Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données (2016/679)

Version 3.0

4 juin 2019

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Adopté

Historique des versions

Version 3.0	4 juin 2019	Ajout de l'annexe 1 (version 2.0 de l'annexe 1 adoptée le 4 juin 2019 après consultation publique)
Version 2.0	4 décembre 2018	Adoption des lignes directrices après une consultation publique; le même jour, l'annexe 1 (version 1.0) a été adoptée pour consultation publique.
Version 1.0	6 février 2018	Adoption des lignes directrices par le groupe de travail «article 29» (version destinée à une consultation publique). Cette version a été approuvée par le comité européen de la protection des données le 25 mai 2018.

Table des matières

Le comité européen de la protection des données

vu l'article 70, paragraphe 1, point e), du 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,

vu les résultats de la consultation publique sur les lignes directrices qui a eu lieu en février 2018 et de celle sur l'annexe qui s'est tenue entre le 14 décembre 2018 et le 1er février 2019, conformément à l'article 70, paragraphe 4, du règlement général sur la protection des données,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

1 INTRODUCTION

1. Le règlement général sur la protection des données [règlement (UE) 2016/679, ci-après le «RGPD»], entré en vigueur le 25 mai 2018, offre un cadre de conformité modernisé et basé sur la responsabilité et les droits fondamentaux en matière de protection des données en Europe. Un ensemble de mesures destinées à faciliter le respect des dispositions du RGPD est au cœur de ce nouveau cadre. Celles-ci comprennent des exigences obligatoires dans des circonstances spécifiques (y compris la nomination de délégués à la protection des données et l'exécution d'analyses d'impact relatives à la protection des données) ainsi que des mesures volontaires telles que des codes de conduite et des mécanismes de certification.

2. Dans le cadre de la mise en œuvre des mécanismes de certification et des labels ou marques en matière de protection des données, en vertu de l'article 43, paragraphe 1, du RGPD, les États membres sont tenus de garantir que les organismes de certification qui délivrent la certification au titre de l'article 42, paragraphe 1, sont agréés par l'autorité de contrôle compétente ou l'organisme national d'accréditation, ou les deux. Si l'organisme national d'accréditation procède à l'agrément conformément à la norme ISO/IEC 17065:2012, les exigences supplémentaires établies par l'autorité de contrôle compétente doivent également être appliquées.

3. Des mécanismes de certification pertinents peuvent améliorer la conformité au RGPD et la transparence pour les personnes concernées ainsi que dans les relations au sein du commerce interentreprises, par exemple entre les responsables du traitement et les sous-traitants. Les responsables du traitement et les sous-traitants bénéficieront d'une attestation indépendante d'un tiers aux fins de démontrer que leurs opérations de traitement respectent le présent règlement[1].

[1] En vertu du considérant 100 du RGPD, la mise en place de mécanismes de certification peut améliorer la transparence et le respect dudit règlement et permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.

4. Dans ce contexte, le comité européen de la protection des données (ci-après dénommé le «comité») reconnaît qu'il est nécessaire de fournir des lignes directrices relatives à l'agrément. L'agrément a pour valeur et but particuliers d'attester avec l'autorité nécessaire les compétences des organismes de certification, ce qui permet d'instaurer la confiance envers le mécanisme de certification.

5. Les présentes lignes directrices visent à offrir des orientations quant à l'interprétation et à la mise en œuvre des dispositions de l'article 43 du RGPD, notamment à aider les États membres, les autorités de contrôle et les organismes nationaux d'accréditation à établir une base cohérente et harmonisée pour l'accréditation des organismes de certification qui délivrent une certification conformément au RGPD.

2 CHAMP D'APPLICATION DES LIGNES DIRECTRICES

6. Les présentes lignes directrices:

- définissent le but de l'agrément dans le cadre du RGPD;
- expliquent les différentes façons d'agréer des organismes de certification conformément à l'article 43, paragraphe 1, et repèrent les principales questions à prendre en considération;
- fournissent un cadre pour établir des exigences supplémentaires en matière d'agrément lorsque ce dernier est géré par l'organisme national d'accréditation; et
- établissent un cadre visant à définir des exigences en matière d'agrément lorsque ce dernier est géré par l'autorité de contrôle.

7. Les présentes lignes directrices ne constituent pas un manuel de procédure aux fins de l'agrément des organismes de certification dans le respect du RGPD. Elles n'établissent pas une nouvelle norme technique en matière d'agrément des organismes de certification aux fins du RGPD.

8. Ces lignes directrices sont destinées aux entités suivantes:

   - les États membres, qui doivent garantir que les organismes de certification sont agréés par l'autorité de contrôle et/ou par l'organisme national d'accréditation;
   - les organismes nationaux d'accréditation qui procèdent à l'agrément des organismes de certification au titre de l'article 43, paragraphe 1, point b);
   - l'autorité de contrôle compétente qui détermine des «exigences supplémentaires» à celles visées dans la norme ISO/IEC 17065:2012[2] lorsque c'est l'organisme national d'accréditation qui procède à l'agrément au titre de l'article 43, paragraphe 1, point b);
   - le comité, lorsqu'il publie un avis concernant les exigences en matière d'agrément de l'autorité de contrôle compétente et les approuve, en vertu de l'article 43, paragraphe 3, de l'article 70, paragraphe 1, point p), et de l'article 64, paragraphe 1, point c);

[2] Organisation internationale de normalisation: Évaluation de la conformité – Exigences pour les organismes certifiant les produits, les procédés et les services.

- l'autorité de contrôle compétente qui détermine les exigences en matière d'agrément lorsque c'est l'autorité de contrôle qui procède à l'agrément au titre de l'article 43, paragraphe 1, point a);
- d'autres acteurs, tels que de potentiels organismes de certification ou les propriétaires de programmes de certification qui proposent des critères et des procédures de certification[3].

9. Définitions

10. Les définitions suivantes visent à permettre une compréhension commune des éléments de base du processus d'agrément. Elles doivent être considérées comme des points de référence et ne prétendent pas être inattaquables. Ces définitions sont fondées sur les normes et les cadres réglementaires existants, en particulier sur les dispositions pertinentes du RGPD et de la norme ISO/IEC 17065:2012.

