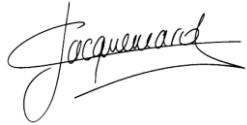


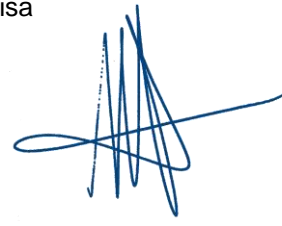
## REGLES SPECIFIQUES DE CERTIFICATION DES COMPETENCES DU DELEGUE A LA PROTECTION DES DONNEES

### HISTORIQUE DES MISES A JOUR :

Révision n°	Date	Nature de la modification
1	30.06.2019	Création
2	02.12.2019	Précision générale et modification de la formulation de « certification DPO » en « certification des compétences du DPO » dans tout le document §4.3.2 : Suppression de la durée de validité des résultats des épreuves. Cette mention n'est pas applicable pour ce dispositif qui ne contient qu'une seule épreuve écrite. §4.5 et §6.4 : Précision sur le 2 <sup>ème</sup> passage à -50% du prix initial en cas d'échec au 1 <sup>er</sup> passage §6.1 : Suppression de phrase de non existence de processus de surveillance. Le certifié doit toujours être conforme aux dispositions de sa déclaration d'engagement. §7.2.1 : Précision sur les examinateurs qui regroupent les évaluateurs et expert référent dont le rôle est détaillé dans les §7.2.2 et §7.2.3. Annexe 1 : Remplacement de la mention de nombre de questions dans base de données par l'actualisation régulière des questions.
3	30.10.2022	Mise à jour pour prise en compte des modifications de la délibération no 2022-128 du 6 octobre 2022 modifiant la délibération no 2018-317 du 20 septembre 2018
4	30.04.2023	Mise à jour pour prise en compte des modifications de la délibération no 2023-062 du 13 avril 2023 modifiant la délibération no 2018-317 du 20 septembre 2018
5	10.01.2025	<b>Mise à jour des règles d'examen</b>

Rédacteur
Responsable ODI
Visa 

Vérificateur
Responsable Qualité de CESI Certification
Visa 

Approbateur
Directeur de CESI Certification
Visa 

Ce référentiel est la propriété de **CESI SAS département** CESI Certification

**Table des matières**

<b>1 – DOMAINE D’APPLICATION</b> .....	<b>3</b>
<b>2 – LES REFERENCES NORMATIVES ET DOCUMENTAIRES</b> .....	<b>3</b>
<b>3 – DOSSIER DE CANDIDATURE</b> .....	<b>4</b>
3.1 – DEMANDE DE DOSSIER DE CANDIDATURE .....	4
3.2 – VALIDATION DE LA CANDIDATURE .....	4
3.3 – CONDITIONS D’ACCES A LA CERTIFICATION .....	4
3.4 – CONNAISSANCES ET APTITUDES SPECIFIQUES AUX MISSIONS DE DPO .....	4
3.5 – LES DIFFERENTES CANDIDATURES .....	5
<b>4 – PROCESSUS DE CERTIFICATION</b> .....	<b>5</b>
4.1 – METHODES D’EVALUATION .....	<b>ERREUR ! SIGNET NON DEFINI.</b>
4.2 – EPREUVE ECRITE.....	6
4.3 – CRITERES DE REUSSITE AUX EPREUVES DE CERTIFICATION .....	<b>ERREUR ! SIGNET NON DEFINI.</b>
4.4 – ORGANISATION DES EPREUVES .....	<b>ERREUR ! SIGNET NON DEFINI.</b>
4.5 – ECHEC ET REPETITION D’EXAMEN.....	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>5 – ATTRIBUTION DU CERTIFICAT</b> .....	<b>6</b>
5.1 – OCTROI DU CERTIFICAT .....	6
5.2 – VALIDITE .....	6
5.3 – ELEMENTS FIGURANT SUR LE CERTIFICAT .....	6
<b>6 – GESTION DE LA CERTIFICATION</b> .....	<b>7</b>
6.1 – LA SURVEILLANCE .....	7
6.2 – LES SANCTIONS .....	7
6.3 – CERTIFICATION SIMPLIFIEE APRES SUSPENSION .....	7
6.4 – RENOUELEMENT DE CERTIFICATION.....	7
6.5 – TRANSFERT DE CERTIFICATION.....	8
6.6 – ABANDON DE LA CERTIFICATION .....	8
<b>7 – INTERVENANTS</b> .....	<b>8</b>
7.1 – COMITE PARTICULIER DE CERTIFICATION.....	8
7.2 – LES EXAMINATEURS .....	9
7.3 – LES AUTRES INTERVENANTS .....	9
<b>8 – REGLES DE CONFIDENTIALITE ET D’IMPARTIALITE</b> .....	<b>9</b>
<b>9 – LES PUBLICATIONS</b> .....	<b>9</b>
<b>10 – APPELS ET PLAINTES</b> .....	<b>10</b>
<b>11 – LE REGIME FINANCIER</b> .....	<b>10</b>

## 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 délégué à la protection des données 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 délégué à la protection des données ainsi que les modalités de désignation, sa fonction et ses missions.

