Commission nationale de l'informatique et des libertés

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)

NOR : *CNIL1827455X*

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° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de 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 agréer des organismes en vue de délivrer la certification des compétences du délégué à la protection des données (ci-après « DPO ») sur la base de critères qu'elle a adoptés.

La présente délibération fixe les critères d'agrément d'organismes de certification pour la certification des compétences de personnes physiques en tant que délégué à la protection des données, tel que visé 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 l'agrément par la Commission d'organismes en charge de la certification 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 D'AGRÉMENT D'ORGANISMES DE CERTIFICATION
POUR LA CERTIFICATION DES COMPÉTENCES DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

Catégorie 1. Accréditation

Exigence 1.1. L'organisme de certification est accrédité, pendant toute la durée de son agrément par la CNIL, par un organisme d'accréditation membre de l'IAF (*International Accreditation Forum*) au regard de la norme ISO/IEC 17024 : 2012 « *Evaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes* » pour un dispositif particulier de certification de personnes.

Exigence 1.2. L'organisme de certification élabore et met en œuvre un dispositif de certification de personnes pour le DPO en conformité avec la norme ISO/IEC 17024 : 2012, les exigences fixées par le présent référentiel ainsi que les exigences fixées par le référentiel de certification des compétences du DPO (délibération n° 2018-318 du 20 septembre 2018).

Catégorie 2. Evaluation du candidat à la certification

Exigence 2.1. L'organisme de certification vérifie le respect des conditions préalables prévues à la catégorie 1 du référentiel de certification des compétences du DPO (délibération n° 2018-318 du 20 septembre 2018).

Exigence 2.2. L'organisme de certification vérifie les compétences et le savoir-faire du candidat par une épreuve écrite dont les caractéristiques répondent aux exigences suivantes.

Exigence 2.3. L'épreuve écrite consiste en un questionnaire à choix multiple (QCM) en français comprenant au moins 100 questions. 30% des questions de chacun des domaines sont énoncées sous forme de cas pratique.

Exigence 2.4. L'épreuve écrite est réalisée dans des conditions garantissant le pseudonymat lors de la correction.

Exigence 2.5. Les questions du QCM évaluent les compétences et savoir-faire s'agissant des exigences de la catégorie 2 de la délibération n° 2018-318 du 20 septembre 2018 et couvrent tous les domaines du programme figurant en annexe de la présente délibération selon la répartition suivante :

Domaine 1. – Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité : 50% des questions ;

Domaine 2. – Responsabilité : 30% des questions ;

Domaine 3. – Mesures techniques et organisationnelles pour la sécurité des données au regard des risques : 20% des questions.

Exigence 2.6. Pour chaque question, 4 réponses sont proposées dont l'une ou plusieurs sont exactes.

Exigence 2.7. Les questions du QCM sont régulièrement actualisées.

Exigence 2.8. L'épreuve écrite est réussie :

– si, au total, au moins 75% des réponses sont exactes ; et

– si, pour chacun des trois domaines, au moins 50% des réponses aux questions sont exactes.

Exigence 2.9. Les organismes de certification permettent à des observateurs de la Commission d'être présents pendant le déroulement des épreuves.

Catégorie 3. Délivrance de la certification

Exigence 3.1. L'organisme de certification délivre la certification aux candidats qui ont réussi l'épreuve écrite.

Exigence 3.2. L'organisme de certification adresse à la personne certifiée un certificat de DPO certifié portant sur le libellé « *Délégué à la protection des données certifié conformément au référentiel de certification des compétences du DPO de la CNIL* ».

Exigence 3.3. La certification est valable 3 ans à compter de sa délivrance.

Exigence 3.4. L'organisme de certification tient un registre à jour des personnes certifiées. Le registre comprend, pour chaque personne certifiée, ses nom et prénoms, la date de délivrance de la certification, la date d'expiration et le statut de la certification (délivrée, suspendue, retirée, renouvelée).

Exigence 3.5. Le registre mis à jour est transmis à la Commission tous les 6 mois à compter de la délivrance de l'agrément.

Catégorie 4. Renouvellement de la certification

Exigence 4.1. Le renouvellement de la certification est possible avant la date d'échéance du certificat à condition que la personne certifiée :

– réussisse une nouvelle épreuve écrite répondant aux exigences de la catégorie 2 du présent référentiel ; et

– démontre qu'elle dispose d'une expérience professionnelle d'au moins un an, acquise dans le courant des trois dernières années, dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données ou de la sécurité de l'information, attestée par un tiers (employeur ou client).

Catégorie 5. Matériel d'évaluation

Exigence 5.1. L'organisme de certification développe et applique son matériel d'évaluation et la documentation descriptive de sa mise en œuvre (exigences de certification) afin d'évaluer la conformité aux critères du référentiel de certification (délibération n° 2018-318 du 20 septembre 2018).

Catégorie 6. Comité de certification

Exigence 6.1. Les organismes de certification agréés invitent à leur comité du dispositif particulier un représentant de la Commission.

Catégorie 7. Eléments à fournir avec la demande d'agrément

Exigence 7.1. Les organismes de certification qui demandent à être agréés par la Commission lui fournissent un dossier comprenant :

– un extrait K-*bis* ou équivalent ;

– l'attestation d'accréditation ISO/IEC 17024 : 2012 conformément à l'exigence 1.1 de la présente délibération ;

– un document qui présente le processus de certification des compétences du DPO ; et

– leur matériel d'évaluation (notamment les questions posées et les réponses pour l'épreuve écrite) et la documentation descriptive de leur mise en œuvre (règles de certification) concernant la certification des compétences du DPO.

