CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

CRITÈRES D'AGRÉMENT D'ORGANISMES DE CERTIFICATION POUR LA CERTIFICATION DE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

PROJET

Catégorie 1. Accréditation

Exigence 1.1 L'organisme de certification est accrédité 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 les activités de certification de personnes.

Exigence 1.2 L'organisme de certification applique la norme ISO/IEC 17024 :2012 pour la certification de délégué à la protection des données (DPO).

Catégorie 2. Evaluation du candidat à la certification

Exigence 2.1 L'organisme de certification vérifie les compétences et le savoir-faire du candidat par une épreuve écrite puis une épreuve orale dont les caractéristiques répondent aux exigences suivantes.

Exigence 2.2 L'épreuve écrite consiste en un questionnaire à choix multiple (QCM) en français comprenant 150 questions. 20% des questions (soit 30 questions) sont énoncées sous forme de cas pratique (règlementaire, organisationnel et technique).

Exigence 2.3 Les questions du QCM couvrent tous les domaines du programme figurant en **Annexe 1** du présent référentiel selon la répartition et la pondération suivantes :

- **Domaine 1 - réglementation générale en matière de protection des données** : réglementation européenne et française, lignes directrices et avis du G29 et du Comité européen de protection des données. Pondération : 50%, 75 questions dont 15 questions sous forme de cas pratique.

- **Domaine 2 - responsabilité :** analyse et gestion des risques des traitements de données personnelles, analyse d'impact relative à la protection des données, protection des données dès la conception et par défaut, tenue des registres. Pondération : 30%, 45 questions dont 9 questions sous forme de cas pratique.

- **Domaine 3 - mesures techniques et organisationnelles pour la sécurité des données au regard des risques**. Pondération : 20%, 30 questions dont 6 questions sous forme de cas pratique.

Exigence 2.4 Pour chaque question, 4 réponses sont proposées dont l'une seulement est exacte.

Exigence 2.5 L'épreuve écrite est réussie :
- si, au total, 75% des réponses sont exactes et
- si, pour chacun des trois domaines, 50% des réponses aux questions sont exactes.

Exigence 2.6 Seuls les candidats ayant réussi l'épreuve écrite peuvent accéder à l'épreuve orale.

Exigence 2.7 L'épreuve orale consiste en un entretien en français d'une heure.

Exigence 2.8 L'épreuve orale teste le savoir-faire du candidat s'agissant des exigences de la catégorie 2 du référentiel de la CNIL de certification de DPO.

Exigence 2.9 Chaque organisme de certification informe la CNIL de la date d'examen au moins 1 mois à l'avance.

Exigence 2.10 Les organismes de certification permettent à des observateurs de la CNIL d'être présents pendant le déroulement des épreuves.

Catégorie 3. Evaluateurs

Exigence 3.1 L'organisme de certification constitue un dossier contenant le *curriculum vitae* des évaluateurs ainsi que la documentation relative aux qualifications, formations et expérience démontrant leurs compétences, leurs aptitudes et le respect des exigences ci-dessous.

Exigence 3.2 L'évaluateur est titulaire d'un diplôme universitaire de premier cycle et justifie d'au moins 5 ans d'expérience en matière de protection des données ou de sécurité de l'information.

Exigence 3.3 L'évaluateur informe l'organisme de certification de toute relation professionnelle, familiale ou autre susceptible d'affecter l'objectivité et l'impartialité de son travail d'évaluation. Les évaluateurs dont l'indépendance peut être compromise en raison d'un conflit d'intérêts sont exclus du processus d'évaluation.

Catégorie 4. Délivrance de la certification

Exigence 4.1 L'organisme de certification délivre la certification aux candidats qui ont réussi les épreuves écrites et orales.

Exigence 4.2 L'organisme de certification adresse à la personne certifiée une attestation de certification de DPO certifié portant mention « *Délégué à la protection des données certifié conformément au référentiel de certification de DPO de la CNIL* ».

Exigence 4.3 La certification est valable 3 ans à compter de sa délivrance.

Exigence 4.4 L'organisme de certification tient un registre à jour des personnes certifiées. Le registre comprend, pour chaque personne certifiée, son nom, prénoms, la date de délivrance de la certification, la date d'expiration et le statut de la certification (délivrée, suspendue, retirée, renouvelée).

