When requested by professional organisations or institutions of which the members are mainly data controllers... the Commission Nationale de l'Informatique et des Libertés can deliver 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".

The Act No. 2014-344 of 17 March 2014 on consumption amended the French Data Protection Act by introducing especially the CNIL's power to "determine, on its own initiative, if a product or procedure is capable of benefiting from a privacy seal".

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

The usefulness of the creation of a standard on data protection governance procedures within organisations was clearly identified by the Commission within different communications between its Departments and public organisations which expressed their interest in such a project.

The Commission has also contributed to the drafting of standards on privacy management systems which were elaborated by the *International Organization for Standardization (ISO)*. These elements confirm thus that the subject of data protection governance within organisations is a real issue at the national and international level.

The willingness of the Commission to contribute to the changing of behaviours regarding the manner of protecting personal data and privacy, of raising awareness within organisations on the upcoming obligations within the future European data protection regulation as well as of responding to the needs of identified professional sectors has led the Commission to decide to create the Privacy Governance privacy seal.

Article 33 of the CNIL internal regulation specifies that "the Commission adopts standards defining the characteristics that products and procedures must respect for the deliverance of any privacy seal. These standards specify the compliance assessment criteria in regards to the French Data Protection Act as well as the particularities regarding any subsequent verification concerning the deliverance of the privacy seal".

As a result, the present deliberation establishes the assessment standard for governance procedures aiming to protect individuals during the processing of their personal data.

The Commission has therefore decided to adopt the standard annexed to this deliberation giving leave to the assessment of Privacy Governance privacy seal requests submitted by organisations.

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

Chairwoman

I. Falque-Pierrotin

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

ANNEX

STANDARD FOR THE CERTIFICATION OF PRIVACY GOVERNANCE PROCEDURES WITHIN ORGANISATIONS

Introduction

The governance of personal data protection, also known as “Privacy Governance”, establishes the set of measures, rules and best practices that allow for the application of laws and regulations on the handling of personal data as well as provide the specific liabilities inherent to this handling.

This privacy seal is intended to help private and public organisations in the implementation of personal data protection measures and help them be accountable accordingly for their measures.

This standard defines the assessment criteria and the means at the Commission’s disposal for the assessment of privacy governance procedures’ effectiveness in protecting personal data, the objective of this privacy seal.

The Commission drew inspiration from the following sources for the drafting of one part of this standard:

The proposed European data protection regulation which defines the set of rules and measures for data protection;

The ISO standards (ISO/IEC 27001:2013 on Information security management systems and ISO/IEC DIS 29190:2014 on Privacy Capability Assessment Model) and adapting them to the practices of CNIL recognized data protection officers (Correspondants Informatique et Libertés “CILs”);

A consultation with representatives from organisations within the industry.

The standard has 25 requirements, all cumulative, which are divided into three parts:

The internal organisation concerning data protection (with requirements on data protection policy as well as on its status, training, resources, and the activities of CNIL recognized data protection officers, labelled as “EORxx” in Chapter I);

The method for assessing data processing compliance with the French Data Protection Act (with the requirements on analyses, and compliance investigations, labelled as “EMxx” in Chapter II);

The handling of claims and incidents (obligations on the handling of claims and rights of individuals, on the documentation of security events and the handling of data breaches, labelled as “EGxx” in Chapter III).

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

The applicants must demonstrate that they have satisfied the standard's requirements by providing motivated justifications as well as documented evidence. The evidence and justifications can take the forms of affidavits, internal documents describing the organisation's implemented policy, the available tools, descriptions on operating procedures, screen shots, etc... In order for the documentation to be valid, the proposed presentation must not only restate the content in their requirements for it to pass the assessment, but it must demonstrate how the assessed procedure complies with the standard in precise detail.

The applicant, a privacy seal candidate, can be a private or public organisation with an internal CNIL recognised data protection officer, which is a natural or legal person from within or outside the applicant organisation and can be shared amongst others.

Terminology

CNIL Informational workshops	Informational workshops are offered by the Data Protection Officer (CIL) Department within the CNIL to ensure a strong informational campaign. These workshops are scheduled regularly, are theme-based, and are available to different groups of people. They are for CNIL recognized Data Protection Officers (CILs), or on special admittance to individuals that will soon become a CIL and to CIL collaborators. These workshops are led by CNIL agents who work directly on the subjects at hand and by certain CILs to give feedback on their experience. The workshops aim to present the general legal principles and CNIL doctrine. They generally finish with a quiz at the end of the session with the correction given orally by the presenters.
Audits	A systematic process, independent and documented, aiming to obtain evidence and assess them objectively in order to determine to what extent the predetermined criteria were met (NF ISO 19011:2002).
Binding Corporate Rules (BCR)	Codes of conduct which define a group's policy in regard to personal data transfers. BCRs give an adequate level of protection to