11. Les définitions suivantes s'appliquent aux fins des présentes lignes directrices:

12. «agrément» des organismes de certification: voir section 3 sur l'interprétation de l'agrément aux fins de l'article 43 du RGPD;

13. «exigences supplémentaires»: exigences établies par l'autorité de contrôle compétente et en vertu desquelles l'agrément est effectué[4];

14. «certification»: évaluation et attestation impartiale par un tiers[5] selon laquelle le respect des critères de certification a été prouvé;

15. «organisme de certification»: organisme tiers d'évaluation[6] de la conformité[7] qui applique un mécanisme de certification[8];

16. «programme de certification»: programme de certification lié à des produits, processus et services particuliers auxquels s'appliquent les mêmes exigences, règles et procédures spécifiques[9];

---

[3] Un propriétaire de programme est une organisation identifiable qui a établi des critères et des exigences en matière de certification lesquels servent à évaluer la conformité. L'agrément concerne l'organisation qui procède aux évaluations (article 43, paragraphe 4) en fonction des exigences du programme de certification et délivre les certifications (c'est-à-dire l'organisme de certification, également appelé organisme d'évaluation de la conformité). Il est possible que l'organisation qui effectue les évaluations soit la même que celle ayant élaboré le programme et en est propriétaire, mais des arrangements peuvent exister selon lesquels une organisation est propriétaire du programme et une autre (ou plusieurs autres) effectue(nt) les évaluations.

[4] Article 43, paragraphes 1, 3 et 6.

[5] Il convient de noter qu'en vertu de la norme ISO 17000, l'attestation réalisée par une tierce partie (certification) «recouvre tous les objets de l'évaluation de la conformité» (5.5) «excepté les organismes d'évaluation de la conformité proprement dits, auxquels l'accréditation est applicable» (5.6).

[6] L'opération d'évaluation de la conformité par une tierce partie est effectuée par une organisation indépendante de la personne ou de l'organisation qui fournit l'objet et des intérêts de l'utilisateur concernant cet objet, cf. ISO 17000, 2.4.

[7] Voir ISO 17000, 2.5: «organisme qui fournit des services d'évaluation de la conformité»; ISO 17011: «organisme qui exerce des activités d'évaluation de la conformité et qui peut être l'objet d'une accréditation»; ISO 17065, 3.12.

[8] Article 42, paragraphes 1 et 5, du RGPD.

[9] Voir point 3.9, lu conjointement avec l'annexe B, de la norme ISO 17065.

17. «critères» ou critères de certification: critères en vertu desquels une certification (évaluation de la conformité) est effectuée[10];

18. «organisme national d'accréditation»: l'unique organisme dans un État membre, désigné conformément au règlement (CE) nº 765/2008 du Parlement européen et du Conseil, qui procède à des agréments en vertu d'une autorité qui lui est conférée par l'État[11].

3 INTERPRÉTATION DU TERME «AGRÉMENT» AUX FINS DE L'ARTICLE 43 DU RGPD

19. Le RGPD ne propose pas de définition du terme «agrément». À l'article 2, point 10, du règlement (CE) nº 765/2008, qui établit des exigences générales en matière d'agrément (désigné par le terme «accréditation» dans ledit règlement), l'agrément/l'accréditation est défini(e) comme une

20. «attestation délivrée par un organisme national d'accréditation selon laquelle un organisme d'évaluation de la conformité satisfait aux critères définis par les normes harmonisées et, le cas échéant, à toute autre exigence supplémentaire, notamment celles fixées dans les programmes sectoriels pertinents, requis pour effectuer une opération spécifique d'évaluation de la conformité».

21. Conformément à la norme ISO/IEC 17011,

22. on entend par «agrément» (désigné par le terme «accréditation» dans la norme) une «attestation délivrée par une tierce partie, ayant rapport à un organisme d'évaluation de la conformité, constituant une reconnaissance formelle de la compétence de ce dernier à réaliser des activités spécifiques d'évaluation de la conformité».

23. L'article 43, paragraphe 1, dispose ce qui suit:

24. «Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente au titre des articles 57 et 58, les organismes de certification disposant d'un niveau d'expertise approprié en matière de protection des données délivrent et renouvellent les certifications, après en avoir informé l'autorité de contrôle pour qu'elle puisse exercer au besoin les pouvoirs qui lui sont dévolus en vertu de l'article 58, paragraphe 2, point h). Les États membres veillent à ce que ces organismes de certification soient agréés par une des entités suivantes ou les deux:

    (a) l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56;
    (b) l'organisme national d'accréditation désigné conformément au règlement (CE) nº 765/2008 du Parlement européen et du Conseil, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56.»

25. En ce qui concerne le RGPD, les exigences en matière d'agrément sont déterminées par:

[10] Voir article 42, paragraphe 5.
[11] Voir article 2, paragraphe 11, du règlement (CE) nº 765/2008.

- la norme ISO/IEC 17065:2012 et les «exigences supplémentaires» établies par l'autorité de contrôle compétente, en vertu de l'article 43, paragraphe 1, point b), lorsque c'est l'organisme national d'accréditation qui effectue l'agrément, et par l'autorité de contrôle lorsque cette dernière effectue elle-même l'agrément.

26. Dans les deux cas, les exigences consolidées doivent couvrir les exigences visées à l'article 43, paragraphe 2.

27. Le comité reconnaît que l'agrément a pour but d'attester avec l'autorité nécessaire la compétence d'un organisme pour effectuer une certification (activités d'évaluation de la conformité)[12]. Au sens du RGPD, l'agrément s'entend comme suit:

28. une attestation[13] délivrée par un organisme national d'accréditation et/ou par une autorité de contrôle, selon laquelle un organisme de certification[14] est qualifié pour procéder à une certification conformément aux articles 42 et 43 du RGPD, en tenant compte de la norme ISO/IEC 17065:2012 et des exigences supplémentaires établies par l'autorité de contrôle et/ou par le comité.

4 AGRÉMENT EN VERTU DE L'ARTICLE 43, PARAGRAPHE 1, DU RGPD

29. L'article 43, paragraphe 1, reconnaît qu'il existe plusieurs options pour l'agrément des organismes de certification. Conformément au RGPD, les autorités de contrôle et les États membres sont tenus de définir le processus d'agrément des organismes de certification. La présente section expose les possibilités d'agrément prévues à l'article 43.

4.1 Rôle des États membres

30. En vertu de l'article 43, paragraphe 1, les États membres sont tenus de *veiller à ce que* les organismes de certification soient agréés, mais peuvent chacun déterminer qui doit être chargé d'effectuer l'évaluation qui mène à l'agrément. Sur la base de l'article 43, paragraphe 1, trois options sont disponibles; l'agrément est effectué:

(1) uniquement par l'autorité de contrôle, sur la base de ses propres exigences;
(2) uniquement par l'organisme national d'accréditation, désigné conformément au règlement (CE) nº 765/2008 et sur la base de la norme ISO/IEC 17065:2012 et conformément aux exigences supplémentaires établies par l'autorité de contrôle compétente; ou
(3) à la fois par l'autorité de contrôle et par l'organisme national d'accréditation (et conformément à toutes les exigences énumérées au point 2 ci-dessus).

