Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement

Version 3.0

4 juin 2019

Adopté

Historique des versions

Version 3.0	4 juin 2019	Inclusion de l'annexe 2 (version 2.0 de cette annexe adoptée le 4 juin 2019 après consultation publique)
Version 2.1	9 avril 2019	Adoption d'un rectificatif des lignes directrices (paragraphe 45)
Version 2.0	23 janvier 2019	Adoption des lignes directrices après consultation publique, à la même date à laquelle l'annexe 2 (version 1.0) a été adoptée avant d'être soumise à consultation publique
Version 1.0	25 mai 2018	Adoption des lignes directrices à soumettre à consultation

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 (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen, et en particulier son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018,

vu les articles 12 et 22 de son règlement intérieur du 25 mai 2018,

et ayant pris en considération les résultats de la consultation publique sur les lignes directrices, qui s'est déroulée du 30 mai 2018 au 12 juillet 2018, et sur l'annexe 2, qui s'est déroulée du 15 février 2019 au 29 mars 2019, conformément à l'article 70, paragraphe 4, du RGPD,

A ADOPTE LES LIGNES DIRECTRICES SUIVANTES:

1 INTRODUCTION

1. Le règlement général sur la protection des données [règlement (UE) 2016/279, le «RGPD», ou le «règlement»], constitue un cadre réglementaire modernisé en matière de protection des données en Europe, axé sur la notion de responsabilité et le respect des droits fondamentaux. Une série de mesures destinées à faciliter le respect des dispositions du RGPD est au cœur de ce nouveau cadre. Il s'agit notamment d'exigences obligatoires dans des circonstances particulières (y compris la nomination de délégués à la protection des données et la réalisation d'analyses d'impact relatives à la protection des données) et de mesures volontaires telles que des codes de conduite et des mécanismes de certification.

2. Avant l'adoption du RGPD, le groupe de travail «Article 29» avait établi que la certification pouvait jouer un rôle important dans le cadre de responsabilisation relatif à la protection des données1. Pour que la certification apporte la preuve, fiable, de la conformité en matière de protection des données, il importe de mettre en place des règles claires énonçant les exigences en matière de certification2. L'article 42 du RGPD fournit la base juridique pour l'élaboration de telles règles.

3. L'article 42, paragraphe 1, du RGPD dispose:

   «Les États membres, les autorités de contrôle, le comité [européen de la protection des données] et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées

[1] Avis 3/2010 du groupe de travail «Article 29» sur le principe de responsabilité, WP173, 13 juillet 2010, paragraphes 69 à 71.
[2] Avis 3/2010 du groupe de travail «Article 29» sur le principe de responsabilité (WP173), paragraphe 69.

par des responsables du traitement et des sous-traitants respectent le présent règlement. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération».

4. Les mécanismes de certification3 peuvent améliorer la transparence pour les personnes concernées, mais également dans les relations entre entreprises, par exemple entre les responsables du traitement et les sous-traitants. Le considérant 100 du RGPD indique que la mise en place de mécanismes de certification peut favoriser la transparence et le respect du règlement et permettre aux personnes concernées d'évaluer le niveau de protection des données offert par les produits et services en question4.

5. Le RGPD n'introduit pas de droit ou d'obligation de certification pour les responsables du traitement et les sous-traitants: conformément à l'article 42, paragraphe 3, la certification est un processus volontaire qui contribue à démontrer le respect du RGPD. Les États membres et les autorités de contrôle sont invités à encourager la mise en place de mécanismes de certification et détermineront la participation des parties prenantes au processus de certification et à son cycle de vie.

6. En outre, le respect des mécanismes de certification approuvés est un facteur que les autorités de contrôle doivent considérer comme une circonstance aggravante ou atténuante pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende [article 83, paragraphe 2, point j)]5.

1.1 Champ d'application des lignes directrices

7. Le champ d'application des présentes lignes directrices est limité; elles ne constituent pas un manuel de procédure pour la certification conformément au RGPD. Le but premier des présentes lignes directrices est de définir des exigences et des critères généraux pouvant s'appliquer à tous les types de mécanismes de certification mis en place en vertu des articles 42 et 43 du RGPD. À cette fin, les présentes lignes directrices:

    - se penchent sur les raisons pour lesquelles la certification constitue un outil de responsabilisation;
    - expliquent les concepts clés des dispositions des articles 42 et 43 relatives à la certification;
    - expliquent le champ d'application des éléments qui peuvent être certifiés en vertu des articles 42 et 43 ainsi que la finalité de la certification; et

[3] Les présentes lignes directrices désigneront collectivement les mécanismes de certification et les labels et marques de protection des données sous le nom de «mécanismes de certification», voir section 1.3.2.
[4] Le considérant 100 indique que la mise en place de mécanismes de certification devrait être encouragée «[a]fin de favoriser la transparence et le respect du présent règlement pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question».
[5] Voir groupe de travail «Article 29», Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679 (WP 253).

- facilitent que le résultat de la certification soit utile, univoque, aussi reproductible que possible et comparable, et ce quel que soit l'organisme de certification (comparabilité).

8. Le RGPD permet aux États membres et aux autorités de contrôle de mettre en œuvre les articles 42 et 43 de plusieurs manières. Les présentes lignes directrices apportent des conseils sur l'interprétation et la mise en œuvre des dispositions des articles 42 et 43, et aideront les États membres, les autorités de contrôle et les organismes nationaux d'accréditation à adopter une approche harmonisée, plus cohérente, quant à la mise en œuvre des mécanismes de certification conformément au RGPD.

9. Les conseils figurant dans les présentes lignes directrices seront utiles:

    - aux autorités de contrôle compétentes et au comité européen de la protection des données lorsqu'ils approuvent les critères de certification conformément à l'article 42, paragraphe 5, à l'article 58, paragraphe 3, point f), et à l'article 70, paragraphe 1, point o);

    - aux organismes de certification lorsqu'ils élaborent et révisent les critères de certification avant de les soumettre à l'autorité de contrôle compétente pour approbation conformément à l'article 42, paragraphe 5;

    - au comité européen de la protection des données lorsqu'il approuve un label européen de protection des données en vertu de l'article 42, paragraphe 5, et de l'article 70, paragraphe 1, point o);

    - aux autorités de contrôle lorsqu'elles élaborent leurs propres critères de certification;

    - à la Commission européenne, qui est habilitée à adopter des actes délégués aux fins de préciser les exigences à prendre en considération en ce qui concerne les mécanismes de certification visés à l'article 43, paragraphe 8;

    - au comité européen de la protection des données lorsqu'il rend à la Commission européenne un avis sur les exigences de certification conformément à l'article 70, paragraphe 1, point q), et à l'article 43, paragraphe 8;

    - aux organismes nationaux d'accréditation qui devront tenir compte des critères de certification lors de la délivrance de l'agrément aux organismes de certification conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences complémentaires prévues à l'article 43; et

    - aux responsables du traitement et aux sous-traitants lorsqu'ils définissent leur propre stratégie de conformité avec le RGPD et qu'ils envisagent la certification comme moyen de démontrer cette conformité.

