Procédure de la Commission nationale pour la protection des données (CNPD) relative à l'agrément des organismes de certification

Table des matières

Chapitre 1er — Introduction

Art. 1er. Objet de la procédure

Les demandes d'agrément d'organismes de certification introduites en vertu de l'article 43 du règlement général sur la protection des données (ci-après : « RGPD »), ainsi que de l'article 15 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ci-après: « loi du 1er août 2018 »), sont traitées par les services de la Commission nationale pour la protection des données (ci-après « Commission nationale ») d'après les modalités décrites ci-après.

Chapitre 2 — Champ d'application

Art. 2 Condition de recevabilité initiale

Un agrément en tant qu'organisme de certification peut uniquement être accordé aux personnes morales. Les personnes physiques ne peuvent pas obtenir d'agrément en tant qu'organisme de certification.

Tout organisme qui souhaite être agrée par la Commission nationale en application de l'article 43 du RGPD, de l'article 15 de la loi du 1er août 2018 et sur base des critères d'agrément adoptés par la Commission nationale par sa décision N° 8/2020 du 3 avril 2020 doit être établi sur le territoire luxembourgeois et exercer une activité opérationnelle liée à l'émission de certifications adoptées suivant l'article 42 du RGPD (critères de certification à portée nationale et critères de certification bénéficiant d'un label européen). A cet effet, un agrément est lié à un schéma de certification.

Chapitre 3 — Demande d'agrément

Art. 3 Formulaire de candidature

Le formulaire de candidature pour l'obtention d'un agrément en tant qu'organisme de certification, ainsi que des recommandations pour constituer un dossier complet, sont disponibles sur le site internet de la Commission nationale. Les décisions de la Commission nationale sur les critères d'agrément d'organismes de certification sont également disponibles sur le site internet.

Le formulaire de candidature contient une liste détaillée des informations et des documents que l'organisme de certification candidat doit fournir lors de la candidature afin que la Commission nationale analyse sa recevabilité.

Le dossier de candidature comprenant le formulaire de candidature dûment rempli et accompagné des pièces justificatives doit être envoyé soit par voie électronique à l'adresse

suivante certification@cnpd.lu (une clé de chiffrement est disponible sur le site internet pour sécuriser le transfert) soit par voie postale à l'adresse suivante :

CNPD – Service conformité - Agréments
15 boulevard du Jazz
4370 Belvaux

Le dossier de candidature peut également être déposé directement dans les locaux de la CNPD contre la remise d'un accusé de réception.

Art. 4 Redevances

L'organisme de certification candidat qui dépose une candidature d'agrément est redevable d'une redevance lors des différentes étapes de la procédure d'agrément suivant les dispositions du « Règlement N°7/2020 du 3 avril 2020 de la Commission nationale pour la protection des données fixant le montant et les modalités de paiement des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation » disponible sur le site internet de la Commission nationale. Le versement de la redevance doit être effectué avant chacune des étapes pour lesquelles une redevance est due. Une preuve de paiement doit être envoyée à la Commission nationale par voie électronique ou postale aux adresses susmentionnées.

Lors de la réception de la candidature et de la preuve de paiement de la redevance pour l'analyse préalable de la demande d'agrément (Art. 4 point a) du règlement N°7/2020), la Commission nationale accuse réception du dossier de candidature à l'organisme de certification candidat.

Chapitre 4 — Equipe d'audit

Art. 5 Commissaire en charge

Le commissaire en charge du service « Conformité » diligente l'audit d'agrément et désigne l'équipe d'audit qui, sous sa supervision, procède à l'analyse préliminaire de la candidature et, le cas échéant, à l'audit d'agrément.

Chapitre 5 — Revue préliminaire de la candidature

Art. 6 Déroulement de la revue préliminaire

L'objectif de la revue préliminaire est d'analyser la complétude et la qualité du dossier de candidature par rapport aux critères d'agrément.

L'équipe d'audit effectue une revue globale préliminaire de l'organisme de certification candidat basée sur :

a) un entretien préliminaire avec l'organisme de certification candidat,
b) les informations remplies dans le formulaire d'autoévaluation de la maturité en matière de certification de l'organisme de certification candidat,
c) les documents fournis par l'organisme de certification candidat.

Art. 7 Acceptation de la demande d'agrément

Suite à la revue préliminaire de la candidature, la Commission nationale accepte la demande d'agrément et démarre un audit d'agrément, sous la condition que le dossier correspond aux critères d'agrément et reflète une maturité suffisante.

Une candidature mature s'appuie sur un environnement de contrôle qui correspond aux critères d'agrément, sur une documentation complète, claire et précise ainsi que sur des preuves de conformité fournies à la Commission nationale.

Si la candidature est incomplète et/ou jugée insuffisamment mature pour démarrer un audit d'agrément, le dossier est clos. L'organisme de certification a toutefois la possibilité de soumettre une nouvelle demande d'agrément.

La Commission nationale informe l'organisme de certification de l'acceptation ou de la clôture de la demande d'agrément.

Chapitre 6 — Le déroulement de l'audit d'agrément

Art. 8 Planification de l'audit d'agrément

Le gestionnaire principal désigné parmi l'équipe d'audit dresse la planification de l'audit d'agrément sous la supervision du commissaire en charge du service « Conformité » et définit les éléments ci-dessous :

a) le ou les nom(s) de ou du/des membre(s) l'équipe d'audit à laquelle le commissaire en charge du service « Conformité délègue l'exécution de l'audit d'agrément,
b) le calendrier d'intervention et le périmètre de travail,
c) la réunion d'ouverture avec l'organisme audité destinée à convenir sur le périmètre de travail et sur le calendrier d'intervention.