Exigence 4.5 Le registre mis à jour est transmis à la CNIL tous les 6 mois à compter de la délivrance de l'agrément.

Catégorie 5. Non-respect de la charte de déontologie du DPO certifié

Exigence 5.1 L'organisme de certification dispose d'une procédure relative à la suspension et au retrait de la certification si la personne certifiée ne respecte pas la charte de déontologie du DPO certifié.

Catégorie 6. Renouvellement de la certification

Exigence 6.1 Le renouvellement de la certification est possible à l'issue du délai de validité de 3 ans à condition que le candidat démontre :

- Avoir suivi au moins 60 heures de formation pendant la période de validité de sa certification, avec un minimum annuel de 15 heures, en matière de protection des données personnelles et

PROJET

- Disposer d'une expérience professionnelle d'au moins un an pendant la période de validité de la certification 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 7. Matériel d'évaluation

Exigence 7.1 L'organisme de certification développe et applique son matériel d'évaluation et la documentation descriptive de sa mise en œuvre (règles de certification) afin d'évaluer la conformité aux critères du référentiel de certification de DPO de la CNIL.

Catégorie 8. Comité de certification

Exigence 8.1 Les organismes de certification agréés invitent à leur comité de certification un représentant de la CNIL.

Catégorie 9. Éléments à fournir avec la demande d'agrément

Exigence 9.1 Les organismes de certification qui demandent à être agréés par la CNIL lui fournissent un dossier comprenant :
- un extrait K-bis ou équivalent ;
- un document qui présente le programme de certification de DPO ;
- l'attestation d'accréditation ISO/IEC 17024:2012 ;
- leur matériel d'évaluation (notamment les questions posées pour les épreuves écrites et orales) et la documentation descriptive de leur mise en œuvre (règles de certification) concernant la certification de DPO.

Catégorie 10. Éléments à fournir de manière régulière

Exigence 10.1 Les organismes de certification agréés font parvenir à la CNIL :
- 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 de DPO ;
- tous les 6 mois à compter de la délivrance de l'agrément, le registre actualisé des personnes certifiées DPO comprenant les noms, prénoms et la date de délivrance de la certification, la date d'expiration et le statut de la certification ;
- tous les 6 mois à compter de la délivrance de l'agrément, les plaintes et réclamations à leur encontre dans le cadre de la certification de DPO ;
- toute difficulté rencontrée dans l'application des critères de certification du DPO approuvés dans la délibération n° 2018-xxx du XXX 2018

PROJET

Annexe 1 – Démonstration du respect des conditions préalables

Formation

Le candidat doit fournir un certificat et/ou un diplôme justifiant d'avoir reçu ou dispensé une formation en matière de protection des données[1] de 60, 100 ou 180 heures selon les conditions préalables applicables de l'exigence 1.1 du référentiel de certification de DPO de la CNIL.

Expérience professionnelle

Le candidat doit justifier d'une expérience professionnelle d'au moins 2, 3 ou 5 ans dans des projets, activités ou tâches en lien avec les missions du DPO s'agissant de la protection des données. Pour ce faire, il doit fournir la preuve objective d'une expérience générale ou spécifique par une déclaration d'un employeur ou d'un client, un contrat, etc.

Si l'expérience professionnelle n'a pas duré une année complète, l'expérience de 6 mois ou plus sera comptabilisée comme une demi-année.

Si le candidat n'a pas l'expérience requise (moins d'un an d'expérience), il pourra disposer des 60 points pour une année en démontrant des qualifications additionnelles. Le tableau ci-dessous est utilisé pour calculer l'expérience professionnelle.

Expérience	Points pour une année d'expérience	Minimum de points d'expérience requis
5 ans	60 points	300 points
3 ans	60 points	180 points
2 ans	60 points	120 points

Reconnaissance de qualifications additionnelles

Si le candidat atteint le nombre de points requis s'agissant des conditions préalables en matière d'expérience professionnelle, il n'est pas nécessaire d'évaluer les qualifications additionnelles. Le tableau ci-dessous des qualifications est utilisé uniquement pour compléter le score d'un candidat qui ne dispose pas du minimum de points requis en raison de son nombre d'années d'expérience professionnelle.