10. Le comité européen de la protection des données publiera des lignes directrices distinctes pour la détermination des critères d'approbation des mécanismes de certification en tant qu'outils de transfert vers des pays tiers ou des organisations internationales, conformément à l'article 42, paragraphe 2.

1.2 L'objectif de la certification au titre du RGPD

11. L'article 42, paragraphe 1, prévoit la mise en place de mécanismes de certification «aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement».

12. Le RGPD illustre le contexte dans lequel les mécanismes de certification approuvés peuvent être utilisés en tant qu'élément permettant de démontrer le respect par les responsables du traitement et les sous-traitants des obligations qui leur incombent en ce qui concerne:

    - la mise en œuvre et la démonstration des mesures techniques et organisationnelles appropriées visées à l'article 24, paragraphes 1 et 3, à l'article 25 et à l'article 32, paragraphes 1 et 3;

    - des garanties suffisantes (données par le sous-traitant au responsable du traitement) visées à l'article 28, paragraphe 1 et paragraphes 4 et 5 (données par un autre sous-traitant au sous-traitant initial).

13. Étant donné que la certification ne prouve pas la conformité en soi, mais qu'elle constitue plutôt un élément qui peut être utilisé pour démontrer cette conformité, elle devrait être produite de manière transparente. Des documents justificatifs sont nécessaires pour démontrer la conformité, en particulier des rapports écrits qui non seulement reprennent les critères mais décrivent également la manière dont ils sont respectés et qui, si ces critères n'étaient pas respectés au départ, décrivent les rectifications et les mesures correctives ainsi que leur pertinence, expliquant ainsi les motifs pour lesquels la certification doit être délivrée et maintenue. Ces documents doivent notamment décrire chaque décision de délivrance, de renouvellement ou de retrait d'un certificat. Ils devraient exposer les motifs, les arguments et les preuves résultant de l'application des critères, ainsi que les conclusions, les jugements ou les déductions des faits ou des prémisses recueillis pendant la certification.

1.3 Concepts clés

14. La section suivante étudie les concepts clés des articles 42 et 43. Cette analyse permet de comprendre les termes de base et la portée de la certification au titre du RGPD.

1.3.1 Interprétation du terme «certification»

15. Le RGPD ne définit pas le terme «certification». L'Organisation internationale de normalisation (ISO) donne une définition universelle de la certification: il s'agit d'une «assurance écrite (sous la forme d'un certificat) donnée par une tierce partie qu'un produit, service ou système est conforme à des exigences spécifiques». La certification est également définie comme une «évaluation de la conformité par une tierce partie» et les organismes de certification peuvent également être appelés «organismes d'évaluation de la conformité» (OEC). La norme EN-ISO/IEC 17000:2004 - Évaluation de la conformité -- Vocabulaire et principes généraux (auxquels la norme ISO17065 fait référence) - définit la certification en ces termes:

«attestation réalisée par une tierce partie... relative à des produits, des processus et des services».

16. Une attestation est la «fourniture d'une affirmation, basée sur une décision qui fait suite à la revue, démontrant que des exigences spécifiées sont respectées» (section 5.2, norme ISO 17000:2004).

17. Dans le cadre de la certification au titre des articles 42 et 43 du RGPD, la certification se réfère à l'attestation par un tiers relative aux opérations de traitement effectuées par les responsables du traitement et les sous-traitants.

1.3.2 Mécanismes de certification, labels et marques

18. Le RGPD ne définit pas les termes «mécanismes de certification», «labels» ou «marques» et les utilise collectivement. Un certificat est une attestation de conformité. Un label ou une marque peuvent être utilisés pour indiquer qu'une procédure de certification a été menée à bien. Un label ou une marque font généralement référence à un logo ou à un symbole dont la présence (en plus d'un certificat) indique que l'objet de la certification a été soumis à une évaluation indépendante dans le cadre d'une procédure de certification et qu'il est conforme à des exigences spécifiées, énoncées dans des documents normatifs tels que des règlements, des normes ou des spécifications techniques. Ces exigences relatives à la certification au titre du RGPD sont énoncées dans les exigences complémentaires qui complètent les règles d'agrément des organismes de certification de la norme EN-ISO/IEC 17065/2012 et les critères de certification approuvés par l'autorité de contrôle compétente ou le comité. Un certificat, un label ou une marque ne peuvent être délivrés au titre du RGPD qu'à l'issue d'une évaluation indépendante des preuves réalisée par un organisme de certification agréé ou par une autorité de contrôle compétente, indiquant que les critères de certification sont remplis.

19. Le tableau fournit un exemple générique d'un processus de certification.

Présentation de la demande par le responsable du traitement ou le sous-traitant	Contrôle formel par l'organisme de certification	Évaluation Pré-évaluation	Évaluation Évaluation de la cible d'évaluation	Évaluation Validation des résultats	Information à l'autorité de contrôle compétente	Certification	Contrôle	Renouvellement de la certification
La description de la cible d'évaluation est-elle univoque et complète, y compris les interfaces ?	La description de la cible d'évaluation peut-elle être acceptée ?	Quels sont les critères applicables ?	La cible d'évaluation satisfait-elle aux critères ?	Tous les critères pertinents spécifiés tiennent-ils compte de la cible d'évaluation ?	Les raisons de la délivrance ou du retrait de la certification ont-elles été fournies ?	Le certificat peut-il être délivré ?	La cible d'évaluation continue-t-elle de satisfaire aux critères ?	Le traitement satisfait-il encore aux critères ?
L'accès aux activités de traitement de la cible d'évaluation peut-il être accordé ?	Tous les documents sont-ils complets et à jour ?	Quelles sont les méthodes d'évaluation applicables ?	La documentation de la cible d'évaluation est-elle correcte ?	L'évaluation a-t-elle été suffisamment documentée ?		Les rapports sont-ils prêts à être publiés ?	Le certificat, le label ou la marque de confiance sont-ils utilisés à bon escient ?	Les domaines de développement ont-ils été traités de manière satisfaisante ?
Article 42, paragraphe 6	Article 43, paragraphe 4	Article 43, paragraphe 4	Article 42, paragraphe 5, Article 43, paragraphe 4	Article 43, paragraphe 4	Article 43, paragraphe 1, Article 43, paragraphe 5	Article 43, paragraphe 1, Article 42, paragraphe 7	Article 42, paragraphe 7	Article 42, paragraphe 7

2 LE ROLE DES AUTORITES DE CONTROLE

20. L'article 42, paragraphe 5, prévoit que la certification est délivrée par un organisme de certification agréé ou par une autorité de contrôle compétente. Le RGPD ne prévoit pas que la délivrance des certifications soit réservée aux seules autorités de contrôle, mais permet, au lieu de cela, plusieurs modèles différents. Par exemple, une autorité de contrôle peut choisir une ou plusieurs des options suivantes:

    - délivrer la certification elle-même, dans le cadre de son propre système de certification;
    - délivrer la certification elle-même, dans le cadre de son propre système de certification, mais déléguer tout ou partie du processus d'évaluation à des tiers;
    - créer son propre système de certification et confier la procédure de certification à des organismes de certification qui délivrent la certification; et
    - encourager le marché à mettre au point des mécanismes de certification.

