Commission nationale de l'informatique et des libertés

Délibération n° 2014-500 du 11 décembre 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et libertés

NOR : *CNIL1500341X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 11 (3°, *c*) et 13 ;

Vu la loi n° 2014-344 du 17 mars 2014 relative à la consommation ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés, notamment ses articles 32 et suivants ;

Après avoir entendu M. Jean-François CARREZ, commissaire, en son rapport et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

L'article 11 (3°, *c*) de la loi du 6 janvier 1978 modifiée dispose qu'« *à la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements, la Commission nationale de l'informatique et des libertés délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la loi du 6 janvier 1978 modifiée*. »

La loi du 17 mars 2014 relative à la consommation a modifié la loi Informatique et libertés en introduisant notamment la possibilité pour la commission de « *déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label* ».

L'utilité de créer une norme de référence sur les procédures de gouvernance des données personnelles au sein des organismes a été clairement identifiée par la commission, dans le cadre des échanges entre ses services et les entreprises et organismes publics concernés, qui ont manifesté leur intérêt pour ce projet.

La commission contribue, par ailleurs, à la rédaction de normes sur les systèmes de management de la vie privée élaborées par l'*International Organization for Standardization* (ISO). Ces éléments confirment donc que le sujet de la gouvernance des données personnelles au sein des organismes reflète une véritable préoccupation tant sur le plan national qu'international.

La volonté de la commission de contribuer au changement des comportements dans la manière de protéger les données personnelles et de respecter la vie privée, de sensibiliser les organismes aux exigences du futur règlement européen sur la protection des données et de répondre aux besoins des professionnels qu'elle a identifiés ont conduit la commission à décider de créer un label en matière de gouvernance Informatique et libertés.

L'article 33 du règlement intérieur de la CNIL précise que « *la commission adopte des référentiels définissant les caractéristiques que doivent présenter des produits ou des procédures pour permettre la délivrance d'un label individuel. Ceux-ci précisent les modalités d'appréciation de la conformité à la loi et, le cas échéant, les particularités relatives aux vérifications subséquentes à la délivrance du label* ».

Par conséquent, la présente délibération fixe le référentiel d'évaluation des procédures de gouvernance tendant à la protection des personnes à l'égard du traitement des données à caractère personnel.

Décide en conséquence d'adopter le référentiel annexé à la présente délibération permettant l'évaluation des demandes de label relatives aux procédures de gouvernance des données personnelles au sein des organismes. Cette délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. FALQUE-PIERROTIN

ANNEXE

RÉFÉRENTIEL AUX FINS DE LABELLISATION DES PROCÉDURES DE GOUVERNANCE INFORMATIQUE ET LIBERTÉS AU SEIN DES ORGANISMES

Introduction

La gouvernance des données à caractère personnel, appelée gouvernance « Informatique et libertés », désigne l'ensemble des mesures, des règles et des bonnes pratiques qui permettent l'application des lois et règlements pour la gestion de ces données, et de préciser les responsabilités qui interviennent dans cette gestion.

Ce label a vocation à aider les organismes privés et publics à mettre en œuvre la protection des données et à rendre compte de l'action qu'ils mènent en la matière.

Le présent référentiel définit les critères d'évaluation et les moyens permettant à la commission de déterminer si les procédures de gouvernance, objet d'une demande de label, atteignent l'objectif visé.

Une partie de ce référentiel a été élaborée par la commission à partir :

– du projet de règlement européen relatif à la protection des données personnelles, qui définit un ensemble de règles et de mesures de protection ;

– de normes ISO (ISO/IEC 27001:2013 sur les systèmes de management de la sécurité de l'information et ISO/IEC 29190:2014 sur la maturité dans le domaine de la protection de la vie privée) en les adaptant aux pratiques des correspondants Informatique et libertés ;

– d'une concertation avec les organisations représentatives du secteur.

Il comporte vingt-cinq exigences, toutes cumulatives, réparties en trois parties :

– l'organisation interne liée à la protection des données (avec des exigences sur la politique de protection des données et sur le statut, la formation, les ressources et les activités du correspondant Informatique et libertés, notées « EORxx » dans le chapitre I) ;

– la méthode de vérification de la conformité des traitements à la loi Informatique et libertés (avec des exigences sur l'analyse et le contrôle de la conformité, notées « EMxx » dans le chapitre II) ;

– la gestion des réclamations et incidents (avec des exigences sur la gestion des réclamations et droits des personnes, sur la journalisation des événements de sécurité et sur la gestion des violations de données, notées « EGxx » dans le chapitre III).

