

Commission nationale de l'informatique et des libertés

Délibération 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)

NOR : CNIL2305666X

La Commission nationale de l'informatique et des libertés,

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 (règlement général sur la protection des données) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8 I 2° h ;

Vu le décret n° 2019-536 du 29 mai 2019 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 74 ;

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) ;

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 le rapport Mme Anne DEBET, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Formule les observations suivantes :

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 d'exigences qu'elle adopte ;

Le fonctionnement du dispositif de certification de personnes des compétences du DPO a fait l'objet d'une évaluation en vue d'adapter, le cas échéant, les exigences du référentiel adopté par la Commission ;

Cette délibération modifie la délibération n° 2018-317 du 20 septembre 2018, qui fixe les exigences d'agrément des organismes de certification pour la certification des compétences de personnes physiques en tant que délégué à la protection des données, tel que mentionné à la section 4 du chapitre IV du règlement (UE) 2016/679,

Décide :

1° 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) est ainsi modifiée :

a) Après la phrase : « Formule les observations suivantes », la phrase : « Conformément à l'article 11-I-2° *f bis* de la loi n° 78-17 modifiée, » est supprimée ;

b) Après l'alinéa :

« 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. », il est inséré un alinéa ainsi rédigé :

« Le fonctionnement du dispositif de certification de personnes des compétences du DPO a fait l'objet d'une évaluation, qui a conduit la Commission à modifier le référentiel par une délibération n° 2022-128 en date du 6 octobre 2022. » ;

c) Après l'alinéa :

« 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. »,

l'alinéa :

« 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. »

est remplacé par :

« L'agrément est délivré par la Commission pour une durée de cinq ans. » ;

2° Le référentiel annexé à 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) est ainsi modifié :

a) La référence à la norme ISO/IEC 17024 : 2012 est remplacée par une référence à la norme EN ISO/IEC 17024 en vigueur ;

b) L'exigence 1.1 est remplacée par les dispositions suivantes :

« Exigence 1.1. L'organisme de certification est accrédité, pendant toute la durée de son agrément par la Commission, par le *Comité Français d'Accréditation* ou par un autre organisme national d'accréditation visé par le règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 "fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) n° 339/93 du Conseil", signataire d'un accord de reconnaissance multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation au regard de la norme EN ISO/IEC 17024 en vigueur "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.

« Seule une accréditation délivrée spécifiquement pour le dispositif de certification des compétences du DPO est prise en compte par la Commission dans le cadre d'une demande initiale d'agrément ou d'une demande de renouvellement d'un agrément.

« Dans le cas où l'organisme de certification n'est pas accrédité pour ce dispositif de certification au moment de sa demande auprès de la Commission, il est autorisé, par agrément délivré par la Commission, à démarrer les activités de certification après notification d'une recevabilité opérationnelle favorable de sa demande d'accréditation par l'instance d'accréditation. Pendant cette période transitoire, l'organisme de certification délivre des certificats hors accréditation. L'organisme de certification doit obtenir l'accréditation dans un délai de douze mois à compter de la décision de recevabilité opérationnelle favorable de la part de l'instance d'accréditation. Une fois l'accréditation obtenue, l'organisme de certification transmet à la Commission l'attestation de cette accréditation et réemet les certificats sous accréditation selon les règles de l'instance d'accréditation.

« A défaut de l'obtention de cette accréditation au terme de cette échéance, l'agrément délivré par la Commission est retiré. Les certificats déjà délivrés restent valides pendant une période de six mois. Les personnes certifiées sollicitent un nouvel organisme de certification agréé par la Commission.

« L'organisme de certification informe la Commission de l'évolution du statut de son accréditation prise en compte pour l'obtention de son agrément. » ;

c) A l'exigence 1.2, après les mots : « le référentiel de certification des compétences du DPO », sont ajoutés les mots : « adoptés par la Commission » ;

d) L'exigence 1.2 est complétée par un alinéa ainsi rédigé :

« Lorsque l'organisme de certification est accrédité pour le dispositif de certification de personnes des compétences DPO, l'organisme de certification démontre la conformité aux exigences 2.3, 2.6 et 2.7 du présent référentiel dans le cadre de la procédure d'agrément de la Commission. Les autres exigences du présent référentiel sont évaluées par l'instance d'accréditation dans le cadre de la procédure d'accréditation. » ;

e) Après l'exigence 2.4 est insérée une exigence 2.4 *bis* ainsi rédigée :

« **Exigence 2.4 bis.** L'épreuve écrite peut se dérouler à distance. La lutte contre la fraude dans le cadre de cette modalité ne dispense pas l'organisme certificateur du respect des règles relatives à la protection des données (notamment au moment de la vérification de l'identité du candidat, et pendant toute la durée de l'examen). Pour ce faire, il peut prendre en compte les recommandations de la CNIL relatives aux modalités de mise en œuvre des dispositifs de télésurveillance pour les examens en ligne. » ;

f) L'exigence 3.5 est supprimée.

g) Après l'exigence 5.1 est ajoutée une exigence 5.2 ainsi rédigée :

« **Exigence 5.2.** L'organisme de certification agréé par la Commission l'informe de toute modification substantielle de son questionnaire. » ;

h) L'exigence 6.1 est complétée par les mots : « ainsi qu'un membre d'une association représentative de professionnels dans le secteur de la protection des données » ;

i) Le titre de la catégorie 7 est complétée par les mots : « ou la demande de renouvellement de l'agrément » ;

j) A l'exigence 7.1, après les mots : « Les organismes de certification qui demandent à être agréés par la Commission », sont ajoutés les mots : « ou demandent le renouvellement de leur agrément » ;

k) A l'exigence 7.1, après les mots : « conformément à l'exigence 1.1 de la présente délibération », sont ajoutés les mots : « ou la copie du courrier de recevabilité opérationnelle favorable de la demande de cette accréditation transmis par une instance d'accréditation » ;

l) A l'exigence 7.1, la phrase : « - un document qui présente le processus de certification des compétences du DPO ; et » est supprimée ;

m) A l'exigence 8.1, après les mots : « sur la certification des compétences du DPO comprenant », sont ajoutés les mots : « les statistiques de réussite de l'épreuve écrite, ».

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

Le 6 octobre 2022.

La présidente,
M.-L. DENIS