21. Une autorité de contrôle devra également considérer son rôle à la lumière des décisions prises au niveau national concernant les mécanismes d'agrément, en particulier si l'autorité de

contrôle elle-même est habilitée à délivrer des agréments aux organismes de certification en vertu de l'article 43, paragraphe 1, du RGPD. Ainsi, chaque autorité de contrôle déterminera l'approche à adopter pour atteindre l'objectif général de la certification au titre du RGPD. Cette approche sera déterminée non seulement dans le contexte des missions et des pouvoirs visés aux articles 57 et 58, mais également par le fait que la certification est un facteur à prendre en compte dans le calcul des amendes administratives et, plus généralement, en tant que moyen de démontrer la conformité.

2.1 Autorité de contrôle en tant qu'organisme de certification

22. Lorsqu'une autorité de contrôle choisit de se charger de la certification, elle devra évaluer son rôle avec précision par rapport aux missions dont elle est investie au titre du RGPD. Elle devrait faire preuve de transparence dans l'exercice de ses fonctions. Elle devra tenir compte en particulier de la séparation des pouvoirs en matière d'enquête et d'application des règles afin d'éviter tout conflit d'intérêts potentiel.

23. Si elle agit en tant qu'organisme de certification, l'autorité de contrôle devra veiller à ce qu'un mécanisme de certification soit mis en place de manière correcte et à élaborer ses propres critères de certification ou à en adopter d'autres. En outre, chaque autorité de contrôle qui délivre des certifications a pour mission de procéder à leur examen périodique [article 57, paragraphe 1, point o)] et dispose du pouvoir de les retirer si les exigences applicables à la certification ne sont pas ou plus satisfaites [article 58, paragraphe 2, point h)]. Pour satisfaire à ces exigences, il est utile de mettre en place une procédure de certification et des exigences concernant le processus et, sauf disposition contraire, par exemple de la législation nationale, de mettre en place un accord juridiquement contraignant avec chaque organisme demandeur pour l'exécution d'activités de certification. Il convient de veiller à ce que cet accord de certification exige du demandeur qu'il respecte au moins les critères de certification, y compris les dispositions nécessaires pour procéder à l'évaluation, au contrôle du respect des critères et à l'examen périodique, notamment l'accès aux informations et/ou aux locaux, la documentation et la publication de rapports et de résultats et la conduite d'enquêtes en cas de réclamations. Outre les exigences prévues à l'article 43, paragraphe 2, il est escompté qu'une autorité de contrôle respecte les exigences des lignes directrices concernant l'agrément des organismes de certification.

2.2 Autres missions de l'autorité de contrôle en matière de certification

24. Dans les États membres où des organismes de certification sont créés, l'autorité de contrôle a le pouvoir et la mission, indépendamment de ses propres activités:

    - d'évaluer les critères d'un système de certification et d'élaborer un projet de décision (article 42, paragraphe 5);
    - de communiquer le projet de décision au comité lorsqu'elle a l'intention d'approuver les critères de certification [article 64, paragraphe 1, point c) et article 64, paragraphe 7] et d'examiner l'avis du comité [article 64, paragraphe 1, point c) et article 70, paragraphe 1, point t)];

- d’approuver les critères de certification [article 58, paragraphe 3, point f)] avant que l’agrément et la certification puissent avoir lieu [article 42, paragraphe 5, et article 43, paragraphe 2, point b)];
- de publier les critères de certification (article 43, paragraphe 6);
- d’agir en tant qu’autorité compétente pour les systèmes de certification à l’échelle de l’UE, ce qui peut donner lieu à des labels européens de protection des données approuvés par le comité européen de la protection des données [article 42, paragraphe 5, et article 70, paragraphe 1, point o)]; et
- d’ordonner à un organisme de certification a) de ne pas délivrer de certification ou b) de retirer la certification si les exigences applicables à la certification (procédures ou critères de certification) ne sont pas ou plus satisfaites [article 58, paragraphe 2, point h)].

25. Le RGPD charge l’autorité de contrôle d’approuver les critères de certification, mais pas de les élaborer. Afin d’approuver les critères de certification en vertu de l’article 42, paragraphe 5, l’autorité de contrôle devrait savoir clairement à quoi s’attendre, notamment s’agissant de la portée et du contenu de la démonstration du respect du RGPD ainsi que de sa mission consistant à contrôler l’application du règlement et à veiller au respect de celui-ci. L’annexe fournit des orientations visant à garantir une approche harmonisée concernant l’évaluation des critères aux fins de l’approbation.

26. L’article 43, paragraphe 1, impose aux organismes de certification d’informer leur autorité de contrôle avant de délivrer ou de renouveler des certifications afin de permettre à l’autorité de contrôle compétente d’exercer le pouvoir d’adopter des mesures correctrices que lui confère l’article 58, paragraphe 2, point h). En outre, l’article 43, paragraphe 5, exige également des organismes de certification qu’ils communiquent à l’autorité de contrôle compétente les raisons de la délivrance ou du retrait de la certification demandée. Bien que le RGPD permette aux autorités de contrôle de déterminer comment recevoir, reconnaître, examiner et traiter ces informations sur le plan opérationnel (par exemple à l’aide de solutions technologiques permettant aux organismes de certification d’établir des rapports), un processus et des critères permettant à l’organisme de certification de traiter les informations et les rapports fournis concernant chaque projet de certification abouti, conformément à l’article 43, paragraphe 1, pourraient être mis en place. Sur la base de ces informations, l’autorité de contrôle peut exercer son pouvoir consistant à ordonner à l’organisme de certification de retirer ou de ne pas délivrer une certification [article 58, paragraphe 2, point h)] et de contrôler l’application des exigences et des critères de certification et de veiller au respect de celles-ci en vertu du RGPD [article 57, paragraphe 1, point a), et article 58, paragraphe 2, point h)]. Cela favorisera une approche harmonisée et la comparabilité des certifications délivrées par les différents organismes de certification, et permettra aux autorités de contrôle de disposer d’informations sur le statut d’une organisation en matière de certification.

3 LE ROLE D'UN ORGANISME DE CERTIFICATION

27. Un organisme de certification a pour fonction de délivrer, d'examiner, de renouveler et de retirer les certifications (article 42, paragraphes 5 et 7) sur la base d'un mécanisme de certification et de critères approuvés (article 43, paragraphe 1). Cela exige de l'organisme de certification ou du propriétaire d'un système de certification qu'il détermine et mette en place des critères et des procédures de certification, notamment des procédures de contrôle du respect des critères, d'examen, de traitement des réclamations et de retrait. Les critères de certification sont examinés dans le cadre du processus d'agrément qui prend en considération les règles et procédures de délivrance des certifications, des labels ou des marques [article 43, paragraphe 2, point c)].

