

Demandez votre label CNIL !

[DONNEES PERSONNELLES]

Délibérations CNIL n°2011-249 du 8 septembre 2011, n° 2011-315 et n° 2011-316 du 6 octobre 2011

La loi n°2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures avait modifié l'article 11 de la Loi Informatique et Libertés du 6 janvier 1978, en attribuant à la CNIL le pouvoir de délivrer de labels « à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel » et ce, « à la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements ».

Le 8 septembre 2011, la CNIL a modifié son règlement intérieur en intégrant notamment un nouveau chapitre IV bis intitulé « Procédure de labellisation », prévoyant le cadre dans lequel de tels labels seront créés et attribués.

En premier lieu, le texte prévoit un « comité de labellisation » composé de membres de la CNIL désignés par le président, ayant pour principales missions de :

- ✓ proposer des orientations relatives à la politique de labellisation, notamment celles relatives aux demandes de création de label.
- ✓ élaborer les projets de référentiels aux fins de labellisation de produits ou de procédures.

Toute personne souhaitant obtenir un label CNIL devra renseigner un modèle de formulaire de conformité au référentiel concerné ;

- ✓ évaluer la conformité des demandes de label aux référentiels de labellisation de produits ou de procédure. Le comité peut auditionner le demandeur ou toute personne susceptible de l'aider dans l'accomplissement de ses missions.

Une fois le formulaire de conformité adressé, la CNIL dispose d'un délai de deux mois à compter de l'attribution d'un numéro d'enregistrement pour étudier la demande, une absence de réponse à l'issue de ce délai équivalant à un refus tacite d'attribution du label.

Une fois accordé, le label est délivré pour une période de trois ans renouvelables, le titulaire du label devant, au moins six mois avant la date d'échéance, transmettre une demande de renouvellement. Le label sera alors prolongé jusqu'à ce que la CNIL se soit prononcée sur cette demande. Naturellement, si le produit ou la procédure concernée sont modifiés, le titulaire du label doit alors immédiatement en informer la CNIL afin de déterminer si ces modifications sont de nature à nécessiter une nouvelle évaluation.

A ce stade, la CNIL a adopté ses deux premiers référentiels le 6 octobre 2011, à la demande du Club EBIOS (communauté d'experts en gestion des risques) et de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP).

Le premier référentiel porte sur la délivrance de labels en matière de procédure d'audit de traitements. La CNIL précise à ce titre que ces audits concernent les traitements de données à caractère personnel au sein d'un périmètre donné (audits de traitements), et non la manière dont la protection de la vie privée est gérée (audit de gouvernance).

Ainsi, le référentiel comporte 36 exigences, divisées en deux catégories principales :

- d'une part, celles relatives à la méthode utilisée par le candidat au label, notamment au regard des démarches mises en œuvre (préparation des audits, réalisation, finalisation) et de la compétence des auditeurs, juridiques et techniques ;
- d'autre part, celles relatives au contenu de l'audit (base de connaissance utilisée, identification des traitements sujets de l'audit, durée de conservation, accès des personnes,...).

Par ailleurs, la CNIL a adopté un second référentiel pour la délivrance de labels en matière de formation, la CNIL présentant ce label comme ayant pour objet de « *contribuer à former des experts de haut niveau sur la protection des libertés et de la vie privée* ».

Le référentiel comporte 44 exigences portant principalement sur :

- l'évaluation de l'activité de formation au regard de la loi informatique et libertés (respect par le formateur de la loi informatique et libertés, identification des besoins de formation, compétence des formateurs, conditions de conception et de réalisation de la formation) ;
- sur l'évaluation du contenu de la formation.

Nul doute que ces labels constitueront une source complémentaire de sécurité juridique en matière de respect de la réglementation en vigueur en matière de données personnelles.

Olivier HAYAT