Catégorie 8. Eléments à fournir de manière régulière ou à la demande de la Commission

Exigence 8.1. Les organismes de certification agréés font parvenir à la Commission :

– sans délai, toute modification de leur statut d'accréditation telle que la suspension ou le retrait de l'accréditation ISO/IEC 17024 : 2012 ;
– un rapport annuel d'activité sur la certification des compétences du DPO comprenant les plaintes et réclamations à l'encontre de l'organisme de certification dans le cadre de la certification des compétences du DPO ainsi que toute difficulté rencontrée dans l'application des critères de certification des compétences du DPO adoptés dans la délibération n° 2018-318 du 20 septembre 2018 ;
– tous les 6 mois à compter de la délivrance de l'agrément, les statistiques de réussite de l'épreuve écrite ainsi que le registre actualisé des personnes certifiées DPO comprenant les noms, prénoms, la date de délivrance de la certification et la date d'expiration.

Exigence 8.2. Les organismes de certification agréés sont en mesure, à la demande de la Commission, de démontrer à tout moment le respect des exigences :

– du présent référentiel, et en particulier de l'exigence 1.2 ; et
– du référentiel de certification des compétences du DPO (délibération n° 2018-318 du 20 septembre 2018).

Annexe

Programme de l'évaluation écrite (domaines)

Domaine 1. – Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité

(50% des questions)

1.1. Règlement européen et loi française sur la protection des données – fondamentaux :

1.1.1. Champ d'application.
1.1.2. Définitions et notions.
1.1.3. Organismes soumis aux obligations règlementaires.

1.2. Règlement européen et loi française sur la protection des données – principes :

1.2.1. Licéité du traitement.
1.2.2. Loyauté et transparence.
1.2.3. Limitation des finalités.
1.2.4. Minimisation des données.
1.2.5. Exactitude des données.
1.2.6. Conservation limitée des données.
1.2.7. Intégrité, confidentialité des données.

1.3. Règlement européen et loi française sur la protection des données – validité du traitement :

1.3.1. Bases juridiques d'un traitement.
1.3.2. Consentement.
1.3.3. Consentement des mineurs.
1.3.4. Catégories particulières de données à caractère personnel.
1.3.5. Données relatives aux condamnations pénales et aux infractions.

1.4. Droits des personnes concernées :

1.4.1. Transparence et information.
1.4.2. Accès, rectification et effacement (droit à l'oubli).
1.4.3. Opposition.
1.4.4. Décisions individuelles automatisées.
1.4.5. Portabilité.
1.4.6. Limitation du traitement.
1.4.7. Limitations des droits.

1.5. Mesures prises pour la mise en conformité :

1.5.1. Politiques ou procédure en matière de protection des données
1.5.2. Qualification des acteurs d'un traitement de données : responsables du traitement, responsables conjoints du traitement, sous-traitants
1.5.3. Formalisation des relations (contrat sous-traitant, accord entre responsables conjoints du traitement).
1.5.4. Codes de conduite et certifications.

1.6. Délégué à la protection des données (DPO) :

1.6.1. Désignation et fin de mission.

1.6.2. Qualités professionnelles, connaissances spécialisées et capacité à accomplir ses missions.

1.6.3. Fonction du DPO (moyens, ressources, positionnement, indépendance, confidentialité, absence de conflit d'intérêts, formation).

1.6.4. Missions du DPO et rôle du DPO en matière d'audits.

1.6.5. Relations du DPO avec les personnes concernées et gestion des demandes d'exercice des droits.

1.6.6. Coopération du DPO avec l'autorité de contrôle.

1.6.7. Qualités personnelles, travail en équipe, management, communication, pédagogie.

1.7. Transferts de données hors de l'Union européenne :

1.7.1. Décision d'adéquation.

1.7.2. Garanties appropriées.

1.7.3. Règles d'entreprise contraignantes.

1.7.4. Dérogations.

1.7.5. Autorisation de l'autorité de contrôle.

1.7.6. Suspension temporaire.

1.7.7. Clauses contractuelles.

1.8. Autorités de contrôle :

1.8.1. Statut.

1.8.2. Pouvoirs.

1.8.3. Régime de sanction.

1.8.4. Comité européen de protection des données.

1.8.5. Recours juridictionnels.

1.8.6. Droit à réparation.

1.9. Doctrine et jurisprudence :

1.9.1. Lignes directrices du G29.

1.9.2. Avis, lignes directrices et recommandations du comité européen de protection des données.

1.9.3. Jurisprudence française et européenne.

Domaine 2. – Responsabilité

(30% des questions)

2.1. Analyse d'impact relative à la protection des données (AIPD).

2.2. Protection des données dès la conception et par défaut.

2.3. Registre des activités de traitement (responsable de traitement) et registre des catégories d'activités de traitement (sous-traitant).

2.4. Violations de données à caractère personnel, notification des violations et communication à la personne concernée.

Domaine 3. – Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

(20% des questions)

3.1. Pseudonymisation et chiffrement des données personnelles.

3.2. Mesures pour garantir la confidentialité, l'intégrité et la résilience des systèmes et des services de traitement.

3.3. Mesures permettant de rétablir la disponibilité des données et l'accès aux données en cas d'incident physique ou technique.