28. Un mécanisme de certification et des critères de certification doivent exister pour que l'organisme de certification puisse être agréé conformément à l'article 43. La portée et le type de critères de certification, qui ont une incidence significative sur les procédures de certification, et vice versa, influent fortement sur les activités d'un organisme de certification. Des critères spécifiques peuvent, par exemple, nécessiter des méthodes d'évaluation spécifiques, telles que des inspections sur site et la révision du code. Ces procédures sont obligatoires pour l'agrément et sont expliquées plus en détail dans les lignes directrices relatives à l'agrément.

29. L'organisme de certification est tenu par le RGPD de fournir des informations aux autorités de contrôle, notamment concernant les certifications respectives, qui sont nécessaires pour contrôler l'application du mécanisme de certification [article 42, paragraphe 7, article 43, paragraphe 5, et article 58, paragraphe 2, point h)].

4 APPROBATION DES CRITERES DE CERTIFICATION

30. Les critères de certification font partie intégrante de tout mécanisme de certification. Par conséquent, le RGPD exige de l'autorité de contrôle compétente qu'elle approuve les critères de certification d'un mécanisme de certification [article 42, paragraphe 5, et article 43, paragraphe 2, point b)]. Dans le cas d'un label européen de protection des données, les critères de certification sont approuvés par le comité européen de la protection des données [article 42, paragraphe 5, et article 70, paragraphe 1, point o)]. Les deux méthodes d'approbation des critères de certification sont expliquées ci-dessous.

31. Le comité européen de la protection des données reconnaît les objectifs suivants concernant l'approbation des critères de certification:

    - refléter correctement les exigences et les principes concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel énoncés dans le règlement (UE) 2016/679; et
    - contribuer à l'application cohérente du RGPD.

32. L'approbation est accordée sur la base de l'exigence du RGPD selon laquelle le mécanisme de certification permet aux responsables du traitement et aux sous-traitants de démontrer que les critères de certification respectent pleinement le RGPD.

4.1 Approbation des critères par l'autorité de contrôle compétente

33. L'autorité de contrôle compétente doit approuver les critères de certification avant ou pendant le processus d'agrément d'un organisme de certification. L'approbation est également requise pour les systèmes ou ensembles de critères mis à jour ou complémentaires au titre de la norme ISO 17065 par le même organisme de certification, avant l'utilisation des mécanismes de certification modifiés [articles 42, paragraphe 5 et article 43, paragraphe 2, point b)]. Les autorités de contrôle traitent toutes les demandes d'approbation des critères de certification sur un pied d'égalité et de manière non discriminatoire, selon une procédure accessible au public qui stipule les conditions générales qui doivent être satisfaites et décrit le processus d'approbation.

34. Un organisme de certification ne peut délivrer une certification dans un État membre donné que sur la base des critères que l'autorité de contrôle de cet État membre a approuvés. Autrement dit, l'autorité de contrôle compétente doit approuver les critères de certification si l'organisme de certification souhaite offrir des services de certification et s'il obtient l'agrément. Voir la section ci-dessous pour les systèmes de certification à l'échelle européenne.

4.2 Approbation des critères par le comité européen de la protection des données pour le label européen de protection des données

35. Un organisme de certification peut également délivrer une certification conformément aux critères approuvés par le comité européen de la protection des données pour le label européen de protection des données. Les critères de certification approuvés par le comité européen de la protection des données conformément à l'article 63 peuvent donner lieu à un label européen de protection des données (article 42, paragraphe 5). À la lumière des conventions existantes en matière de certification et d'agrément, le comité européen de la protection des données reconnaît qu'il est souhaitable d'éviter la fragmentation du marché de la certification en matière de protection des données. Il note que l'article 42, paragraphe 1, prévoit que les États membres, les autorités de contrôle, le comité et la Commission encouragent la mise en place de mécanismes de certification, en particulier au niveau de l'Union.

4.2.1 Demande d'approbation

36. La demande d'approbation des critères conformément à l'article 42, paragraphe 5, et à l'article 70, paragraphe 1, point o), par le comité européen de la protection des données doit être présentée par l'intermédiaire d'une autorité de contrôle compétente et doit indiquer l'intention du propriétaire du système, du demandeur ou de l'organisme de certification agréé de proposer ces critères dans un mécanisme de certification destiné aux responsables du traitement et aux sous-traitants dans tous les États membres. L'autorité de contrôle

compétente fournira un projet au comité européen de la protection des données lorsqu'elle estimera que ledit comité pourrait approuver les critères.

37. Le choix du lieu de dépôt d'une demande d'approbation des critères dépendra du siège des propriétaires du système de certification ou des organismes de certification.

38. Si un organisme de certification dépose une demande, normalement sa demande d'agrément est en cours ou l'agrément lui a déjà été délivré soit par l'autorité de contrôle compétente, soit par l'organisme national d'accréditation de son État membre. Le fait que l'organisme de certification dispose déjà d'un agrément pour un mécanisme de certification au titre du RGPD peut contribuer à simplifier le processus d'approbation.

4.2.2 Critères du label européen de protection des données

39. Le comité européen de la protection des données coordonnera le processus d'évaluation et approuvera les critères du label européen de protection des données le cas échéant. L'évaluation portera sur des aspects tels que: le champ d'application des critères et la capacité à servir de certification commune. Lorsque le comité européen de la protection des données approuve les critères, l'autorité de contrôle compétente pour le siège européen de l'organisme de certification est censée traiter les réclamations relatives au mécanisme en tant que tel et informer les autres autorités de contrôle. Cette autorité de contrôle est également compétente pour prendre des mesures à l'encontre de l'organisme de certification. Selon le cas, l'autorité de contrôle compétente en informe les autres autorités de surveillance et le comité européen de la protection des données.

40. Les critères de certification portant sur une certification commune sont soumis à des exigences à l'échelle de l'UE et devraient fournir un mécanisme spécifique permettant d'y répondre. Les mécanismes de certification européens doivent pouvoir être utilisés dans tous les États membres. Sur la base de l'article 42, paragraphe 5, le mécanisme relatif à un label européen de protection des données et ses critères doivent pouvoir être adaptés de manière à tenir compte, le cas échéant, des réglementations sectorielles nationales, par exemple pour le traitement des données dans les établissements scolaires, et doivent prévoir une application à l'échelle européenne.

41. Exemple: une école internationale dispensant un enseignement aux personnes concernées dans l'Union est établie dans l'État membre «A». Cet établissement souhaite faire certifier son processus d'inscription en ligne par un système de certification à l'échelle européenne afin d'obtenir un label européen de protection des données. Cette école souhaite demander la certification des opérations de traitement par un organisme de certification établi dans l'État membre «B» sur la base d'un label européen de protection des données. Les critères du label conçus et documentés dans le mécanisme pertinent doivent pouvoir tenir compte de la réglementation applicable aux établissements scolaires dans l'État membre «A». Les critères devraient également exiger que la procédure d'inscription en ligne de l'établissement scolaire fournisse des informations et tienne compte des exigences applicables en matière de protection des données dans l'État membre, qui peuvent être différentes dans d'autres États membres. Il peut s'agir, par exemple, d'ensembles de données à caractère personnel communiqués aux fins de l'inscription, telles que des notes ou des résultats d'évaluations effectuées à la maternelle, de durées de conservation différentes, de la collecte ou du

traitement de données financières ou biométriques ou de restrictions concernant le traitement ultérieur.

