Commission nationale de l'informatique et des libertés

Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO)

NOR : *CNIL1827457X*

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 le règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 11-I-2° f *bis* ;

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, notamment son article 6-8 ;

Vu la délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO) ;

Après avoir entendu M. Maurice RONAI, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Conformément à l'article 11-I-2° f *bis* de la loi n° 78-17 modifiée, la Commission nationale de l'informatique et des libertés (ci-après, la CNIL ou la Commission) est compétente pour élaborer ou approuver les critères d'un référentiel de certification des compétences de personnes.

La présente délibération fixe les critères du référentiel de certification pour la catégorie « délégué à la protection des données », tel que visée à la section 4 du chapitre IV du règlement (UE) 2016/679.

Décide :

Les critères du référentiel annexé à la présente délibération en vue de la certification, par des organismes agréés par la Commission, des compétences du délégué à la protection des données, sont approuvés.

Le fonctionnement de ce dispositif fera l'objet, au plus tard dans un délai de deux ans à compter de son entrée en vigueur, d'une évaluation en vue d'adapter, le cas échéant, les exigences du présent référentiel.

La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. FALQUE-PIERROTIN

ANNEXE

RÉFÉRENTIEL DE CERTIFICATION DES COMPÉTENCES DU DÉLEGUÉ À LA PROTECTION DES DONNÉES (DPO)

Catégorie 1. Conditions préalables à remplir par le candidat à la certification

Exigence 1.1. Pour pouvoir accéder à la phase d'évaluation, le candidat remplit l'une des conditions préalables suivantes :

- justifier d'une **expérience professionnelle d'au moins 2 ans** dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données personnelles ; ou
- justifier d'une **expérience professionnelle d'au moins 2 ans** ainsi que d'une **formation d'au moins 35 heures** en matière de protection des données personnelles reçue par un organisme de formation.

Catégorie 2. Compétences et savoir-faire

Exigence 2.1. Le candidat connaît et comprend les principes de licéité du traitement, de limitation des finalités, de minimisation des données, d'exactitude des données, de conservation limitée des données, d'intégrité, de confidentialité et de responsabilité.

Exigence 2.2. Le candidat sait identifier la base juridique d'un traitement.

Exigence 2.3. Le candidat sait déterminer les mesures appropriées et le contenu de l'information à fournir aux personnes concernées.

Exigence 2.4. Le candidat sait établir des procédures pour recevoir et gérer les demandes d'exercice des droits des personnes concernées.

Exigence 2.5. Le candidat connaît le cadre juridique relatif à la sous-traitance en matière de traitement de données personnelles.

Exigence 2.6. Le candidat sait identifier l'existence de transferts de données hors Union européenne et sait déterminer les instruments juridiques de transfert susceptibles d'être utilisés.

Exigence 2.7. Le candidat sait élaborer et mettre en œuvre une politique ou des règles internes en matière de protection des données.

Exigence 2.8. Le candidat sait organiser et participer à des audits en matière de protection des données.

Exigence 2.9. Le candidat connaît le contenu du registre d'activités de traitement, du registre des catégories d'activités de traitement et de la documentation des violations de données ainsi que de la documentation nécessaire pour prouver la conformité à la réglementation en matière de protection des données.

Exigence 2.10. Le candidat sait identifier des mesures de protection des données dès la conception et par défaut adaptées aux risques et à la nature des opérations de traitement.

Exigence 2.11. Le candidat sait participer à l'identification des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement.

Exigence 2.12. Le candidat sait identifier les violations de données personnelles nécessitant une notification à l'autorité de contrôle et celles nécessitant une communication aux personnes concernées.

Exigence 2.13. Le candidat sait déterminer s'il est nécessaire ou non d'effectuer une analyse d'impact relative à la protection des données (AIPD) et sait en vérifier l'exécution.

Exigence 2.14. Le candidat sait dispenser des conseils en matière d'analyse d'impact relative à la protection des données (en particulier sur la méthodologie, l'éventuelle sous-traitance, les mesures techniques et organisationnelles à adopter).

Exigence 2.15. Le candidat sait gérer les relations avec les autorités de contrôle, en répondant à leurs sollicitations et en facilitant leur action (instruction des plaintes et contrôles en particulier).

Exigence 2.16. Le candidat sait élaborer, mettre en œuvre et est en capacité de dispenser des programmes de formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données.

Exigence 2.17. Le candidat sait assurer la traçabilité de ses activités, notamment à l'aide d'outils de suivi ou de bilan annuel.