Des éléments déjà pris en compte en tant que conditions préalables ne peuvent pas être considérés comme des qualifications.

Catégorie	Points maximum	Qualification	Points unitaires[2]	Max
Formation universitaire spécifique ou complémentaire sur la protection des données personnelles selon l'EEES[3]	30	Licence ou diplôme d'ingénieur	6	12
		Diplôme d'études supérieures ou maîtrise non reconnu par l'Etat	6	12
		Diplôme d'études supérieures	8	16
		Master 1	9	9
		Doctorat	10	20
Formation spécifique ou gratuite en protection des données personnelles	50	Assister à des cours, séminaires, évènements, sessions ou conférences reconnues et organisées par des organismes de formation autorisés ou par des organismes de certification (minimum 1 crédit ou 10 heures)	1	25

[1] Ces formations peuvent être celles labellisées ou certifiées par la CNIL dans le cadre de son référentiel en matière de formation relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
[2] Attribué à chaque qualification prise individuellement. Dans certains cas comme assister à des évènements, une unité a été atteinte lorsque le nombre total d'heures minimum reconnues a été crédité.
[3] Espace européen de l'enseignement supérieur.

PROJET

Catégorie	Points maximum	Qualification	Points unitaires[2]	Max
		Assister à des cours ou séminaires non universitaires organisés par des organisations professionnelles (minimum 2 crédits ou 20 heures)	0,2	10
		Assister à des cours ou séminaires universitaires (minimum 2 crédits ou 20 heures)	0,5	10
		Assister à des évènements, sessions ou conférences (au moins 20 heures par an)	0,5	5
Projet de fin d'études en matière de données personnelles	5	Valider le projet de fin d'études et avoir passé au moins 40 heures sur ce projet	1,5	5
Stages au sein d'un organisme en matière de protection des données personnelles	50	Au moins 40 heures de stage dans l'organisme	1,5	5
Expérience professionnelle en matière de protection des données personnelles	50[4]	Fonctions spécifiques en protection des données personnelles, par année d'expérience	10	30
		Professionnel ou employé exerçant des activités diverses, par projet (complexité, durée et rôle exercé seront pris en considération)	5	20
Activité d'enseignement en matière de protection des données personnelles	30	Enseignant dans un programme universitaire (pour 10 heures)	0,5	10
		Enseignant pour des cours ou séminaires - Niveau basique (pour 20 heures) - Niveau spécialisé (pour 10 heures)	0,2	5
		Intervenant d'un organisme de formation (pour 10 heures)	0,5	10
		Intervenant ou animateur de conférence (par évènement)	0,1	5
Activité de recherche et publications en matière de protection des données personnelles	20	Auteur ou co-auteur d'ouvrages	2,5	8
		Auteur ou co-auteur de chapitres d'ouvrages, de rapports de conférence ou documents similaires	0,5	5
		Auteur ou co-auteur d'articles dans des revues spécialisées	0,25	5
		Auteur ou co-auteur de contributions dans des médias ou des blogs	0,1	2
Récompenses en matière de protection des données	10	Récompenses et autres reconnaissances professionnelles	5	10
Certifications en matière de protection des données	10	Certification DPO de l'Université de Maastricht, de l'Institut européen d'administration publique, de Bureau Veritas ou certification similaire	4	10
Autres certifications sur les sujets de protection des données	10	CISA/CISM/CRISC de l'ISACA (*Information Systems Audit and Control Association*), CISSP de l'ISC, CIPP/CIPM/CIPT de l'IAPP (*International Association of Privacy Professionals*), auditeur ISO 27001 ou certification similaire	2	10

[4] Expérience autre que celle utilisée en tant que condition préalable.

PROJET

Annexe 2 : Programme de l'évaluation écrite (domaines)

Domaine 1 – Réglementation générale en matière de protection des données

(Pondération : 50%)

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 de protection des données
1.5.2 Statut des intervenants : 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 Registre des activités de traitement et registre des catégories d'activités de traitement
1.5.5 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
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

1.7 Transferts de données hors Union européenne
1.7.1 Décision d'adéquation
1.7.2 Garanties appropriées
1.7.3 Règles d'entreprise contraignantes

PROJET

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

(Pondération : 30%)

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

(Pondération : 20%)

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

3.4 Audits en matière de protection des données personnelles

PROJET