- Les critères de haut niveau pour l'approbation d'un mécanisme de label européen de protection des données comprennent:
  - les critères approuvés par le comité;
  - l'application dans l'ensemble des systèmes juridiques, en tenant compte, le cas échéant, des exigences juridiques nationales et des réglementations sectorielles spécifiques;

- des critères harmonisés qui peuvent être adaptés aux exigences nationales;
  - la description du mécanisme de certification;
  - les accords de certification reconnaissant les exigences paneuropéennes;
  - des procédures visant à garantir et à apporter des solutions aux différences nationales et à s'assurer que le label contribue à démontrer le respect du RGPD; et
  - la langue des rapports adressés à toutes les autorités de contrôle concernées.

42. L'annexe contient également des conseils relatifs aux critères du label européen de protection des données.

4.2.3 Rôle de l'agrément

43. Comme indiqué au point 4.2.1, lorsqu'il est déterminé que des critères peuvent faire l'objet d'une certification commune et que le comité les a approuvés en tant que tels conformément à l'article 42, paragraphe 5, les organismes de certification peuvent être agréés pour exécuter les tâches de certification au niveau de l'Union selon ces critères.

44. Les systèmes destinés à être proposés dans certains États membres uniquement ne pourront prétendre aux labels de l'Union européenne. L'agrément aux fins d'un label européen de protection des données nécessitera un agrément dans l'État membre où se trouve le siège de l'organisme de certification qui entend exploiter le système, c'est-à-dire de l'organisme de certification chargé de délivrer les certifications et de gérer les activités de certification de ses entités et filiales dans d'autres États membres. Lorsque d'autres établissements ou bureaux gèrent et exécutent des tâches de certification de manière autonome, chacun de ces établissements ou bureaux devra disposer d'un agrément distinct dans l'État membre où il est établi. En d'autres termes, l'agrément est uniquement nécessaire dans l'État membre où se trouve le siège de l'organisme de certification lorsque seul le siège délivre les certificats. En revanche, lorsque d'autres établissements de l'organisme de certification délivrent également des certificats, ces établissements doivent également être agréés.

45. Par conséquent, si un organisme de certification n'est pas agréé pour délivrer des certificats au titre du label européen de protection des données, les critères approuvés par le comité européen de la protection des données ne peuvent être utilisés et le label ne peut être proposé.

5 ÉLABORATION DES CRITERES DE CERTIFICATION

46. Le RGPD a établi le cadre relatif à l'élaboration des critères de certification. Alors que les articles 42 et 43 traitent des exigences fondamentales concernant la procédure de certification tout en fournissant également des critères essentiels pour les procédures de certification, la base des critères de certification doit résulter des principes et des règles du RGPD et contribuer à garantir que ceux-ci sont respectés.

47. Lors de l'élaboration des critères de certification, il convient de se concentrer sur le caractère vérifiable, l'importance et la pertinence des critères de certification destinés à démontrer le respect du règlement. Les critères de certification devraient être formulés de manière à être clairs et compréhensibles et à pouvoir être appliqués dans la pratique.

48. Lors de l'élaboration des critères de certification, il est tenu compte, le cas échéant, des aspects de conformité suivants sur lesquels repose, entre autres, l'évaluation du traitement:

    - la licéité du traitement conformément à l'article 6;
    - les principes du traitement des données conformément à l'article 5;
    - les droits conférés aux personnes concernées en vertu des articles 12 à 23;
    - l'obligation de notifier les violations de données conformément à l'article 33;
    - l'obligation de protection des données dès la conception et par défaut, conformément à l'article 25;
    - si une analyse d'impact relative à la protection des données, conformément à l'article 35, paragraphe 7, point d), a été effectuée, le cas échéant; et
    - les mesures techniques et organisationnelles mises en place conformément à l'article 32.

49. La mesure dans laquelle ces considérations sont prises en compte dans les critères peut varier en fonction de la portée de la certification, qui peut comprendre le type d'opération(s) de traitement et le domaine (par exemple, le secteur de la santé) de la certification.

5.1 Quels éléments peuvent être certifiés au titre du RGPD?

50. Le comité européen de la protection des données considère que le RGPD offre des possibilités très larges quant aux éléments susceptibles d'être certifiés au titre du RGPD, pour autant que l'accent soit mis sur la démonstration du respect de ce règlement par les responsables du

traitement et les sous-traitants pour ce qui a trait à leurs opérations de traitement (article 42, paragraphe 1).

51. Lors de l'évaluation d'une opération de traitement, il y a lieu de prendre en compte les trois éléments fondamentaux suivants, le cas échéant:

    1. les données à caractère personnel (champ d'application matériel du RGPD);
    2. les systèmes techniques: les infrastructures, telles que le matériel et les logiciels, utilisées pour traiter les données à caractère personnel; et
    3. les processus et les procédures liés au(x) opération(s) de traitement.

52. Chaque composant utilisé dans le cadre des opérations de traitement doit faire l'objet d'une évaluation en fonction des critères fixés. Au moins quatre facteurs significatifs différents peuvent avoir une influence: 1) l'organisation et la structure juridique du responsable du traitement ou du sous-traitant; 2) le service, l'environnement et les personnes participant au(x) opération(s) de traitement; 3) la description technique des éléments à évaluer; et enfin 4) les infrastructures informatiques soutenant le traitement, notamment les systèmes d'exploitation, les systèmes virtuels, les bases de données, les systèmes d'authentification et d'autorisation, les routeurs et pare-feu, les systèmes de stockage, les infrastructures de communication ou l'accès Internet et les mesures techniques connexes.

53. Ces trois éléments fondamentaux sont pertinents pour la conception des procédures et des critères de certification. La mesure dans laquelle ils sont pris en compte peut varier en fonction de l'objet de la certification. Par exemple, dans certains cas, certains composants peuvent être ignorés s'ils ne sont pas jugés pertinents par rapport à l'objet de la certification.

54. Afin de préciser davantage les éléments susceptibles d'être certifiés au titre du RGPD, le RGPD comporte d'autres orientations. Il découle de l'article 42, paragraphe 7, que les certifications délivrées au titre du RGPD ne le sont qu'aux responsables du traitement des données et aux sous-traitants, ce qui exclut par exemple la certification des délégués à la protection des données. L'article 43, paragraphe 1, point b), renvoie à la norme ISO 17065 qui prévoit l'agrément des organismes de certification évaluant la conformité des produits, des services et des processus. Une opération de traitement ou un ensemble d'opérations peuvent donner lieu à un produit ou à un service selon la terminologie de la norme ISO 17065 et faire l'objet d'une certification. Par exemple, le traitement des données des employés aux fins du versement des salaires ou de la gestion des congés est un ensemble d'opérations au sens du RGPD et peut donner lieu à un produit, à un processus ou à un service selon la terminologie de l'ISO.