Les demandeurs doivent démontrer qu'ils satisfont aux exigences du référentiel en fournissant des justifications argumentées et des éléments de preuves. Ceux-ci pourront prendre la forme d'attestations, de documents internes décrivant la politique mise en place, d'outils mis à disposition, de descriptifs de méthode de travail, de copies d'écran, etc. Pour être valable, la démonstration proposée ne doit pas se contenter de reprendre le contenu des exigences pour indiquer que la procédure soumise à l'évaluation est conforme à celles-ci, mais doit démontrer en quoi la procédure évaluée y répond de manière spécifique et détaillée.

Le demandeur, candidat au label, peut être un organisme privé ou public disposant obligatoirement d'un correspondant Informatique et libertés (CIL), personne physique ou personne morale, interne ou externe à l'organisme demandeur, mutualisé avec d'autres ou non.

Terminologie

Ateliers d'informations CNIL	Les ateliers d'information sont proposés par le service des correspondants de la commission dans le cadre de sa mission d'information. Ils sont programmés régulièrement et dispensés en groupe important de personnes et par thème. Ils sont réservés aux CIL ou, sur dérogation, aux personnes en voie de désignation, et exceptionnellement aux collaborateurs des CIL. Ces ateliers sont assurés par les agents de la CNIL qui travaillent sur les sujets abordés, sans condition spécifique et par certains CIL pour des retours d'expérience. Ils ont pour but de présenter les principes de la loi et la doctrine de la CNIL. Ils sont généralement assortis d'un quizz en fin de session avec une correction globale donnée à l'oral par les intervenants.
Audit	Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits (NF ISO 19011:2002).
Binding Corporate Rules (BCR)	Code de conduite définissant la politique d'un groupe d'entreprises en matière de transferts de données. Les BCR permettent d'offrir une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers à l'Union européenne au sein d'une même entreprise ou d'un même groupe.
Cartographie des traitements	Recensement de l'ensemble des traitements mis en œuvre par l'organisme et de leurs caractéristiques associés, dépassant le cadre des informations obligatoires à la tenue du registre du CIL (article 48 du décret de 2005 modifié).
Contraintes légales	Les contraintes sont des normes dotées d'une force obligatoire. Le mot « légal » doit être entendu dans son acception large, à savoir conforme au droit (et pas uniquement à la loi). Les contraintes légales comprennent donc l'ensemble des règles de droit explicites édictées par des autorités qualifiées à cet effet (dispositions législatives, réglementaires et autres normes à valeur contraignante).
Correspondant Informatique et libertés (CIL)	Personne physique ou morale, interne ou externe à l'organisme, chargée d'assurer, de manière indépendante et à l'abri de tout conflit d'intérêts, le respect des obligations prévues dans la loi du 6 janvier 1978 modifiée et de son décret d'application du 20 octobre 2005 modifié. Il est également appelé correspondant à la protection des données à caractère personnel.
Désignation	La désignation d'un CIL par le responsable de traitement est notifiée à la CNIL par lettre remise contre signature ou par remise au secrétariat de la commission contre reçu, ou par voie électronique avec accusé de réception qui peut être adressé par la même voie (art. 42 du décret de 2005 modifié). La désignation peut être : – *étendue* : le CIL exerce ses missions pour tous les traitements mis en œuvre par le responsable de traitement ; – *générale* : le CIL exerce ses missions pour les seuls traitements qui devraient faire l'objet d'une déclaration auprès de la CNIL ; – *partielle* : le CIL n'est désigné que pour certains traitements ou catégories de traitements.
Violation de données à caractère personnel	On entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement (article 34 *bis* de la loi du 6 janvier 1978 modifiée).

1. **Evaluation du dispositif interne liée à la protection des données**

1.1. *Exigences relatives à la politique de protection des données*

EOR01. Le demandeur met en place en interne une politique formalisée de protection des données personnelles visant à s'assurer du rôle et de la responsabilité de chacun des acteurs impliqués dans la mise en œuvre de traitements précisant son organisation ainsi que les grands principes de protection des données applicables (finalité déterminée, explicite et légitime, pertinence des données au regard de la finalité, durée de conservation limitée, accès restreint aux données, mesures de sécurité physiques et logiques, information des personnes et, le cas échéant, les règles en matière de transferts de données hors Union européenne).

EOR02. Le demandeur met en place une politique de protection des données personnelles à destination des personnes extérieures concernées par ses traitements. Cette politique reprend les principes évoqués à l'EOR01 et comprend une information claire, accessible et disponible en langue française.

EOR03. Le demandeur garantit que les politiques de protection des données sont diffusées (pour l'EOR01 en interne, pour l'EOR02 en externe) et validées préalablement par le correspondant Informatique et libertés à chaque nouvelle désignation et à défaut tous les trois ans.

1.2. *Exigences relatives au correspondant Informatique et libertés (CIL)*

EOR04. Le demandeur désigne un CIL dont la désignation, dite « étendue », couvre l'ensemble des traitements mis en œuvre par l'organisme.

