REGLES SPECIFIQUES DE CERTIFICATION DES COMPETENCES DU DELEGUE A LA PROTECTION DES DONNEES

Table des matières

1 – Domaine d'application

Le délégué à la protection des données (DPO pour « Data Protection Officer ») est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données (RGPD) au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. Cependant le DPO n'est pas personnellement responsable en cas de non-conformité de l'organisme avec le règlement.

Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions. Le RGPD, entré en vigueur le 25 mai 2018, mentionne les cas dans lesquels il est obligatoire de désigner un DPO ainsi que les modalités de désignation, sa fonction et ses missions. L'annexe 3 « Opportunité et valeur d'usage » détaille les obligations liées au RGPD ainsi que les missions de la Commission nationale de l'informatique et des libertés (CNIL).

Principalement, le DPO est chargé :

- D'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- De contrôler le respect du règlement et du droit national en matière de protection des données ;
- De conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle (la CNIL) et d'être le point de contact de celle-ci.

Le présent dispositif vise à certifier les compétences des DPO suivant les référentiels conçus par la CNIL :

- Un référentiel de certification qui fixe notamment les conditions de recevabilité des candidatures et la liste des 17 compétences et savoir-faire attendus pour être certifié ;
- Un référentiel d'agrément qui fixe les critères applicables aux organismes qui souhaitent être habilités par la CNIL à certifier les compétences du DPO sur la base du référentiel de certification élaboré par la CNIL.

Pour rappel, la certification n'est pas obligatoire pour exercer le métier de délégué à la protection des données. Inversement, il n'est pas exigé d'être désigné en tant que délégué pour être candidat à la certification des compétences du DPO.

Il s'agit d'un mécanisme volontaire permettant à tout professionnel de justifier qu'il répond aux exigences de compétences et de savoir-faire du DPO prévues par le règlement. Acteur clé de la conformité au RGPD, le DPO doit en effet disposer notamment de connaissances spécialisées du droit et des pratiques en matière de protection des données. Le certificat constitue un vecteur de confiance à la fois pour l'organisme faisant appel à ces personnes certifiées mais également pour ses usagers, clients, fournisseurs, agents ou salariés.

2 – Les références normatives et documentaires

Le dispositif particulier de certification des compétences du DPO vérifie l'ensemble des documents suivants :

- 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)
- 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)
- Norme NF EN ISO/CEI 17024 :2012 : « Évaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes »,
- Règles générales de certification des personnes (MGT 01 Doc00c),
- Règles spécifiques de certification des compétences du DPO (MGT 01 Doc00l).

3 – Dossier de Candidature

3.1 – Demande de dossier de candidature

Définies dans les règles générales (MGT 01 Doc00c).

3.2 – Validation de la candidature

Définies dans les règles générales (MGT 01 Doc00c).

3.3 – Conditions d'accès à la certification

Le DPO peut être un salarié de l'organisme ou du sous-traitant. Mais il peut aussi accomplir ses missions en signant un contrat de service. La fonction de délégué peut être exercée à temps plein ou à temps partiel. Dans ce dernier cas, le délégué ne peut occuper des fonctions au sein de l'organisme le conduisant à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie »). L'existence d'un conflit d'intérêts est donc appréciée au cas par cas.

Pour accéder aux épreuves de certification, le candidat doit remplir l'une des conditions 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 ;
- 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.

3.4 – Connaissances et aptitudes spécifiques aux missions de DPO

Le DPO doit démontrer qu'il possède les connaissances et aptitudes nécessaires pour mettre en œuvre la conformité au règlement européen sur la protection des données (RGPD) au sein de l'organisme qui l'a désigné

Pour cela, les compétences évaluées dans le cadre de cette certification sont les suivantes :

- Connaître et comprendre 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,
- Savoir identifier la base juridique d'un traitement,
- Savoir déterminer les mesures appropriées et le contenu de l'information à fournir aux personnes concernées,
- Savoir établir des procédures pour recevoir et gérer les demandes d'exercice des droits des personnes concernées,
- Connaître le cadre juridique relatif à la sous-traitance en matière de traitement de données personnelles,
- Savoir identifier l'existence de transferts de données hors Union européenne et sait déterminer les instruments juridiques de transfert susceptibles d'être utilisés,
- Savoir élaborer et mettre en œuvre une politique ou des règles internes en matière de protection des données,
- Savoir organiser et participer à des audits en matière de protection des données,
- Connaître 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,
- Savoir identifier des mesures de protection des données dès la conception et par défaut adaptées aux risques et à la nature des opérations de traitement,
- Savoir participer à l'identification des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement,
- Savoir identifier les violations de données personnelles nécessitant une notification à l'autorité de contrôle et celles nécessitant une communication aux personnes concernées,
- Savoir 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,
- Savoir 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),
- Savoir 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),
- Savoir élaborer, mettre en œuvre et être en capacité de dispenser des programmes de formation et de sensibilisation du personnel et des instances dirigeantes en matière de protection des données,
- Savoir assurer la traçabilité de ses activités, notamment à l'aide d'outils de suivi ou de bilan annuel.