31. Il revient à chaque État membre de décider si ces opérations d'agrément sont effectuées par l'organisme national d'accréditation ou l'autorité de contrôle, ou par les deux entités à la

[12] Voir considérant 15 du règlement (CE) nº 765/2008.
[13] Voir article 2, point 10, du règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits.
[14] Voir définition du terme «accréditation» (l'équivalent du terme «agrément» dans le RGPD) conformément à la norme ISO/IEC 17011.

fois, mais les États membres doivent dans tous les cas garantir la mise à disposition de ressources adaptées[15].

4.2 Interaction avec le règlement (CE) nº 765/2008

32. Le comité observe qu'à l'article 2, point 11, du règlement (CE) nº 765/2008, un organisme national d'accréditation est défini comme «*l'unique* organisme dans un État membre chargé de l'accréditation, qui tire son autorité de cet État».

33. L'article 2, point 11, pourrait être considéré comme n'étant pas conforme à l'article 43, paragraphe 1, du RGPD, lequel permet à un autre organisme que l'organisme national d'accréditation de l'État membre d'effectuer des opérations d'accréditation/d'agrément. Le comité estime que la législation de l'Union a visé à déroger au principe général selon lequel l'agrément est exclusivement effectué par l'autorité nationale d'accréditation, en conférant le même pouvoir aux autorités de contrôle pour l'agrément des organismes de certification. L'article 43, paragraphe 1, est donc une lex specialis par rapport à l'article 2, point 11, du règlement (CE) nº 765/2008.

4.3 Le rôle de l'organisme national d'accréditation

34. L'article 43, paragraphe 1, point b), dispose que l'organisme national d'accréditation agrée les organismes de certification conformément à la norme ISO/IEC 17065:2012 et aux exigences supplémentaires établies par l'autorité de contrôle compétente.

35. Dans un souci de clarté, le comité note que la référence spécifique au «paragraphe 1, point b)» qui figure à l'article 43, paragraphe 3, signifie que «ces exigences» font référence aux «exigences supplémentaires» établies par l'autorité de contrôle compétente au titre de l'article 43, paragraphe 1, point b), et aux exigences fixées à l'article 43, paragraphe 2.

36. Au cours du processus d'agrément, les organismes nationaux d'accréditation appliquent les exigences supplémentaires que les autorités de contrôle doivent fournir.

37. Un organisme de certification doté d'un agrément sur la base de la norme ISO/IEC 17065:2012 pour des programmes de certification qui ne sont pas liés au RGPD et qui souhaite étendre le champ de son agrément afin d'y inclure une certification délivrée conformément au RGPD devra satisfaire aux exigences supplémentaires établies par l'autorité de contrôle si c'est l'organisme national d'accréditation qui procède à l'agrément. Si l'agrément pour la certification au titre du RGPD est uniquement assuré par l'autorité de contrôle compétente, un organisme de certification qui demande un agrément devra satisfaire aux exigences fixées par l'autorité de contrôle respective.

4.4 Le rôle de l'autorité de contrôle

38. Le comité note que l'article 57, paragraphe 1, point q), dispose que l'autorité de contrôle procède à l'agrément d'un organisme de certification en application de l'article 43, dans le cadre de ses missions d'autorité de contrôle au titre de l'article 57, et que l'article 58, paragraphe 3, point e), énonce que l'autorité de contrôle dispose du pouvoir d'autorisation et du pouvoir consultatif pour agréer des organismes de certification en application de l'article 43. Le libellé de l'article 43, paragraphe 1, offre une certaine flexibilité et la fonction d'accréditation de l'autorité de contrôle doit uniquement être considérée comme une mission dans les cas appropriés. Il est possible de recourir à la législation de l'État membre

[15] Voir article 4, paragraphe 9, du règlement (CE) nº 765/2008.

pour préciser ce point. Au cours du processus d'agrément effectué par un organisme national d'accréditation, l'organisme de certification est cependant tenu, en vertu de l'article 43, paragraphe 2, point a), de démontrer, à la satisfaction de l'autorité de contrôle compétente, son indépendance et son expertise à l'égard de l'objet du mécanisme de certification qu'il propose[16].

39. Si un État membre exige que les organismes de certification soient agréés par l'autorité de contrôle, cette même autorité doit établir des exigences en matière d'agrément comprenant, mais sans s'y limiter, les exigences exposées à l'article 43, paragraphe 2. Par comparaison avec les obligations relatives à l'agrément d'organismes de certification par des organismes nationaux d'accréditation, l'article 43 fournit moins d'instructions quant aux exigences en matière d'agrément lorsque l'autorité de contrôle procède elle-même à l'agrément. Dans le but de contribuer à une approche harmonisée de l'agrément, les critères en la matière utilisés par l'autorité de contrôle devraient être guidés par la norme ISO/IEC 17065:2012 et être complétés par les exigences supplémentaires établies par l'autorité de contrôle conformément à l'article 43, paragraphe 1, point b). Le comité fait remarquer que l'article 43, paragraphe 2, points a) à e), reflète et précise les exigences de la norme ISO IEC 17065:2012, ce qui contribuera à la cohérence.

40. Si un État membre exige que les organismes de certification soient agréés par les organismes nationaux d'accréditation, l'autorité de contrôle doit établir des exigences supplémentaires qui complètent les conventions d'agrément existantes envisagées dans le règlement (CE) nº 765/2008 (où les articles 3 à 14 ont trait à l'organisation et au fonctionnement de l'agrément des organismes d'évaluation de la conformité) et les règles techniques qui décrivent les méthodes et procédures suivies par les organismes de certification. S'agissant de ces éléments, le règlement (CE) nº 765/2008 fournit des orientations supplémentaires: l'agrément (l'«accréditation») est défini à l'article 2, point 10, qui fait référence à des «normes harmonisées» et à «toute autre exigence supplémentaire, notamment celles fixées dans les programmes sectoriels pertinents». Il s'ensuit que les exigences supplémentaires établies par l'autorité de contrôle devraient inclure des exigences spécifiques et viser avant tout à faciliter l'évaluation, entre autres, de l'indépendance des organismes de certification et de leur niveau d'expertise en matière de protection des données, par exemple leur capacité à évaluer et à certifier des opérations de traitement de données à caractère personnel effectuées par des responsables du traitement et des sous-traitants au sens de l'article 42, paragraphe 1. Les compétences requises pour des programmes sectoriels et celles liées à la protection des libertés et des droits fondamentaux des personnes physiques, en particulier leur droit à la protection des données personnelles, en font partie[17]. L'annexe des présentes lignes directrices peut donner des indications aux autorités de contrôle compétentes lorsqu'elles établissent les «exigences supplémentaires» conformément à l'article 43, paragraphe 1, point b), et à l'article 43, paragraphe 3.