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

	personal data transferred from the EU to third countries outside the EU within the same company or group.
Data Processing Mapping	Establishing an inventory of all data processing carried out by an organisation and their associated characteristics which go beyond the required notifications within the CIL registrar (Article 48 of the amended 2005 Decree).
Legally Binding Obligations	Binding obligations are standards which are enforced by law. The word "legally" should be understood broadly, namely to comply with French law (and not just the French Data Protection Act). Legally Binding Obligations are thus the set of explicit legal rules established by qualified authorities (for instance, legislative and regulatory provisions as well as other binding standards).
CNIL recognized Data Protection Officers, otherwise known as Correspondant Informatique et Libertés "CIL"	Natural or legal person from within or outside an organisation tasked with ensuring, in an independent manner sheltered from any conflict of interests, the compliance with obligations foreseen by the amended French Data Protection Act of 6 January 1978 and its amended Implementing Decree of 20 October 2005. The CIL is also called a correspondent for the protection of personal data.
Designation	The designation of a CIL by the data controller is notified to the CNIL by the signed receipt of a delivered letter or by hand delivery to the Commission secretariat, or by electronic means with proof of reception that can be delivered by the same means (Article 42 of the amended 2005 Decree). The designation can be:

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

	extensive: the CIL exercises its functions in regards to all data processing carried out by the data controller; General: the CIL exercises its functions for only the data processing that must be notified at the CNIL; Partial: the CIL is only designated for certain data processing or categories of data processing.
Personal Data Breaches	A personal data breach is any security breach that would result in the accidental or illegal destruction, loss, alteration, divulgation, or unauthorised access to the personal data being processed (Article 34 *bis* of the amended French Data Protection Act)

ASSESSMENT OF THE INTERNAL DATA PROTECTION MECHANISM

Requirements for the Personal Data Protection Policy

EOR01. The applicant implements a formal internal policy on personal data protection aiming to frame the roles and liabilities of each actor implicated in carrying out data processing within the organisation. The policy shall also specify the structure of the data processing as well as the applicable data protection general principles (single purpose which is explicit and legitimate; pertinence of the data in regard to the processing; limited data retention periods; restricted access to data; computerized and physical security measures; notification of data subjects; as well as any possible transfers of personal data outside the European Union).

EOR02. The applicant implements a data protection policy regarding external personnel subject to data processing. This policy will reintegrate the principles invoked in EOR01 and will have a clear and accessible notice which will be available in French.

EOR03. The applicant guarantees that their data protection policy is published (internally for EOR01, and externally for EOR02) and validated beforehand by the CIL each time it is modified/adopted or every three years.

Requirements for CILs

EOR04. The applicant shall designate a CIL. This designation, if “extensive”, will cover all data processing carried out by the organisation.

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

EOR05. The applicant's procedure incorporates the strategic position of the CIL by foreseeing the organisational association of the CIL with a member the organisation's executive board. In this regard, this member of the executive board or the applicant shall commit to formally meeting with the CIL in accordance with a predefined frequency, and at least annually, independently from the annual presentation of the activity report.

EOR06. The applicant formally establishes the CIL's missions within a specific document (mission statement, contract addendum, service contract, etc...).

EOR07. The applicant ensures that their CIL, a natural person, or that all individuals overseeing data protection files within a CIL legal person have mandatorily participated *a minima* in the following CNIL informational workshops: fundamental principles, data security and human resources data.

EOR08. The applicant ensures that the CIL's powers, whether natural person or all individuals overseeing data protection files within a legal person, are regularly maintained.

EOR09. The applicant demonstrates that their CIL has a dedicated annual budget and sufficient resources to fulfil their missions (time dedicated to the CIL missions, human resources, dedicated tools, etc...).

EOR10. The applicant ensures that the compliance steering is led by the CIL thanks to:

- the structuring of validation workflows for all data protection activities and the integration of the CIL within these workflows;
- the implementation of the steering tools (specifically, by the drafting of an annual activity report);
- the establishment of a network of identified personnel (named within each Department or because of their missions), which will serve as contact points for the CIL for each data processing; and
- the CIL consultation from the start of a project with data protection implications and each time the CIL believes useful for the purpose of introducing data protection principles, which can be even at the project's design stage.

EOR11. The applicant's procedure foresees that the CIL formulates a mapping of all data processing carried out by the applicant and updates for each new data processing. The expected data processing mapping will include, but may not be limited to, the following information for each data processing:

- the name (title) and address of the data controller;
- the data processing purpose(s);
- the department(s) in charge of the implementation;

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

- the title and contact information of the individual or department in charge of facilitating the exercise of data subjects' rights;
- the procedure regarding data subject notification and the exercise of their rights;
- a description of the category of processed personal data and the collection source;
- the categories and an estimation of the number of data subjects within each processing;
- the data recipients or categories of data recipients empowered to receive the data;
- the data retention period(s);
- the applicable legal framework, and when applicable, the date of the prior formalities submission and the dated CNIL decision (for processing which require a CNIL authorisation or opinion, the CIL will complete the necessary formalities with the CNIL);
- the measures taken for ensuring the security of the data;
- the existence of any data transfers outside the European Union, and when applicable, the purpose of the transfer, the categories of data subjects, the nature of the transferred data, the categories of data recipients (subsidiary, service provider, etc...), the nature of the data processing carried out by the data recipient, the country of establishment and the legal framework or guaranty giving way to the transfer (such as BCRs, Standard Contractual Clauses and the Safe Harbor);
- the existence of any sub-contracting of any activity to a data processor(along with the statement of existence, the data of the signing of the contract and the data protection clause structuring any data processing);
- the level of likelihood and gravity of any data processing risks;
- the date and the subjects of any updates;
- the procedure for obtaining consent when required;
- the utilisation of cookies when applicable.