3.5 – Les différentes candidatures

3.5.1 – Dossier de candidature initiale

Le dossier de candidature initiale concerne les personnes non certifiées souhaitant s'inscrire pour la première fois ou des personnes certifiées titulaires d'une certification échue (date de validité dépassée) ou retirée.

Outre l'aspect administratif, il a pour but de vérifier la validité des prérequis exigés au §3.3.

Un retour écrit est envoyé sous forme de lettre de recevabilité dans le délai d'un mois après la réception du dossier de candidature.

3.5.2 – Dossier de candidature au renouvellement de certification

Le dossier de candidature au renouvellement de la certification concerne les titulaires de certificats arrivant en fin de validité et s'applique dans le cas d'une continuité de la certification initiale.

La procédure de renouvellement est développée au paragraphe 6.4.

Un retour écrit est envoyé sous forme de lettre de recevabilité dans le délai d'un mois après la réception du dossier de candidature.

4 – Processus de certification

4.1 – Méthodes d'évaluation

Le dispositif de certification des compétences des DPO s'appuie sur les modalités d'évaluation suivantes :
Validation de de la candidature par le biais de l'étude de recevabilité du dossier de candidature et des prérequis

- Epreuve écrite : Questionnaires à Choix Multiples (QCM)

4.2 – Epreuve écrite

L'épreuve écrite est organisée sous la forme d'un questionnaire à choix multiple (QCM) portant sur les compétences et savoir-faire détaillés au §3.4.

Le cahier des charges détaillé en annexe 1 précise la composition du QCM qui respecte les exigences de la catégorie 2 de la délibération n° 2018-317 du 20 septembre 2018 à savoir :

- Il est composé de 100 questions en français qui couvrent tous les domaines du programme figurant en annexe de la délibération n° 2018-317 du 20 septembre 2018 et réparties comme ci-dessous :
  - Domaine 1 - Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité : 50 questions,
  - Domaine 2 – Responsabilité : 30 questions,
  - Domaine 3 - Mesures techniques et organisationnelles pour la sécurité des données au regard des risques : 20 questions.
- 30% des questions de chacun des domaines sont énoncées sous forme de cas pratique,
- Pour chaque question, 4 réponses sont proposées dont l'une ou plusieurs sont exactes.

Comme détaillé au §2.3 de l'annexe 4, l'ensemble des questions du QCM est analysé annuellement afin de valider l'équité des évaluations en fonction du lieu d'examen. De plus, le recueil des données et les outils statistiques permettent d'identifier d'éventuelles dérives sur certaines questions.

Aujourd'hui, le QCM contient 100 questions fixes. Conformément au cahier des charges du QCM, la base de données sera agrandie pour avoir un tirage aléatoire des questions par thème.

La validation de l'épreuve écrite respecte les critères de réussite détaillés au §4.3.

4.3 – Critères de réussite aux épreuves de certification

4.3.1 Validation de l'épreuve écrite

L'épreuve écrite est validée si :
- Le QCM est réalisé à 100%
- Le taux de bonnes réponses total est supérieur ou égal à 75%
- Le taux de bonnes réponses par domaine est supérieur ou égal à 50%

4.4 – Organisation des épreuves

4.4.1 – Validation des sessions

Définies dans les règles générales (MGT 01 Doc00c).

4.4.2 – Convocation des candidats

Définies dans les règles générales (MGT 01 Doc00c).

4.4.3 – Déroulement des épreuves

Les épreuves doivent être organisées conformément au règlement d'examen défini à l'annexe 2.

4.5 – Echec et répétition d'examen

Chaque candidat bénéficie :
- Pour l'épreuve écrite : d'un 2ème passage à -50% du prix initial après un échec notifié à la première épreuve. En cas d'échec à la 2ème épreuve, le candidat devra se réinscrire à une autre session en renseignant un bulletin de réinscription.

5 – Attribution du certificat

5.1 – Octroi du certificat

CESI Certification prend la décision d'accorder ou de refuser l'attribution du certificat en fonction des exigences applicables suivantes :
- Dossier administratif à jour et prérequis validés
- Validation de l'épreuve écrite suivant les critères de réussite définis au §4.3

Cette décision est accompagnée d'un retour écrit indiquant les écarts entre les compétences observées et les compétences attendues dans un délai de deux mois après la fin des dernières épreuves.