Art. 9 Déroulement de l'audit d'agrément

1 ^{0} Evaluation de l'organisme de certification candidat

L'audit d'agrément a pour objectif d'évaluer si l'organisme de certification candidat répond aux critères d'agrément publiés par la Commission nationale.

Le commissaire en charge du service « Conformité » procède à toutes les diligences utiles avec le concours de l'équipe d'audit et des services de la Commission nationale. L'équipe

d'audit peut s'entretenir avec toute personne employée de l'organisme de certification candidat dont l'audition lui paraît utile.

L'équipe d'audit peut demander communication de tout document nécessaire à l'accomplissement de l'audit d'agrément, quel qu'en soit le support, et en prendre copie. Elle peut recueillir sur place tout renseignement et toute justification utile et nécessaire à l'accomplissement de l'audit d'agrément.

Lorsque des documents n'ont pas pu être transmis ou pris en copie pour des raisons motivées, l'organisme de certification candidat est obligé de les conserver dans l'état tel qu'ils ont été consultés pendant toute la durée de vie d'agrément, si ce dernier est octroyé.

2^0 Identification et communication des non-conformités

Une non-conformité est une lacune décelée dans l'organisation de l'organisme de certification candidat résultant d'une exigence d'agrément non-traitée ou traitée partiellement, mais n'ayant pas d'incidence directe sur la fiabilité du système de management des activités de certification.

Une non-conformité majeure est une lacune importante dans l'organisation et dans la gouvernance présentant un risque important pour l'activité de certification.

Des non-conformités peuvent être identifiées par l'équipe d'audit pendant la période d'évaluation. Ces dernières seront communiquées à l'organisme de certification candidat par l'équipe d'audit.

Le cas échéant, la Commission nationale formalisera la nécessité d'un plan de remédiation à soumettre par l'organisme de certification candidat.

3^0 Plan de remédiation

L'organisme de certification candidat dispose de 30 jours ouvrés, à partir de la date de notification par la Commission nationale, pour soumettre un plan de remédiation à la Commission nationale.

Si l'organisme de certification ne souhaite pas soumettre ou ne soumet pas un plan de remédiation dans le délai précité, le dossier est clos au plus tard 30 jours après la notification par la Commission nationale de la nécessité de mise en œuvre d'un plan de remédiation à l'organisme de certification candidat.

4^0 Revue des actions correctives

L'organisme de certification candidat dispose de trois mois pour implémenter les actions correctives mentionnées dans le plan de remédiation. Les trois mois sont comptés à partir de la date de réception du plan de remédiation.

La Commission nationale effectuera une revue des actions correctives implémentées pour lesquelles l'organisme de certification candidat fournira une documentation claire et des preuves de mise en œuvre.

Si le délai n'est pas respecté, l'audit est clôturé.

5^0 Rapport d'audit d'agrément

Un rapport d'audit présentera les conclusions de l'évaluation de l'organisme de certification candidat par rapport aux critères d'agrément.

6^0 Réunion de clôture

L'équipe d'audit effectuera une réunion de clôture avec l'organisme de certification candidat afin d'échanger sur les conclusions du rapport d'audit d'agrément.

Chapitre 7 — Décision d'agrément

Art. 10 Transmission du rapport d'audit au Collège

Le rapport d'audit d'agrément sera communiqué et présenté au Collège de la Commission nationale qui prendra une décision sur l'octroi de l'agrément à l'organisme de certification candidat.

Art. 11 Acceptation ou refus d'octroi d'un agrément

Le collège prendra la décision d'acceptation ou de refus de l'octroi d'agrément de l'organisme de certification candidat conformément aux dispositions de l'article 10 du Règlement d'ordre intérieur de la Commission nationale adopté par décision n° 3AD/2020 en date du 22.01.2020.

La décision d'octroi d'agrément sera envoyée accompagnée du rapport d'audit d'agrément à l'organisme de certification candidat.

Chapitre 8 — Emission du certificat

Art. 12 Certificat d'agrément

En cas d'acceptation d'octroi de l'agrément, un certificat d'agrément sera transmis à l'organisme de certification candidat.

Chapitre 9 — Validité de l'agrément

Art. 13 Audit de renouvellement

L'agrément octroyé est valable cinq ans. Passé ce délai, l'organisme de certification souhaitant continuer l'activité de certification sous le RGPD a la possibilité d'effectuer une demande de renouvellement de son agrément via un formulaire disponible sur le site Internet de la Commission nationale. Le dossier de demande de renouvellement comprenant le formulaire de candidature dûment rempli et accompagné des pièces justificatives doit être envoyé soit par voie électronique soit par voie postale aux adresses susmentionnées (cf. Art. 3).
Le dossier de demande de renouvellement peut également être déposé directement dans les locaux de la CNPD contre la remise d'un accusé de réception.
La demande de renouvellement doit être déposée au moins six mois avant l'expiration de l'agrément afin d'assurer une continuité de l'agrément.

Chapitre 10 — Audit de surveillance

Art. 14 Surveillance

La Commission nationale procédera à des audits de surveillance des organismes de certifications agréées. Durant la période de validité d'un agrément, les audits de surveillance couvriront toutes les sections des exigences d'agrément auxquelles les organismes de certification sont soumis.

Ainsi décidé à l'unanimité des voix à Belvaux, le 21.04.2021

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann	Marc Lemmer
Présidente	Commissaire	Commissaire	Commissaire