EOR12. The applicant's procedure foresees, each year, the CIL's organisation of data protection awareness campaigns. The method, frequency and design should be adapted to the applicant's profile (such as the holding of training sessions, the diffusion of best practices, the compiling of informational material, instructional reminders, the creation of pedagogical tools and methodologies).

EOR13. The applicant's procedure foresees that the CIL is implicated in the different exchanges with the CNIL during any *ex-post* investigations:

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

- during any data protection authority investigation, the CIL shall take all necessary measures to facilitate the execution of the investigation (for example, by structuring the rules regarding the reception of the delegation and by ensuring the transmission of any requested information). The CIL shall then receive a copy of the investigation's record from the data controller and shall additionally be informed by the data controller of any follow-up actions;

- in regard to any official CNIL orders, the CIL ensures the coherence of the subsequent measures performed in response to the order as well as the respect of enforced deadlines; and

- in regard to any sanction procedures before the CNIL's Restricted Committee, the CIL shall receive a copy of the sanction's final report from the data controller, shall be consulted for the drafting of responding observations and ensure the monitoring of any actions.

THE METHOD FOR ASSESSING DATA PROCESSING COMPLIANCE WITH THE FRENCH DATA PROTECTION ACT

Requirements on the Compliance Assessment

EM01. The applicant guarantees that the CIL assesses or obtains an assessment of the data processing compliance with the French Data Protection Act of 6 January 1978 as well as the CNIL recommendations. *A minima*, this assessment should check compliance with legitimate purposes, the proportionality of the data processing, the pertinence of the data in regard to the purpose (by accessing the data except in cases of secrecy protected by law), the retention periods, the number of recipients, the structuring of relationships with data processors, clear and prior notification, the exercising of data subjects' rights, and when applicable, the transfers outside the European Union.

EM02. The applicant's procedure foresees that after the legal assessment the CIL, when applicable, shall make recommendations and propose to the data controller a plan of preventive or corrective actions.

EM03. The applicant's procedure includes a specific procedure for the preservation of confidentiality, integrity and availability of personal data in accordance to the risks presented by each implemented data processing. This procedure, carried out at least every three years, includes:

- the identification and assessment of principle data processing risks to the security of the personal data that have an impact on the data subjects' liberties and private lives. This procedure allows the applicant to evaluate the risk in terms of likelihood and gravity; and

- the determination of implemented security measures and their pertinence against the evaluated risks.

EM04. The applicant's procedure foresees that:

- the CIL ensures the execution of a risk assessment referred to in EM03; and

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

- a copy of this assessment is given to the CIL so they can address any observations to the data controller before any project's implementation.

Requirements on Compliance Supervision over Time

EM05. The applicant's procedure foresees a periodic compliance evaluation (on the basis of an internal or external audit) ensuring that the most sensitive data processing in regards to the risks identified in EM01 and EM03 are implemented in accordance with the French Data Protection Act and with the risk evaluations previously carried out. The CIL will then be the recipient of the audit results.

EM06. The applicant's procedure foresees that corrective actions are foreseen and carried out in the case of noted violations during the compliance evaluation.

ASSESSMENT OF INCIDENT AND CLAIMS HANDLING

Obligations on the Handling of Claims and on the Exercising of Data Subjects' Rights

EG01. The applicant establishes a specific procedure for the handling of claims and requests regarding the exercising of data subjects' rights (access, rectification, and objection) which include *a minima* the procedure for the exercising of said rights, the processing chain and deadlines for a response.

EG02. The applicant's procedure foresees that the CIL steers the handing of claims and requests regarding the exercising of data subjects' rights by being informed of each request, the handling of said requests, and ensuring the respect of deadlines.

EG03. The applicant's procedure foresees the implementation of claims and requests management tools for the exercising of data subjects' rights (standard responses, guides, training sessions, etc...).

Requirement on the Archiving of Security Events

EG04. The applicant's procedure foresees the implementation of an archive architecture allowing for the conservation, for a period of six months outside of specific legal constraints, of the trace of the time and context of the data security events, the devices (computer workstation, firewall, network equipment, server, etc...), the risks and the legal framework.

Requirements on the Handing of Personal Data Breaches

EG05. The applicant establishes a specific procedure for the handling of personal data breaches including:

- The detection of breaches;
- The notification of the CIL with 24 hours of the breach's detection;
- The determination of the breach's nature;

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00

- The drafting of CIL recommendations and their transmission to the data controller;
- The appropriate plan of actions which is validated by the data controller;
- The execution of corrective actions and the notification of the CIL;
- The revision of the risk assessment, when applicable.

EG06. The applicant carries out, in cases of unauthorised third party access to personal data, a notification of said access to the concerned individuals within a delay of 72 hours.

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00