La personne certifiée a la possibilité de faire appel de la décision prise suivant le processus disponible sur http://www.cesi-certification.fr

5.2 – Validité

Chaque certificat de compétences du DPO délivré par CESI Certification est accordé pour une période de trois ans

5.3 – Eléments figurant sur le certificat

Les éléments figurant obligatoirement sur le certificat sont les suivants :
- Les nom et prénom du candidat,
- Ses dates et lieu de naissance,
- La date du certificat,
- La mention « Délégué à la protection des données certifié conformément au référentiel de certification des compétences du DPO de la CNIL ».,

- La période de validité du certificat,
- Le numéro d'identification du certificat.

6 – Gestion de la certification

6.1 – La surveillance

Un processus de surveillance permet de s'assurer que la personne certifiée assure le maintien de la conformité de sa compétence dans le respect du dispositif de certification tout au long de la validité de son certificat.
Dans le cas contraire, les sanctions de suspension de la certification ou de retrait peuvent être prises.

6.2 – Les sanctions

6.2.1 – Suspension de la certification pour un délai déterminé

Cette sanction est applicable dans les cas de manquements graves relatifs à la déclaration d'engagement signée par le titulaire du certificat,
Dans ce cas, le titulaire du certificat doit restituer son certificat à CESI Certification.
Cette sanction peut être levée après correction des manquements qui ont amenés la suspension, dans le délai accordé par CESI Certification. Elle peut s'accompagner d'une mesure de certification simplifiée en fonction de la durée du délai de la suspension.

La personne certifiée a la possibilité de faire appel de la décision prise suivant le processus disponible sur http://www.cesi-certification.fr

6.2.2 – Suspension volontaire à la demande de la personne certifiée

Lorsqu'une personne certifiée souhaite suspendre son certificat, elle doit en informer CESI Certification qui prononce alors sa suspension volontaire pour une durée donnée.

Cette suspension est peut-être levée ou renouvelée une fois sur demande écrite de la personne certifiée

6.2.3 – Retrait de la certification

Cette sanction est applicable en cas de manquements graves à la déclaration d'engagement signée par le titulaire du certificat restés sans effet malgré les injonctions de CESI Certification.
Dans ce cas, le titulaire du certificat doit restituer son certificat à CESI Certification.

6.3 – Certification simplifiée après suspension

La mesure de certification simplifiée applicable consiste pour le titulaire du certificat à repasser une épreuve écrite détaillée au §4.2 et adaptée le cas échéant par CESI Certification.

Cette mesure s'applique après une durée de suspension supérieure à 6 mois et uniquement sur demande écrite du certifié.

6.4 – Renouvellement de certification

Le renouvellement de certification permet au titulaire du certificat de prolonger sa durée de validité de certification. Elle ne s'applique que si la fin de la validité de la certification n'est pas dépassée et dans le cas d'une continuité de certification. La personne certifiée doit donc anticiper le passage des épreuves dans les limites de 12 mois avant la fin de validité de sa certification.

Le dossier de candidature d'une demande de renouvellement observe le §3. Une fois le dossier de candidature de renouvellement validé par CESI Certification, le candidat doit se présenter à l'épreuve écrite selon le processus de certification initiale du §4.

Pour le renouvellement, la personne certifiée doit également démontrer 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.

Les preuves peuvent provenir d'une ou plusieurs entreprises et/ou expériences professionnelles.

Chaque preuve doit être attestée par l'employeur ou le client et doit détailler :
- L'organisme dans lequel ont été réalisées les activités (l'organisme doit être identifié par un logo, un entête et/ou un pied de page),
- La fonction principale occupée dans l'organisme par le certifié,
- Le détail des activités réalisées en identifiant bien :
  - Le lien avec les missions du DPO portant sur les compétences et savoir-faire détaillés au §3.4,
  - La date et la durée des activités,
- Le nom, la fonction et la signature de la personne attestant la véracité des informations mentionnées,
- Toute preuve ne respectant pas les critères ci-dessous ne sera pas prise en compte.

Les preuves d'activités sont validées si :
- 100% des renseignements demandés sont présents,
- La durée totale de l'expérience professionnelle est supérieure ou égal à 1 an sur les 3 dernières années.

La validité des preuves vient s'ajouter aux règles d'attribution et de gestion du certificat détaillées aux §5 et §6. La durée du certificat est de 3 ans à partir de la date de fin de validité de l'ancien certificat.

En cas d'échec pour non complétude des informations, une 2ème évaluation est proposée à -50% du prix initial. En cas d'échec à la 2ème évaluation, le candidat devra se réinscrire à une autre session en renseignant un bulletin de réinscription.