Principalement, le délégué à la protection des données 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 délégués à la protection des données 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 délégué à la protection des données.

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 délégué à la protection des données prévues par le règlement. Acteur clé de la conformité au RGPD, le délégué à la protection des données 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 délégué à la protection des données vérifie l'ensemble des documents suivants :

- Délibération de la CNIL 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)
- 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 de la CNIL n° 2022-128 du 6 octobre 2022 modifiant 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)
- Délibération n° 2023-062 du 13 avril 2023 modifiant 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) et 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)
- Norme NF EN ISO/CEI 17024 :2012 : « Évaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes »,
- CERT CEPE REF 36 : « Exigences spécifiques pour l'accréditation des organismes procédant à la certification des compétences du délégué à la protection des données (DPO) »
- Règles générales de certification des personnes (MGT 01 Doc00c),

- Règles spécifiques de certification des compétences du DPO (MGT 01 Doc00j).

### 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

Ce chapitre traite des conditions d'accès à la certification initiale, les obligations dans le cadre d'une recertification sont décrites au paragraphe 6.4.

Le délégué à la protection des données 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 délégué à la protection des données 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 délégué à la protection des données 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 – Organisation des épreuves

### 4.1 - Validation des sessions

Définies dans les règles générales (MGT 01 Doc00c).

### 4.2 - Convocation des candidats

Définies dans les règles générales (MGT 01 Doc00c).

### 4.3 - Déroulement des épreuves

#### 4.3.1 Accueil

***Les candidats doivent se présenter auprès de la personne chargée du déroulement des épreuves de certification.***

***Ils doivent :***

- ***Présenter leur convocation (pour un examen à distance, la connexion via le lien de la réunion Zoom fait foi),***
- ***Présenter une pièce d'identité valide,***
- ***Signer la feuille d'émargement (pour un examen à distance, l'enregistrement de la vidéo fait foi),***
- ***Signaler un éventuel conflit d'intérêt avec l'un ou plusieurs évaluateurs mentionnés au dos de la feuille d'émargement (lors d'un examen à distance, cette étape est réalisée lors du test technique).***

### 4.3.2 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 QCM respecte les exigences de la catégorie 2 de la délibération n° 2018-317 du 20 septembre 2018 modifiée 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 modifiée 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.

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. Cette analyse est une donnée d'entrée pour l'actualisation régulière des questions.

La validation de l'épreuve écrite respecte les critères de réussite détaillés au §5.1.

## 5 – Attribution du certificat

### 5.1 – Décision de CESI SAS département CESI Certification

CESI SAS département 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 suivants :
  - 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%

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>

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

### 5.2 – Validité

Chaque certificat de compétences du délégué à la protection de données délivré par CESI SAS département CESI Certification est accordé pour une durée 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 « Certifié conformément au référentiel de certification des compétences du délégué à la protection des données 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 SAS département CESI Certification. Cette sanction peut être levée après correction des manquements qui ont amenés la suspension, dans le délai accordé par CESI SAS département 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 SAS département 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 SAS département 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 §4.3 et adaptée le cas échéant par CESI SAS département 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 SAS département 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 (employeur ou client)

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 délégué à la protection des données 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 2<sup>ème</sup> évaluation est proposée à -50% du prix initial. En cas d'échec à la 2<sup>ème</sup> 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 délégués à la protection des données est constitué à minima des collègues suivants :

- Au moins un représentant des personnes certifiées,
- Au moins un représentant d'organisme ou personnalité techniquement compétents dans le domaine,
- Représentant de CESI SAS département CESI Certification.

De plus, CESI SAS département CESI Certification invite à chaque tenue de comité :

- Un représentant de la CNIL,
- Un représentant d'une association représentative de professionnels dans le secteur de la protection des données

Lorsque le comité est amené à voter des décisions en séance, le vote se fait à main levée suivant les conditions suivantes :

- Chaque collègue 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,
- Les représentations de la CNIL et d'une association de professionnels comptent pour 1 collègue chacun s'ils sont présents,
- Le représentant de CESI SAS département CESI Certification ne vote pas,
- La décision est adoptée si elle remporte la majorité des voix,



## 7.2 – Les experts référents

Les experts référents participent à la conception de l'épreuve écrite.

Les experts regroupent les personnes agréées par CESI SAS département 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 de la protection des données ou de la sécurité de l'information
- 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.

## 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 pour les examens en présentiel ou réalisent le test technique en amont de l'examen pour les examens à distance,
- Ils appliquent les consignes liées au déroulement des épreuves,
- Ils transmettent les informations à CESI SAS département 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 SAS département 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 SAS département 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 SAS département 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 délégué à la protection des données comprenant les statistiques de réussite de l'épreuve écrite, les plaintes et réclamations à l'encontre de l'organisme de certification dans le cadre de la certification des compétences du délégué à la protection des données ainsi que toute difficulté rencontrée dans l'application des critères de certification des compétences du délégué à la protection des données adoptés dans la délibération n° 2018-318 du 20 septembre 2018.

**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).