41. L'article 43, paragraphe 6, dispose que «[l]es exigences visées au paragraphe 3 du présent article et les critères visés à l'article 42, paragraphe 5, sont publiés par les autorités de contrôle sous une forme aisément accessible». L'ensemble des critères et des exigences

[16] Les exigences en matière d'indépendance et d'expertise doivent être précisées dans les exigences supplémentaires établies par l'autorité de contrôle conformément à l'article 43, paragraphe 1, point b). Voir également l'annexe 1 des lignes directrices.
[17] Article 1er, paragraphe 2, du RGPD.

approuvés par une autorité de contrôle doit dès lors être publié afin de garantir la transparence. En ce qui concerne la qualité et la confiance à l'égard des organismes de certification, il serait souhaitable que le public puisse facilement accéder à toutes les exigences en matière d'agrément.

4.5 Autorité de contrôle agissant comme organisme de certification

42. L'article 42, paragraphe 5, dispose qu'une autorité de contrôle peut délivrer des certifications, mais le RGPD n'exige pas qu'elle soit agréée comme respectant les exigences énoncées dans le règlement (CE) nº 765/2008. Le comité fait remarquer que l'article 43, paragraphe 1, point a), et, spécifiquement, l'article 58, paragraphe 2, point h), et l'article 58, paragraphe 3, points a) et e) à f), confèrent aux autorités de contrôle le pouvoir de procéder à l'agrément et à la certification et dans le même temps de prodiguer des conseils et, le cas échéant, de retirer des certifications ou d'ordonner aux organismes de certification de ne pas délivrer de certifications.

43. Dans certaines situations, la séparation des rôles et des devoirs liés à l'agrément et à la certification peut être appropriée ou nécessaire, par exemple lorsqu'une autorité de contrôle et d'autres organismes de certification coexistent au sein d'un État membre et délivrent le même éventail de certifications. Les autorités de contrôle devraient donc prendre des mesures organisationnelles suffisantes afin de séparer les missions relevant du RGPD de manière à fixer et à faciliter les mécanismes de certification tout en prenant les précautions nécessaires pour éviter l'apparition de conflits d'intérêts qui pourraient découler de ces missions. En outre, les États membres et les autorités de contrôle devraient garder à l'esprit le niveau européen harmonisé lorsqu'ils formulent des lois et des procédures nationales relatives à l'agrément et à la certification conformément au RGPD.

4.6 Exigences en matière d'agrément

44. L'annexe des présentes lignes directrices contient des orientations concernant la manière d'établir des exigences supplémentaires en matière d'agrément. Les dispositions pertinentes du RGPD y sont recensées et l'annexe contient des suggestions d'exigences que les autorités de contrôle et les organismes nationaux d'accréditation devraient envisager afin de garantir la conformité au RGPD.

45. Comme indiqué ci-dessus, lorsque les organismes de certification sont agréés par l'organisme national d'accréditation conformément au règlement (CE) nº 765/2008, la norme d'agrément pertinente est la norme ISO/IEC 17065:2012, complétée par les exigences supplémentaires établies par l'autorité de contrôle. L'article 43, paragraphe 2, reflète les dispositions générales de la norme ISO/IEC 17065:2012 à la lumière de la protection des droits fondamentaux au titre du RGPD. L'article 43, paragraphe 2, et la norme ISO/IEC 17065:2012 constituent la base du cadre établi dans l'annexe pour la définition d'exigences et de critères supplémentaires relatifs à l'évaluation de l'expertise des organismes de certification en matière de protection des données et à leur capacité à respecter les droits et libertés des personnes physiques en ce qui concerne le traitement de données à caractère personnel, tels que consacrés par le RGPD. Le comité observe qu'une attention particulière est accordée à la nécessité de veiller à ce que les organismes de certification possèdent un niveau approprié d'expertise en matière de protection des données conformément à l'article 43, paragraphe 1.

46. Les exigences supplémentaires en matière d'agrément établies par l'autorité de contrôle s'appliquent à tous les organismes de certification qui demandent un agrément. L'organisme

d'accréditation évalue si ledit organisme de certification dispose des compétences nécessaires pour effectuer l'opération de certification conformément aux exigences supplémentaires et à l'objet de la certification. Il est fait référence aux secteurs ou domaines de certification spécifiques pour lesquels l'organisme de certification est agréé.

47. Le comité observe aussi qu'une expertise spéciale dans le domaine de la protection des données est également nécessaire, en plus des exigences relevant de la norme ISO/IEC 17065:2012, si d'autres organismes – externes – tels que des laboratoires ou des auditeurs, effectuent une partie ou certains éléments des opérations de certification pour le compte d'un organisme de certification agréé. Dans de tels cas, l'agrément de ces organismes externes au titre du RGPD est impossible. Afin de garantir l'aptitude de ces organismes à mener ces opérations au nom des organismes de certification agréés, il est néanmoins nécessaire que l'organisme de certification agréé veille à ce que l'expertise en matière de protection des données que l'organisme agréé est tenu de posséder existe et soit démontrée également chez l'organisme externe, en ce qui concerne l'opération concernée.

48. Le cadre permettant de définir des exigences supplémentaires en matière d'agrément présenté dans l'annexe des présentes lignes directrices ne constitue pas un manuel de procédure pour le processus d'agrément effectué par l'organisme national d'accréditation ou l'autorité de contrôle. Il fournit des orientations quant à la structure et à la méthode et dote dès lors les autorités de contrôle d'outils pour la détermination d'exigences supplémentaires en matière d'agrément.

ANNEXE 1

L'annexe 1 fournit des orientations pour la spécification d'exigences «supplémentaires» en matière d'agrément au regard de la norme ISO 17065:2012 et conformément à l'article 43, paragraphe 1, point b), et à l'article 43, paragraphe 3, du RGPD.

La présente annexe expose des suggestions d'exigences destinées à être formulées par l'autorité de contrôle de la protection des données et à s'appliquer lors de l'agrément d'un organisme de certification par un organisme national d'accréditation ou par l'autorité de contrôle compétente[18]. Ces exigences supplémentaires doivent être communiquées au comité européen de la protection des données pour approbation, conformément à l'article 64, paragraphe 1, point c).

Il convient de lire la présente annexe conjointement avec la norme ISO/IEC 17065:2012. La numérotation des sections utilisée dans le présent document correspond à celle utilisée dans la norme ISO/IEC 17065:2012. Lorsque des autorités de contrôle délivrent un agrément en vertu de l'article 43, paragraphe 1, point a), il serait souhaitable que la présente approche soit suivie dans la mesure du possible. L'harmonisation de l'agrément à l'échelle de l'Union serait ainsi favorisée.