55. Sur la base de ces considérations, le comité européen de la protection des données considère que la portée de la certification au titre du RGPD s'étend aux opérations ou aux ensembles d'opérations de traitement. Il peut s'agir de processus de gouvernance, c'est-à-dire de mesures organisationnelles qui font donc partie intégrante d'une opération de traitement (par exemple, le processus de gouvernance mis en place pour la gestion des réclamations dans le cadre du traitement des données des employés aux fins du versement des salaires).

56. Afin d'évaluer le respect de l'opération de traitement au regard des critères de certification, il y a lieu de fournir un cas d'utilisation. Par exemple, la conformité de l'utilisation

d'infrastructures techniques déployées dans le cadre d'une opération de traitement dépend des catégories de données que ces infrastructures sont destinées à traiter. Les mesures organisationnelles dépendent des catégories et du volume de données ainsi que des infrastructures techniques utilisées pour leur traitement, compte tenu de la nature, de la portée, du contenu et des finalités du traitement, ainsi que des risques pour les droits et les libertés des personnes concernées.

57. En outre, il ne faut pas oublier que les applications informatiques peuvent être très différentes même si elles servent les mêmes objectifs de traitement. Il convient donc d'en tenir compte lors de la définition de la portée des mécanismes de certification et de l'élaboration des critères de certification, c'est-à-dire que ces deux aspects ne doivent pas être restreints au point d'exclure des applications informatiques conçues différemment.

5.2 Détermination de l'objet de la certification

58. Il y a lieu de distinguer le champ d'application d'un mécanisme de certification et son objet, que l'on appelle également cible d'évaluation, dans les différents projets de certification relevant d'un mécanisme de certification. Un mécanisme de certification peut définir sa portée de manière générale ou par rapport à un type ou à un domaine spécifique d'opérations de traitement, et peut donc déjà déterminer les objets de certification qui relèvent de sa portée (par exemple, le stockage sécurisé et la protection de données à caractère personnel contenues dans un coffre-fort numérique). En tout état de cause, une évaluation fiable et valable de la conformité ne peut avoir lieu que si l'objet d'un projet de certification est décrit avec précision. Il convient de décrire clairement les opérations de traitement comprises dans l'objet de la certification et d'indiquer quels sont les éléments fondamentaux, c'est-à-dire les données, les processus et les infrastructures techniques, qui seront évalués et ceux qui ne le seront pas. Pour ce faire, il y a lieu de toujours prendre en compte et de décrire les interfaces avec d'autres processus. Il est clair que des éléments inconnus ne peuvent faire partie de l'évaluation et ne peuvent donc être certifiés. En tout état de cause, l'objet de la certification doit faire sens au regard du message ou de l'affirmation formulé(e) concernant/par la certification et ne doit pas induire en erreur l'utilisateur, le client ou le consommateur.

59. [Exemple 1]

    Une banque propose à ses clients un site web offrant des services bancaires en ligne. Dans le cadre de ces services, il est possible d'effectuer des virements, d'acheter des actions, de mettre en place des virements permanents et de gérer son compte. Dans le cadre d'un mécanisme de certification de la protection des données ayant une portée générale fondée sur des critères génériques, la banque souhaite certifier les éléments suivants:

    a) Connexion sécurisée

       La connexion sécurisée est une opération de traitement compréhensible pour l'utilisateur final et pertinente du point de vue de la protection des données, car elle joue un rôle important pour garantir la sécurité des données à caractère personnel en question. Par conséquent, cette opération de traitement est nécessaire pour une connexion sécurisée et peut donc constituer une cible d'évaluation valable si le

certificat indique clairement que seule l'opération de traitement relative à la connexion est certifiée.

b) Interface frontale (front-end)

Bien que l'interface frontale puisse être pertinente du point de vue de la protection des données, elle n'est pas compréhensible pour l'utilisateur final et ne peut donc constituer une cible d'évaluation valable. En outre, l'utilisateur ne comprend pas clairement quels sont les services en ligne et, partant, les opérations de traitement, que couvre la certification.

c) Services bancaires en ligne

Les opérations au niveau de l'interface frontale et de l'interface dorsale (back-end) sont des opérations de traitement fournies dans le cadre des services bancaires en ligne qui peuvent avoir un sens pour l'utilisateur. Dans ce contexte, les deux doivent faire partie de la cible d'évaluation, alors que les opérations de traitement qui ne sont pas directement liées à la prestation des services bancaires en ligne, telles que les opérations de traitement destinées à la prévention du blanchiment de capitaux, peuvent être exclues de la cible d'évaluation.

Toutefois, les services bancaires en ligne que la banque propose sur son site web peuvent également inclure des services supplémentaires qui, à leur tour, nécessitent leurs propres opérations de traitement. Dans ce contexte, il peut par exemple s'agir d'un produit d'assurance. Étant donné que ce service supplémentaire n'est pas directement lié à l'objectif consistant à fournir des services bancaires en ligne, il peut être exclu de la cible d'évaluation. Si ce service supplémentaire (assurance) est exclu de la cible d'évaluation, les interfaces de ce service intégrées au site web font partie de la cible d'évaluation et doivent donc être décrites afin de distinguer clairement les différents services. Une telle description est nécessaire afin de déterminer et d'évaluer les éventuels flux de données entre les deux services.

60. [Exemple 2]

Une banque offre à ses clients un service leur permettant d'agréger les informations relatives à différents comptes et cartes de crédit de plusieurs banques (agrégation de comptes). La banque souhaite faire certifier son service au titre du RGPD. L'autorité de contrôle compétente a approuvé un ensemble spécifique de critères de certification portant sur ce type d'activité. La portée du mécanisme de certification ne couvre que les aspects de conformité suivants:

- l'authentification de l'utilisateur; et
- les moyens acceptables pour obtenir les données à agréger auprès d'autres banques/services.

Étant donné que la portée de ce mécanisme de certification définit à elle seule la cible d'évaluation, il n'est pas possible de restreindre de manière sensée la portée proposée et de certifier uniquement des caractéristiques spécifiques ou une seule activité de traitement. Dans ce scénario, une cible d'évaluation doit correspondre à une portée spécifique.

5.3 Méthodes d'évaluation et méthodologies de l'évaluation

61. Une évaluation de la conformité qui vise à contribuer à démontrer que les opérations de traitement respectent le règlement exige de définir et de déterminer les méthodes d'évaluation et la méthodologie de l'évaluation. Il importe de savoir si les informations nécessaires à l'évaluation sont collectées uniquement à partir de documents (ce qui ne serait pas suffisant en soi) ou si elles sont activement collectées sur site et par accès direct ou indirect. La manière dont les informations sont collectées a des conséquences sur la pertinence de la certification: il convient donc de définir et de décrire comment elles sont collectées.