La personne certifiée a la possibilité de faire appel de la décision prise suivant le processus disponible sur http://www.cesi-certification.fr

6.5 – Transfert de certification

Aucun processus de transfert n'est identifié pour la certification des compétences du DPO.

6.6 – Abandon de la certification

Les modalités d'abandon sont définies dans les règles générales (MGT01 Doc00c).

7 – Intervenants

7.1 – Comité particulier de certification

Le comité particulier de certification des compétences du DPO est responsable du maintien du présent dispositif de certification. Il doit vérifier chaque année :
- La conformité du dispositif avec les référentiels de certification (délibérations n° 2018-317 et n° 2018-318 du 20 septembre 2018),
- Le respect des exigences du dispositif dans sa mise en œuvre par l'organisme de certification

Le comité particulier de certification est constitué des collèges suivants :
- 2 à 3 représentants des personnes certifiées,
- 2 à 3 représentants d'organisme ou personnalité techniquement compétents dans le domaine,
- 1 représentant de la CNIL,
- 1 représentant de CESI Certification.

Lorsque le comité est amené à voter des décisions en séance, le vote se fait à main levé suivant les conditions suivantes :
- Chaque collège représente une voix indépendamment du nombre de représentant dans le collège,

- Pour les collèges composés de plusieurs représentants, les membres du collège se mettent d'accord sur leur vote unique,
- Le représentant de CESI Certification ne vote pas,
- La décision est adoptée si elle remporte la majorité des voix,

7.2 – Les examinateurs

7.2.1 – Dispositions communes à l'ensemble des examinateurs

Les examinateurs regroupent les évaluateurs et expert référent désignés ci-après et agréés par CESI Certification doivent, répondre aux exigences suivantes :

- Connaître le dispositif particulier de certification applicable
- Connaître de façon approfondie les méthodes et documents d'examens applicables
- Détenir la compétence appropriée du domaine à examiner
- Avoir une pratique courante aussi bien orale qu'écrite de la langue française
- Être libre de tout intérêt susceptible d'entacher leur impartialité
- Respecter la confidentialité
- Ne pas avoir eu de lien, de quelque nature que ce soit, susceptible d'entacher leur éthique, avec les candidats.

Les examinateurs peuvent appartenir à une ou plusieurs des catégories ci-après définies.

7.2.2 – L'évaluateur

L'évaluateur réalise les évaluations des preuves d'activités fournies par les personnes certifiées candidates au renouvellement au moyen des documents et des consignes fournies par CESI Certification.

Il n'y a pas d'évaluateur pour l'épreuve écrite car la correction est automatiquement réalisée sur la plateforme d'épreuve.

7.2.3 – L'expert référent

CESI Certification nommera un expert référent pour le domaine. La nomination de l'expert référent sera soumise pour avis au comité particulier.

L'expert référent participe à la conception de l'épreuve écrite et aux modalités d'évaluation.
Il participe à la conception des documents d'évaluation.
L'expert référent sera sollicité entant qu'expert technique pour l'agrément de nouveaux évaluateurs. La décision d'agrément reste sous la responsabilité du Directeur de CESI Certification qui prendra en compte l'avis technique de l'expert référent.

7.3 – Les autres intervenants

7.3.1 – Les correspondants certification

Les correspondants certification veillent au bon déroulement des épreuves écrites dans les centres d'examen, à ce titre :

- Ils préparent les salles d'examen,
- Ils appliquent les consignes liées au déroulement des épreuves,
- Ils transmettent les informations à CESI Certification conformément aux consignes.

La désignation des correspondants vérifie qu'ils n'ont pas de relations de nature à mettre en cause leur indépendance et impartialité vis-à-vis des candidats. Ils sont nommés par leur hiérarchie et leur nomination approuvée par le Directeur de CESI Certification.

7.3.2 – Autres personnes

- Le service informatique

Les autres intervenants dans le processus de certification appartiennent au service informatique attaché au centre d'examen, ils observent les mêmes règles d'indépendance et d'impartialité vis-à-vis des candidats.

8 – Règles de confidentialité et d'impartialité

Elles sont définies dans les règles générales (MGT 01 Doc00c).

9 – Les publications

Outre les règles établies dans les règles générales (MGT01 Doc00c)

CESI 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).

De plus, CESI Certification fait 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 des compétences du DPO comprenant les plaintes et réclamations à l'encontre de CESI 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.

10 – Appels et plaintes

Le traitement des appels et plaintes est défini dans les règles générales (MGT01 Doc00c).

11 – Le régime financier

Le régime financier est défini dans les règles générales (MGT01 Doc00c).