EOR05. La procédure du demandeur assure le positionnement stratégique du CIL en prévoyant que la fonction de CIL est rattachée à un membre de l'instance exécutive. A cet égard, ce membre de l'instance exécutive ou le demandeur s'engage à recevoir formellement son CIL, selon une périodicité définie et au moins une fois par an, indépendamment de la présentation du bilan annuel d'activité.

EOR06. Le demandeur formalise dans un document spécifique les missions confiées au CIL (lettre de mission, avenant au contrat, contrat de service, etc.).

EOR07. Le demandeur s'assure que son CIL personne physique, ou que toutes les personnes supervisant des dossiers Informatique et libertés au sein du CIL personne morale ont obligatoirement et *a minima* participé à l'ensemble des ateliers d'information de la CNIL relatifs aux principes fondamentaux, à la sécurité et aux ressources humaines.

EOR08. Le demandeur s'assure que les compétences de son CIL personne physique, ou toutes les personnes supervisant des dossiers Informatique et libertés au sein du CIL personne morale, sont régulièrement entretenues.

EOR09. Le demandeur justifie que son CIL bénéficie d'un budget annuel dédié et de moyens lui permettant d'assurer ses missions (temps consacré à la mission, moyens humains, outils dédiés…).

EOR10. Le demandeur s'assure que le pilotage de la mise en conformité est réalisé par son CIL grâce à :

– la définition des circuits de validation pour l'ensemble des activités liées à la protection des données et l'intégration du CIL dans ces circuits ;
– la mise en place d'outils de pilotage (notamment par la réalisation d'un bilan annuel d'activités) ;
– l'établissement d'un réseau de personnes identifiées (nommément, par fonction ou par service) comme interlocuteurs du CIL pour chaque traitement ;
– la consultation du CIL dès l'initialisation d'un projet impliquant un traitement de données personnelles et à chaque fois qu'il le juge utile, dans le but d'introduire le respect de la protection des données dès la conception du projet.

EOR11. La procédure du demandeur prévoit que le CIL réalise une cartographie de l'ensemble des traitements mis en œuvre par le demandeur et le met à jour pour tout nouveau traitement. La cartographie attendue comprend notamment pour chaque traitement :

– le nom (dénomination) et l'adresse du responsable du traitement ;
– la ou les finalités de traitement ;
– le ou les services chargés de sa mise en œuvre ;
– la fonction de la personne ou le service auprès duquel s'exercent les droits des personnes ainsi que leurs coordonnées ;
– les modalités d'information et d'exercice des droits des personnes ;
– une description des catégories de données traitées et de l'origine de leur collecte ;
– les catégories et une estimation du nombre de personnes concernées par le traitement ;
– les destinataires ou catégories de destinataires habilités à recevoir communication des données ;
– la ou les durées de conservation des données traitées ;
– le régime juridique applicable et, le cas échéant, la date de dépôt des formalités ainsi que la décision datée de la CNIL (pour les traitements relevant des demandes d'autorisation ou d'avis, le CIL procède à l'accomplissement des formalités nécessaires auprès de la CNIL) ;
– les dispositions prises pour assurer la sécurité des données ;
– l'existence ou non d'un transfert hors Union européenne et, le cas échéant, la finalité du transfert, les catégories de personnes concernées, la nature des données transférées, les catégories de destinataires du transfert (filiale, prestataire, etc.), la nature des traitements opérés chez le destinataire, le pays d'établissement et la garantie permettant d'encadrer le transfert (telle que les BCR, clauses contractuelles types et Safe Harbor) ;
– l'existence ou non de la sous-traitance d'une activité (avec mention de l'existence et de la date de signature du contrat de sous-traitance comportant une clause Informatique et libertés) ;
– un niveau de vraisemblance et de gravité pour l'ensemble des risques liés au traitement ;
– la date et l'objet des mises à jour ;
– les modalités de recueil du consentement lorsque nécessaire ;
– l'utilisation de cookies le cas échéant.

EOR12. La procédure du demandeur prévoit, chaque année, la réalisation par le CIL d'actions de sensibilisation, avec une forme et une fréquence adaptées au contexte (telles que la tenue de formations, la diffusion de bonnes pratiques, la réalisation de supports de communication, le rappel des consignes, la création d'outils pédagogiques et méthodologiques).

EOR13. La procédure du demandeur prévoit que le CIL est associé aux échanges avec la CNIL lors de ses missions de contrôle *a posteriori :*

– dans le cadre de la réalisation d'un contrôle par l'autorité de protection des données, le CIL prend toutes les mesures utiles pour faciliter le déroulement de la mission de contrôle (définition des règles d'accueil de la délégation et assurance de la transmission des informations demandées par exemple), le CIL reçoit du responsable de traitement la copie du procès-verbal de contrôle et est également informé des suites par le responsable de traitement ;
– dans le cadre d'une mise en demeure, le CIL s'assure de la cohérence des actions réalisées suite à la mise en demeure, et du respect des délais ;

– dans le cadre de poursuites devant la formation restreinte, le CIL reçoit du responsable de traitement la copie du rapport à fin de sanction, est consulté pour la rédaction des observations en réponse et s'assure du suivi des actions.