    Les procédures de délivrance et d'examen périodique des certifications devraient comprendre des spécifications permettant de déterminer le niveau d'évaluation approprié (ampleur et niveau de détail) pour satisfaire aux critères de certification, et notamment les éléments suivants:

    - des informations sur les méthodes d'évaluation appliquées et les résultats obtenus, par exemple lors d'audits sur site ou à partir de documents,
    - des méthodes d'évaluation portant sur les opérations de traitement (données, systèmes, processus) et la finalité du traitement,
    - la détermination des catégories de données, des besoins en matière de protection et la question de savoir si des sous-traitants ou des tiers sont impliqués,
    - la détermination des rôles et de l'existence d'un mécanisme de contrôle des accès défini en fonction des rôles et des responsabilités.

62. L'ampleur de l'évaluation a une incidence sur la pertinence et la valeur de la certification. La réduction de l'ampleur de l'évaluation à des fins pragmatiques ou pour diminuer les coûts réduira la pertinence d'une certification en matière de protection des données. Par ailleurs, les décisions relatives au niveau de détail de l'évaluation peuvent dépasser les capacités financières du demandeur et, souvent, les capacités des évaluateurs et des auditeurs également. Pour démontrer le respect du règlement, il n'est pas toujours essentiel que l'analyse des systèmes informatiques utilisés soit très détaillée pour rester pertinente.

5.4 Documentation de l'évaluation

63. La documentation de la certification doit être complète et exhaustive. Une évaluation appropriée ne peut avoir lieu si toute la documentation n'est pas réunie. La documentation de la certification a pour fonction essentielle d'assurer la transparence du processus d'évaluation dans le cadre du mécanisme de certification. La documentation apporte des réponses aux questions concernant les exigences prévues par la loi. Les mécanismes de certification devraient prévoir une méthode normalisée en matière de documentation. Par la suite, l'évaluation permettra de comparer la documentation de la certification avec la situation réelle sur site et par rapport aux critères de certification.

64. Une documentation complète sur les éléments qui ont fait l'objet de la certification et sur les méthodes utilisées contribue à la transparence. Conformément à l'article 43, paragraphe 2, point c), les mécanismes de certification devraient mettre en place des procédures permettant l'examen des certifications. Afin de permettre à l'autorité de contrôle d'évaluer si la

certification peut être reconnue dans le cadre d'une enquête formelle et dans quelle mesure elle peut l'être, une documentation détaillée peut constituer le moyen de communication le plus approprié. La documentation produite au cours de l'évaluation devrait donc porter sur trois aspects principaux:

- la cohérence et l'homogénéité des méthodes d'évaluation mises en œuvre;
- les méthodes d'évaluation visant à démontrer que l'objet de la certification respecte les critères de certification et, partant, le règlement; et
- le fait que les résultats de l'évaluation ont été validés par un organisme de certification indépendant et impartial.

5.5 Documentation des résultats

65. Le considérant 100 fournit des informations sur les objectifs de l'introduction de la certification.

«Afin de favoriser la transparence et le respect du présent règlement, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.»

66. La documentation et la communication des résultats jouent un rôle important pour favoriser la transparence. Les organismes de certification qui utilisent des mécanismes de certification, des labels ou des marques destinés aux personnes concernées (en leur qualité de consommateurs ou de clients) devraient fournir des informations facilement accessibles, intelligibles et qui fassent sens sur la ou les opérations de traitement certifiées. Ces informations publiques devraient au moins comprendre

    - la description de la cible d'évaluation;
    - la référence aux critères approuvés appliqués à la cible d'évaluation spécifique;
    - la méthodologie de l'évaluation des critères (évaluation sur site, documentation, etc.); et
    - la durée de validité du certificat; et
    - devraient permettre la comparabilité des résultats par les autorités de contrôle et le public.

6 ORIENTATIONS RELATIVES A LA DEFINITION DES CRITERES DE CERTIFICATION

67. Les critères de certification font partie intégrante de tout mécanisme de certification. La procédure de certification comporte des exigences relatives à la manière, à l'auteur, à l'ampleur et au niveau de détail de l'évaluation qui doit avoir lieu dans les projets de certification individuels concernant un objet ou une cible d'évaluation spécifique. Les critères de certification fournissent les exigences nominales par rapport auxquelles est évaluée l'opération de traitement réelle définie dans la cible d'évaluation. Les présentes lignes directrices relatives à la définition des critères de certification fournissent des conseils d'ordre général qui faciliteront l'évaluation des critères de certification aux fins de l'approbation.

    Il y a lieu de prendre en compte les considérations générales suivantes lors de l'approbation ou de la définition des critères de certification. Les critères de certification devraient:

    - être uniformes et vérifiables,
    - être vérifiables afin de faciliter l'évaluation des opérations de traitement au titre du RGPD, en précisant notamment les objectifs et les orientations en matière de mise en œuvre concernant la réalisation de ces objectifs;
    - être pertinents par rapport au public cible (par exemple: B to B et B to C);
    - prendre en compte d'autres normes et, le cas échéant, être interopérables avec celles-ci (normes ISO, normes nationales, par exemple); et
    - être souples et modulables afin qu'ils puissent s'appliquer à différents types et tailles d'organisations, y compris les micro, petites et moyennes entreprises, conformément à l'article 42, paragraphe 1, et à l'approche fondée sur les risques conformément au considérant 77.

68. Une petite entreprise locale, telle qu'un commerçant, effectue généralement des opérations de traitement moins complexes qu'une grande multinationale de la distribution. Si les exigences relatives à la licéité des traitements sont les mêmes, il y a lieu de prendre en compte l'ampleur et la complexité du traitement des données: les mécanismes de certification et leurs critères doivent donc être modulables en fonction de l'activité de traitement en question.

6.1 Normes existantes

69. Les organismes de certification devront examiner la manière dont des critères spécifiques tiennent compte des instruments pertinents existants, tels que les codes de conduite, les normes techniques ou les initiatives réglementaires et juridiques nationales. Idéalement, les critères seront interopérables avec les normes existantes qui peuvent aider un responsable du traitement ou un sous-traitant à respecter ses obligations en vertu du RGPD. Cependant, alors que les normes sectorielles privilégient souvent la protection et la sécurité de l'organisation contre les menaces, le RGPD est axé sur la protection des droits fondamentaux des personnes physiques. Il convient de prendre en compte cette perspective différente lors de la conception des critères ou de l'approbation des critères ou des mécanismes de certification fondés sur des normes sectorielles.

6.2 Définition des critères

70. Les critères de certification doivent correspondre à la déclaration de certification (message ou affirmation) d'un mécanisme ou d'un système de certification et répondre aux attentes que celui-ci suscite. Le nom d'un mécanisme de certification peut déjà en indiquer la portée et aura des conséquences sur la détermination des critères.