Nonobstant les orientations ci-après ou l'absence d'orientation sur tout point de la norme ISO/IEC 17065:2012, l'autorité de contrôle compétente peut formuler d'autres exigences supplémentaires quant à ces points si celles-ci respectent le droit national.

0 INTRODUCTION

[Cette section concerne, le cas échéant, toutes les conditions de coopération dont l'organisme national d'accréditation et l'autorité de contrôle de la protection des données sont convenus, par exemple, qui devrait être responsable de la réception des demandes ou comment organiser la reconnaissance de critères approuvés en tant que parties intégrantes du processus d'agrément.]

1 DOMAINE D'APPLICATION[19]

Le domaine d'application de la norme ISO/IEC 17065:2012 s'applique conformément au RGPD. Les lignes directrices relatives à l'agrément et à la certification offrent de plus amples informations. L'organisme national d'accréditation et l'autorité de contrôle compétente devraient tenir compte de la portée du mécanisme de certification (par exemple, certification des opérations de traitement de services en nuage) au cours de leur évaluation dans le cadre du processus d'agrément, notamment en ce qui concerne les critères, l'expertise et la méthode d'évaluation. Le vaste domaine d'application de la norme ISO/IEC 17065:2012, qui comprend des produits, des procédés et des services, ne doit pas réduire ou outrepasser les exigences du RGPD; par exemple, un mécanisme de gouvernance ne saurait être le seul élément d'un mécanisme de certification puisque la certification doit inclure le traitement de données personnelles, c'est-à-dire les opérations de traitement. En vertu de l'article 42, paragraphe 1, la certification prévue par le RGPD s'applique uniquement aux opérations de traitement effectuées par les responsables du traitement et les sous-traitants.

[18] Pour de plus amples informations sur le processus d'approbation des critères de certification, se reporter à la section 4 des lignes directrices relatives à la certification.
[19] La numérotation fait référence à la norme ISO/IEC 17065:2012.

2 RÉFÉRENCES NORMATIVES

Le RGPD prime sur la norme ISO/IEC 17065:2012. S'il est fait référence à d'autres normes ISO dans les exigences supplémentaires ou dans le cadre d'un mécanisme de certification, celles-ci sont interprétées conformément aux exigences définies dans le RGPD.

3 TERMES ET DÉFINITIONS

Dans le contexte de la présente annexe, les termes et définitions des lignes directrices relatives à l'agrément (WP 261) et à la certification (EDPB 1/2018) s'appliquent et priment sur les définitions de la norme ISO.

4 EXIGENCES GÉNÉRALES RELATIVES À L'AGRÉMENT

4.1 Domaine juridique et contractuel

4.1.1 Responsabilité juridique

Un organisme de certification doit être en mesure de prouver (à tout moment) à l'organisme national d'accréditation ou à l'autorité de contrôle compétente qu'il est doté de procédures à jour démontrant la conformité aux responsabilités juridiques établies dans les conditions d'agrément, y compris aux exigences supplémentaires dans le cadre de l'application du règlement (UE) 2016/679. Il convient de noter que puisque l'organisme de certification est lui-même responsable du traitement/sous-traitant, il doit être à même de prouver que ses procédures et mesures sont conformes au règlement (UE) 2016/679 en ce qui concerne spécifiquement le contrôle et le traitement des données personnelles de l'organisation cliente dans le cadre du processus de certification.

L'autorité de contrôle compétente peut décider d'ajouter des exigences et des procédures supplémentaires pour vérifier la conformité des organismes de certification au RGPD avant l'agrément.

4.1.2 Contrat de certification

Les exigences minimales pour un contrat de certification sont complétées par les éléments suivants.

L'organisme de certification doit prouver, outre les exigences de la norme ISO/IEC 17065:2012, que ses contrats de certification:

1. exigent du demandeur qu'il respecte en permanence à la fois les exigences générales en matière de certification au sens du point 4.1.2.2 a) de la norme ISO/IEC 17065:2012 et les critères approuvés par l'autorité de contrôle compétente ou par le comité conformément à l'article 43, paragraphe 2, point b), et à l'article 42, paragraphe 5;
2. exigent du demandeur qu'il autorise la pleine transparence vis-à-vis de l'autorité de contrôle compétente s'agissant de la procédure de certification, y compris en ce qui concerne des questions contractuellement confidentielles relatives au respect de la protection des données conformément à l'article 42, paragraphe 7, et à l'article 58, paragraphe 1, point c);
3. ne diminuent pas la responsabilité du demandeur pour ce qui est du respect du règlement (CE) 2016/697 et sont sans préjudice des missions et des pouvoirs des autorités de contrôle compétentes en vertu de l'article 42, paragraphe 5;

4. exigent que le demandeur fournisse à l'organisme de certification toutes les informations et l'accès à ses activités de traitement dans la mesure nécessaire à la conduite de la procédure de certification en vertu de l'article 42, paragraphe 6;
5. exigent que le demandeur respecte les délais et les procédures applicables. Le contrat de certification doit mentionner que les délais et les procédures découlant, par exemple, du programme de certification ou d'autres réglementations doivent être respectés;
6. en ce qui concerne le point 4.1.2.2 c) 1) de la norme ISO/IEC 17065:2012, établissent les règles de validité, de renouvellement et de retrait conformément à l'article 42, paragraphe 7, et à l'article 43, paragraphe 4, y compris des règles qui prévoient des intervalles appropriés en matière de réévaluation ou d'examen (régularité) au sens de l'article 42, paragraphe 7;
7. autorisent l'organisme de certification à divulguer toutes les informations nécessaires à la délivrance de la certification conformément à l'article 42, paragraphe 8, et à l'article 43, paragraphe 5;
8. incluent des règles relatives aux précautions nécessaires pour l'instruction des plaintes au sens des points 4.1.2.2 c) 2) et 4.1.2.2 j), ainsi que des déclarations explicites sur la structure et la procédure de la gestion des plaintes conformément à l'article 43, paragraphe 2, point d);
9. outre les exigences minimales du point 4.1.2.2 de la norme ISO/IEC 17065:2012, si les conséquences du retrait ou de la suspension de l'agrément délivré à l'organisme de certification ont des répercussions sur le client, il convient également de traiter des conséquences pour le client;
10. exigent que le demandeur tienne l'organisme de certification informé d'éventuels changements significatifs concernant sa situation réelle, sa situation juridique ou ses produits, procédés et services concernés par la certification.

4.1.3 Utilisation de labels et de marques en matière de protection des données

Les certificats, les labels et les marques doivent uniquement être utilisés conformément aux articles 42 et 43 et aux lignes directrices relatives à l'agrément et à la certification.