2. **Evaluation de la méthode de vérification de la conformité des traitements à la loi Informatique et libertés**

2.1. *Exigences relatives à l'analyse de la conformité*

EM01. Le demandeur garantit que le CIL analyse ou fait analyser les traitements au regard de la loi du 6 janvier 1978 modifiée et des recommandations de la CNIL, *a minima* en termes de finalité, de proportionnalité du traitement, de pertinence des données au regard de la finalité (en accédant aux données sauf dans l'hypothèse d'un secret prévu par la loi), de durée de conservation, du nombre de destinataires, d'encadrement des relations avec les sous-traitants, d'information claire et préalable, d'exercice des droits des personnes et, le cas échéant, d'encadrement des transferts hors Union européenne.

EM02. La procédure du demandeur prévoit qu'à l'issue de son analyse juridique le CIL procède, le cas échéant, à l'élaboration de recommandations et propose au responsable de traitement un plan d'actions préventives et correctives.

EM03. La procédure du demandeur comprend une démarche particulière pour préserver la confidentialité, l'intégrité et la disponibilité des données à caractère personnel au regard des risques présentés par chaque traitement mis en œuvre. Cette démarche, révisée au moins tous les trois ans, comprend :

– l'identification et l'analyse des principaux risques liés à la sécurité des données à caractère personnel que les traitements font peser sur les libertés et la vie privée des personnes concernées. Cette démarche permet notamment d'estimer chaque risque en termes de vraisemblance et de gravité ;
– la détermination des mesures de sécurité mises en œuvre et l'évaluation de leur pertinence vis-à-vis des risques ainsi appréciés.

EM04. La procédure du demandeur prévoit que :

– le CIL s'assure de la réalisation de l'étude de risques visée à l'EM03 ;
– une copie de cette étude est remise au CIL lui permettant de faire part de ses observations au responsable de traitement avant la mise en œuvre du projet.

2.2. *Exigences relatives au contrôle de la conformité dans le temps*

EM05. La procédure du demandeur prévoit un examen de conformité périodique (par le biais d'un audit interne ou externe) permettant de s'assurer que les traitements considérés comme les plus sensibles au regard des risques identifiés à l'EM01 et l'EM03 sont mis en œuvre conformément à la loi et à l'étude des risques précédemment réalisée. Le CIL est destinataire des résultats de l'audit.

EM06. La procédure du demandeur prévoit que des actions correctives sont envisagées et réalisées en cas de manquements constatés lors de l'examen de conformité.

3. **Evaluation de la gestion des réclamations et incidents**

3.1. *Exigences relatives à la gestion des réclamations et à l'exercice des droits des personnes*

EG01. Le demandeur met en place une procédure spécifique de gestion des réclamations et des demandes relatives à l'exercice des droits des personnes (accès, rectification et opposition) comprenant *a minima* les modalités d'exercice, la chaîne de traitement et les délais de communication.

EG02. La procédure du demandeur prévoit que le CIL pilote la gestion des réclamations et demandes relatives à l'exercice des droits des personnes, notamment en étant informé de la réception de chaque demande, du traitement qui y est apporté, et en s'assurant du respect des délais.

EG03. La procédure du demandeur prévoit la mise en place d'outils d'aide à la gestion des réclamations et demandes relatives à l'exercice des droits des personnes (réponses types, guides, formations, etc.).

3.2. *Exigence relative à la journalisation des événements de sécurité*

EG04. La procédure du demandeur prévoit la mise en place d'une architecture de journalisation permettant de conserver, sur une durée de six mois hors contraintes légales spécifiques, une trace des événements de sécurité et du moment où ils ont eu lieu, en choisissant les événements à journaliser en fonction du contexte, des supports (postes de travail, pare-feu, équipements réseau, serveurs…), des risques et du cadre légal.

3.3. *Exigences relatives à la gestion des violations de données*

EG05. Le demandeur met en place une procédure spécifique de gestion des violations de données comprenant :

– la détection des violations ;
– l'information du CIL dans un délai inférieur à 24 heures à partir de la détection de la violation ;
– la détermination de la nature de la violation ;

– la formulation des recommandations du CIL et leur transmission au responsable de traitement ;
– le plan d'actions appropriées, validé par le responsable de traitement ;
– la réalisation des actions correctives et l'information du CIL ;
– la révision de l'étude des risques, le cas échéant.

EG06. Le demandeur procède, en cas d'accès par un tiers non autorisé à des données personnelles, à une notification aux personnes concernées dans un délai inférieur à 72 heures.