4.2 Gestion de l'impartialité

L'organisme d'accréditation doit s'assurer, outre l'exigence visée au point 4.2. de la norme ISO/IEC 17065:2012, que

1. l'organisme de certification respecte les exigences supplémentaires de l'autorité de contrôle compétente [en vertu de l'article 43, paragraphe 1, point b)]
    - **a.** il fournit des preuves distinctes de son indépendance conformément à l'article 43, paragraphe 2, point a), ce qui s'applique en particulier aux preuves concernant le financement de l'organisme de certification dans la mesure où l'assurance d'impartialité est concernée;
    - **b.** ses missions et ses obligations n'entraînent pas de conflit d'intérêts au sens de l'article 43, paragraphe 2, point e);
2. l'organisme de certification n'entretient pas de lien significatif avec le client qu'il évalue.

4.3 Responsabilité et financement

L'organisme d'accréditation, outre l'exigence visée au point 4.3.1 de la norme ISO/IEC 17065:2012, doit s'assurer régulièrement que l'organisme de certification a pris les mesures nécessaires (par

exemple, assurances ou provisions) pour couvrir ses engagements dans les régions géographiques où il opère.

4.4 Conditions non discriminatoires

L'autorité de contrôle peut formuler des exigences supplémentaires si celles-ci sont conformes au droit national.

4.5 Confidentialité

L'autorité de contrôle peut formuler des exigences supplémentaires si celles-ci sont conformes au droit national.

4.6 Informations accessibles au public

L'organisme d'accréditation, outre l'exigence visée au point 4.6 de la norme ISO/IEC 17065:2012, exige au minimum de l'organisme de certification

1. que toutes les versions (actuelles et précédentes) des critères approuvés utilisés au sens de l'article 42, paragraphe 5, soient publiées et facilement accessibles au public, ainsi que toutes les procédures de certification, en mentionnant de manière générale les périodes de validité respectives;
2. que les informations relatives aux procédures de traitement des réclamations et aux recours soient rendues publiques conformément à l'article 43, paragraphe 2, point d).

5 EXIGENCES STRUCTURELLES, ARTICLE 43, PARAGRAPHE 4 [ÉVALUATION «APPROPRIÉE»]

5.1 Organisation et direction

L'autorité de contrôle peut formuler des exigences supplémentaires.

5.2 Dispositifs de préservation de l'impartialité

L'autorité de contrôle peut formuler des exigences supplémentaires.

6 EXIGENCES RELATIVES AUX RESSOURCES

6.1 Personnel de l'organisme de certification

L'organisme d'accréditation s'assure, outre l'exigence visée à la section 6 de la norme ISO/IEC 17065:2012, que les membres du personnel de chaque organisme de certification:

1. ont prouvé qu'ils disposent d'une expertise appropriée et actuelle (connaissances et expérience) concernant la protection des données conformément à l'article 43, paragraphe 1;
2. sont indépendants et disposent d'une expertise actuelle au regard de l'objet de la certification conformément à l'article 43, paragraphe 2, point a), et n'ont pas de conflit d'intérêts conformément à l'article 43, paragraphe 2, point e);
3. s'engagent à respecter les critères visés à l'article 42, paragraphe 5, conformément à l'article 43, paragraphe 2, point b);
4. possèdent les connaissances et l'expérience pertinentes et appropriées concernant l'application de la législation en matière de protection des données;

5. possèdent, le cas échéant, les connaissances et l'expérience pertinentes et appropriées concernant les mesures techniques et organisationnelles de protection des données;
6. sont en mesure de prouver leur expérience dans les domaines spécifiquement mentionnés dans les exigences supplémentaires aux points 6.1.1, 6.1.4, et 6.1.5.

En ce qui concerne les membres du personnel ayant une expertise technique:

- ils ont obtenu une certification correspondant au moins au niveau 6 du cadre européen des certifications[20] dans un domaine d'expertise technique pertinent ou un titre protégé reconnu (par exemple, ingénieur diplômé) dans la profession réglementée concernée ou possèdent une solide expérience professionnelle;
- *les membres du personnel responsables des décisions en matière de certification* doivent posséder une solide expérience professionnelle dans la définition et la mise en œuvre de mesures de protection des données;
- *les membres du personnel responsables des évaluations* doivent posséder une expérience professionnelle dans la protection technique des données ainsi que des connaissances et une expérience concernant des procédures similaires (par exemple certifications/audits), et être enregistrés selon le cas.

Les membres du personnel doivent démontrer qu'ils entretiennent leurs connaissances spécifiques au domaine pour ce qui est des compétences techniques et d'audit grâce à un perfectionnement professionnel continu.

En ce qui concerne les membres du personnel ayant une expertise juridique:

- des études juridiques dans une université de l'Union européenne ou une université agréée par l'État pendant au moins huit semestres ayant notamment débouché sur un diplôme universitaire de Master (LL.M.) ou équivalent, ou une solide expérience professionnelle, sont exigées;
- *les membres du personnel responsables des décisions en matière de certification* doivent démontrer qu'ils possèdent une solide expérience professionnelle de la législation relative à la protection des données et sont enregistrés selon les exigences de l'État membre;
- *les membres du personnel responsables des évaluations* doivent démontrer qu'ils ont au moins deux ans d'expérience professionnelle de la législation relative à la protection des données ainsi que des connaissances et une expérience de procédures similaires (par exemple certifications/audits) et sont enregistrés lorsque l'État membre l'exige.
    - Les membres du personnel doivent démontrer qu'ils entretiennent leurs connaissances spécifiques au domaine pour ce qui est des compétences techniques et d'audit grâce à un perfectionnement professionnel continu.

6.2 Ressources pour l'évaluation

L'autorité de contrôle peut formuler des exigences supplémentaires si celles-ci sont conformes au droit national.

[20] Voir l'outil de comparaison du cadre des certifications à l'adresse suivante: https://ec.europa.eu/ploteus/fr/compare?

7 EXIGENCES RELATIVES AUX PROCESSUS, ARTICLE 43, PARAGRAPHE 2, POINTS C) ET D)

7.1 Généralités

L'organisme d'accréditation doit, outre l'exigence visée au point 7.1 de la norme ISO/IEC 17065:2012:

1. s'assurer que les organismes de certification respectent les exigences supplémentaires émises par l'autorité de contrôle compétente [en vertu de l'article 43, paragraphe 1, point b)] lorsqu'ils présentent leur demande afin que les missions et obligations n'entraînent pas de conflits d'intérêts conformément à l'article 43, paragraphe 2, point b);
2. informer les autorités de contrôle compétentes concernées avant qu'un organisme de certification commence à exploiter un label européen de protection des données approuvé dans un nouvel État membre depuis un bureau satellite.

7.2 Demande

Outre le point 7.2 de la norme ISO/IEC 17065:2012, il convient d'exiger que:

1. l'objet de la certification (cible d'évaluation) fasse l'objet d'une description détaillée dans la demande, ce qui inclut également les interfaces et les transferts vers d'autres systèmes et organisations, protocoles et autres assurances;
2. la demande précise le recours ou non à des sous-traitants et, lorsque le demandeur est un sous-traitant, que ses responsabilités et missions soient décrites et que la demande contienne le ou les contrat(s) pertinent(s) entre le responsable du traitement et le sous-traitant.

7.3 Examen de la demande

Outre le point 7.3 de la norme ISO/IEC 17065:2012, il convient d'exiger que:

1. l'accord de certification prévoie des méthodes d'évaluation contraignantes au regard de la cible d'évaluation;
2. l'évaluation visée au point 7.3 e), destinée à déterminer si l'expertise est suffisante, tienne compte de l'expertise tant technique que juridique en matière de protection des données, dans une mesure appropriée.

7.4 Évaluation

Outre le point 7.4 de la norme ISO/IEC 17065:2012, les mécanismes de certification doivent décrire suffisamment de méthodes d'évaluation aux fins de déterminer si les opérations de traitement sont conformes aux critères d'évaluation, notamment, selon qu'il convient:

1. une méthode d'évaluation de la nécessité et de la proportionnalité des opérations de traitement en relation avec leur objectif et les personnes concernées;
2. une méthode d'évaluation de la couverture, de la composition et de l'estimation de l'ensemble des risques envisagés par le responsable du traitement et par le sous-traitant au regard des conséquences juridiques conformément aux articles 30, 32, 35 et 36 du RGPD, et au regard de la définition des mesures organisationnelles et techniques conformément aux articles 24, 25 et 32 du RGPD, dans la mesure où les articles susmentionnés s'appliquent à l'objet de la certification;
3. une méthode d'évaluation des voies de recours, y compris des garanties, des mesures de sauvegarde et des procédures pour assurer la protection des données à caractère

personnel dans le cadre du traitement qu'il convient d'attribuer à l'objet de la certification et démontrer que les exigences juridiques établies dans les critères sont respectées; et

4. une documentation des méthodes et des conclusions.

L'organisme de certification devrait être tenu de veiller à ce que ces méthodes d'évaluation soient standardisées et s'appliquent de façon générale, ce qui signifie que des méthodes d'évaluation comparables sont utilisées pour des cibles d'évaluation comparables. L'organisme de certification doit justifier tout écart par rapport à cette procédure.

Outre le point 7.4.2 de la norme ISO/IEC 17065:2012, des experts externes reconnus par l'organisme de certification devraient être autorisés à effectuer l'évaluation.

Outre le point 7.4.5 de la norme ISO/IEC 17065:2012, il convient qu'une certification en matière de protection des données effectuée conformément aux articles 42 et 43 du RGPD et qui couvre déjà une partie de l'objet de la certification puisse être incluse dans une certification existante. Elle ne saurait toutefois suffire à remplacer totalement des évaluations (partielles). L'organisme de certification est obligé de vérifier la conformité aux critères. Pour qu'elle soit reconnue, il est dans tous les cas nécessaire qu'un rapport d'évaluation complet ou des informations permettant d'évaluer la précédente activité de certification et ses résultats soient disponibles. Une déclaration de certification ou des certificats de certification similaires ne devraient pas être jugés suffisant pour remplacer un rapport.

Outre le point 7.4.6 de la norme ISO/IEC 17065:2012, dans son mécanisme de certification, l'organisme de certification doit exposer en détail comment les informations requises au point 7.4.6 renseignent le client (celui qui demande une certification) sur les non-conformités au mécanisme de certification. Dans ce contexte, il convient de définir au moins la nature et le calendrier de telles informations.

Outre le point 7.4.9 de la norme ISO/IEC 17065:2012, il devrait être exigé que la totalité de la documentation soit pleinement accessible à l'autorité de contrôle de la protection des données à sa demande.

7.5 Examen

Outre le point 7.5 de la norme ISO/IEC 17065:2012, des procédures de délivrance, d'examen régulier et de retrait des certifications respectives conformément à l'article 43, paragraphes 2 et 3 sont nécessaires.

7.6 Décision de certification

Outre le point 7.6.1 de la norme ISO/IEC 17065:2012, dans ses procédures, l'organisme de certification devrait être tenu d'exposer en détail la façon dont son indépendance et sa responsabilité sont garanties au regard de décisions de certification individuelles.

7.7 Documents de certification

Outre le point 7.7.1 e) de la norme ISO/IEC 17065:2012 et conformément à l'article 42, paragraphe 7, du RGPD, il convient que la période de validité des certifications ne dépasse pas trois ans.

Outre le point 7.7.1 e) de la norme ISO/IEC 17065:2012, il convient que la période de surveillance prévue au sens du point 7.9 soit également documentée.

Outre le point 7.7.1 f) de la norme ISO/IEC 17065:2012, l'organisme de certification devrait être tenu de nommer l'objet de la certification dans les documents de certification (mentionner le statut de la version ou d'autres caractéristiques similaires, le cas échéant).

7.8 Répertoire de produits certifiés

Outre le point 7.8 de la norme ISO/IEC 17065:2012, l'organisme de certification devrait être tenu de mettre à disposition les informations relatives aux produits, aux processus et aux services certifiés, en interne et publiquement. L'organisme de certification publie une synthèse du rapport d'évaluation de manière à favoriser la transparence concernant l'objet de la certification et les méthodes d'évaluation. Cette synthèse explique par exemple:

(a) le domaine d'application de la certification et fournit une description pertinente de l'objet de la certification (cible d'évaluation),

(b) les critères de certification respectifs (y compris la version ou le statut fonctionnel),

(c) les méthodes d'évaluation et les tests effectués, et

(d) le(s) résultat(s).

Outre le point 7.8 de la norme ISO/IEC 17065:2012 et conformément à l'article 43, paragraphe 5, du RGPD, l'organisme de certification communique aux autorités de contrôle compétentes les raisons de la délivrance ou du retrait de la certification demandée.

7.9 Surveillance

Outre les points 7.9.1, 7.9.2 et 7.9.3 de la norme ISO/IEC 17065:2012 et conformément à l'article 43, paragraphe 2, point c), du RGPD, des mesures de surveillance régulière devraient être obligatoires afin de maintenir la certification durant la période de contrôle.

7.10 Changements ayant des conséquences sur la certification

Outre les points 7.10.1, et 7.10.2 de la norme EN ISO/IEC 17065:2012, l'organisme de certification tient notamment compte des changements suivants ayant des conséquences sur la certification: les modifications apportées à la législation applicable à la protection des données, l'adoption d'actes délégués par la Commission européenne conformément à l'article 43, paragraphes 8 et 9, les décisions du comité européen de la protection des données et les décisions juridictionnelles liées à la protection des données. Les procédures liées au changement dont il faudrait convenir pourraient par exemple inclure: des périodes de transition, des processus d'approbation par l'autorité de contrôle compétente, la réévaluation de l'objet de la certification en question et des mesures appropriées pour révoquer la certification si l'opération de traitement certifiée n'est plus conforme aux critères mis à jour.

7.11 Résiliation, réduction, suspension ou retrait de la certification

Outre le point 7.11.1 de la norme ISO/IEC 17065:2012, l'organisme de certification devrait être tenu d'informer immédiatement par écrit l'autorité de contrôle compétente et l'organisme national d'accréditation, le cas échéant, à propos des mesures adoptées et de la prorogation, des restrictions, de la suspension et du retrait d'une certification.

Conformément à l'article 58, paragraphe 2, point h), l'organisme de certification est tenu d'accepter les décisions et les ordres émanant de l'autorité de contrôle compétente aux fins de retirer une certification à un client (demandeur) ou de ne pas la lui délivrer si les exigences applicables à la certification ne sont pas ou plus satisfaites.

7.12 Enregistrements

L'organisme de certification devrait être tenu de maintenir l'ensemble de la documentation sous une forme complète, compréhensible, à jour et susceptible d'audit.

7.13 Réclamations et recours, article 43, paragraphe 2, point d)

Outre le point 7.13.1 de la norme ISO/IEC 17065:2012, l'organisme de certification devrait être tenu de définir:

(a) qui peut introduire des réclamations ou émettre des objections,

(b) qui les traite au nom de l'organisme de certification,

(c) quelles vérifications ont lieu dans ce contexte, et

(d) les possibilités de consulter les parties intéressées.

Outre le point 7.13.2 de la norme ISO/IEC 17065:2012, l'organisme de certification devrait être tenu de définir:

(a) comment et à qui donner une telle confirmation,

(b) les délais à cet effet, et

(c) quels processus doivent ensuite être amorcés.

Outre le point 7.13.1 de la norme ISO/IEC 17065:2012, l'organisme de certification doit définir la manière de garantir la séparation entre les activités de certification et le traitement des recours et des réclamations.

8 EXIGENCES RELATIVES AU SYSTÈME DE GESTION

En vertu de la section 8 de la norme ISO/IEC 17065:2012, une des exigences générales relatives au système de gestion est que la mise en œuvre, par l'organisme de certification agréé, de toutes les exigences prévues dans les chapitres précédents dans le cadre du domaine d'application du mécanisme de certification doit être documentée, évaluée, contrôlée et suivie de manière indépendante.

Le principe de base de la gestion est de définir un système en fonction duquel des objectifs sont fixés de manière efficace et efficiente, plus spécifiquement: la mise en œuvre des services de certification – au moyen de spécifications adéquates. Cela nécessite que l'organisme de certification applique les exigences en matière d'agrément de manière transparente et vérifiable et qu'il s'y conforme en toutes circonstances.

À cet effet, le système de gestion doit spécifier une méthodologie visant à satisfaire à ces exigences et à les contrôler, conformément aux réglementations relatives à la protection des données, et à constamment les vérifier avec l'organisme agréé lui-même.

Ces principes de gestion et leur application documentée doivent être transparents et communiqués par l'organisme de certification agréé conformément à la procédure d'agrément en vertu de l'article 58 et, par la suite, à la demande de l'autorité de contrôle de la protection des données, à tout moment au cours d'une enquête sous la forme d'un examen de la protection des données conformément à l'article 58, paragraphe 1, point b), ou d'un examen des certifications délivrées en application de l'article 42, paragraphe 7, conformément à l'article 58, paragraphe 1, point c).

L'organisme de certification agréé doit notamment rendre public, de façon permanente et continue, quelles sont les certifications qui ont été effectuées et sur quelle base (ou selon quels mécanismes

ou programmes de certification) et quelle est leur durée de validité dans quel cadre et dans quelles conditions (considérant 100).

8.1 Exigences générales relatives au système de gestion

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

8.2 Documents relatifs au système de gestion

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

8.3 Contrôle des documents

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

8.4 Contrôle des registres

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

8.5 Examen de gestion

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

8.6 Audits internes

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

8.7 Actions correctives

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

8.8 Actions préventives

L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

9 AUTRES EXIGENCES SUPPLÉMENTAIRES[21]

9.1 Mise à jour des méthodes d'évaluation

L'organisme de certification établit des procédures destinées à orienter la mise à jour des méthodes d'évaluation applicables dans le cadre de l'évaluation au titre du point 7.4. Cette mise à jour doit s'inscrire dans le contexte de changements dans le cadre juridique, le ou les risques pertinents, l'état de la technique et les coûts de mise en œuvre de mesures techniques et organisationnelles.

9.2 Maintenir le niveau d'expertise

Les organismes de certification établissent des procédures visant à garantir la formation de leurs employés afin d'assurer la mise à jour de leurs compétences, en tenant compte des évolutions énumérées au point 9.1.

[21] L'autorité de contrôle compétente peut spécifier et ajouter des exigences supplémentaires si celles-ci sont conformes au droit national.

9.3 Responsabilités et compétences

9.3.1 Communication entre l'organisme de certification et ses clients

Des procédures doivent être en place pour la mise en œuvre de procédures et de structures de communication adéquates entre l'organisme de certification et son client. Elles comprennent:

1. la conservation de la documentation sur les missions et les responsabilités de l'organisme de certification agréé pour
    a. répondre à des demandes d'informations ou
    b. permettre d'établir un contact en cas de réclamation à propos d'une certification;
2. la gestion d'un processus de demande à des fins
    a. d'information sur le statut d'une demande,
    b. d'évaluation par l'autorité de contrôle compétente concernant
        i. le retour d'informations,
        ii. les décisions prises par l'autorité de contrôle compétente.

9.3.2 Documentation relative aux activités d'évaluation

L'autorité de contrôle peut formuler des exigences supplémentaires.

9.3.3 Gestion du traitement des réclamations

Le traitement d'une réclamation doit faire partie intégrante du système de gestion, lequel met notamment en œuvre les exigences des points 4.1.2.2 c), 4.1.2.2 j), 4.6. d) et 7.13 de la norme ISO/IEC 17065:2012.

Les réclamations et les objections pertinentes devraient être communiquées à l'autorité de contrôle compétente.

9.3.4 Gestion du retrait

Les procédures en cas de suspension ou de retrait de l'agrément doivent être intégrées au système de gestion de l'organisme de certification, y compris les notifications envoyées aux clients.