71. [Exemple 3]

    Un mécanisme appelé «HealthPrivacyMark» devrait limiter sa portée au secteur de la santé. Le nom du label laisse supposer que les exigences en matière de protection des données relatives à la santé ont été examinées. En conséquence, les critères de ce mécanisme doivent être adéquats pour évaluer les exigences en matière de protection des données dans ce secteur.

72. [Exemple 4]

    Un mécanisme relatif à la certification des opérations de traitement comprenant des systèmes de gouvernance en matière de traitement des données devrait déterminer des critères permettant de reconnaître et d'évaluer les processus de gouvernance et les mesures techniques et organisationnelles qui les soutiennent.

73. [Exemple 5]

    Les critères d'un mécanisme relatif à l'informatique en nuage doivent tenir compte des exigences techniques particulières nécessaires à l'utilisation de ce type de services. Par exemple, en cas d'utilisation de serveurs situés hors de l'Union européenne, les critères doivent tenir compte des conditions fixées au chapitre V du RGPD en ce qui concerne les transferts de données vers des pays tiers.

74. Les critères conçus pour s'adapter aux diverses cibles d'évaluation des différents secteurs et/ou États membres devraient: permettre une application dans différents scénarios; permettre de déterminer les mesures adéquates pour s'adapter aux opérations de traitement de petite, moyenne ou grande envergure, et refléter des risques présentant des degrés divers de probabilité et de gravité concernant les droits et les libertés des personnes physiques, conformément au RGPD. Par conséquent, les procédures de certification (par exemple pour la documentation, les essais, la méthode d'évaluation ou l'ampleur de l'évaluation) qui complètent les critères doivent répondre à ces besoins et disposer de règles, par exemple pour appliquer les critères pertinents à des projets de certification individuels. Les critères doivent permettre d'évaluer si des garanties suffisantes ont été fournies pour la mise en œuvre des mesures techniques et organisationnelles appropriées.

6.3 Durée de vie des critères de certification

75. Même si les critères de certification doivent être fiables dans le temps, ils ne doivent pas être figés. Ils sont sujets à révision, par exemple lorsque:

    - le cadre juridique est modifié;

- les modalités et les dispositions sont interprétées par les arrêts de la Cour de justice de l'Union européenne; ou
- l'état de la technique a évolué.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

ANNEXE 1: MISSIONS ET POUVOIRS DES AUTORITES DE CONTROLE EN MATIERE DE CERTIFICATION CONFORMEMENT AU RGPD

	Dispositions	Exigences
Missions	Article 43, paragraphe 6	Exige de l'autorité de contrôle qu'elle rende publics les critères visés à l'article 42, paragraphe 5, sous une forme aisément accessible, et qu'elle les transmette au comité.
	Article 57, paragraphe 1, point n)	Exige de l'autorité de contrôle qu'elle approuve les critères de certification conformément à l'article 42, paragraphe 5.
	Article 57, paragraphe 1, point o)	Prévoit que, si les circonstances l'exigent (c'est-à-dire lorsqu'elle délivre une certification), elle procède à un examen périodique de la certification délivrée conformément à l'article 42, paragraphe 7.
	Article 64, paragraphe 1, point c)	Exige de l'autorité de contrôle qu'elle communique le projet de décision au comité lorsqu'elle entend approuver les critères de certification visés à l'article 42, paragraphe 5.
Pouvoirs	Article 58, paragraphe 1, point c)	Prévoit que l'autorité de contrôle a le pouvoir de réviser la certification conformément à l'article 42, paragraphe 7;
	Article 58, paragraphe 2, point h)	Prévoit que l'autorité de contrôle a le pouvoir de retirer ou d'ordonner à l'organisme de certification de retirer une certification ou de ne pas délivrer une certification.
	Article 58, paragraphe 3, point e)	Prévoit que l'autorité de contrôle a le pouvoir d'agréer des organismes de certification
	Article 58, paragraphe 3, point f)	Prévoit que l'autorité de contrôle a le pouvoir de délivrer des certifications et d'approuver les critères de certification.

ANNEXE 2

1 INTRODUCTION

L'annexe 2 fournit des orientations pour l'examen et l'évaluation des critères de certification visés à l'article 42, paragraphe 5. Elle recense les thèmes qu'une autorité de contrôle de la protection des données et le comité européen de la protection des données examineront et appliqueront aux fins de l'approbation des critères de certification pour un mécanisme de certification. Les questions devraient être prises en considération par les organismes de certification et les propriétaires des systèmes de certification qui souhaitent définir et présenter des critères pour approbation. La liste n'est pas exhaustive, mais présente les thèmes minimaux à prendre en considération. Certaines questions seront sans objet: elles devraient néanmoins être prises en considération au moment de définir les critères et, le cas échéant, il conviendra d'expliquer pour quelles raisons les critères ne couvrent pas certains aspects particuliers. Certaines questions reviennent à plusieurs reprises, mais à chaque fois la perspective est différente. Il convient de prendre en considération les présentes orientations conformément aux exigences juridiques du RGPD et, le cas échéant, de la législation interne.

2 CHAMP D'APPLICATION DU MECANISME DE CERTIFICATION ET CIBLE DE L'EVALUATION

a. Le champ d'application du mécanisme de certification (pour lequel les critères de protection des données seront utilisés) est-il clairement énoncé?

b. Le champ d'application du mécanisme de certification fait-il sens pour le public visé, ou est-il susceptible d'induire ce public en erreur?

- *Exemple: Un «label de société de confiance» donne à penser que l'ensemble des opérations de traitement d'une société ont été contrôlées, alors que seules certaines opérations de traitement spécifiées, p.ex. le traitement des paiements en ligne, sont en fait soumises à certification. Par conséquent, le champ d'application induit en erreur.*

c. Le champ d'application du mécanisme de certification reflète-t-il l'ensemble des aspects pertinents des opérations de traitement?

- *Exemple: une «marque de respect de la vie privée dans le domaine de la santé» doit inclure l'ensemble des données d'évaluation concernant la santé afin de respecter les exigences de l'article 9.*

d. Le champ d'application du mécanisme de certification permet-il une certification valable en matière de protection des données, compte tenu de la nature, du contenu et du risque des opérations de traitement qui en relèvent?

- *Exemple: si le champ d'application du mécanisme de certification ne couvre que certains aspects des opérations de traitement, tels que la collecte de données, mais aucune autre opération de traitement, comme le traitement aux fins de créer des profils publicitaires ou la gestion des droits des personnes concernées, il ne fait pas sens pour les personnes concernées.*

e. Le champ d'application du mécanisme de certification couvre-t-il le traitement des données à caractère personnel dans le pays d'où émane la demande, ou comprend-il le traitement transfrontalier et/ou les transferts?

f. Les critères de certification indiquent-ils avec suffisamment de précision de quelle manière la cible d'évaluation doit être définie?

- *Exemple: un «label de protection de la vie privée» dont le champ d'application général exige uniquement «les spécifications du traitement soumis à certification» ne fournit pas d'orientations suffisamment claires sur la manière de définir et de décrire une cible d'évaluation.*
- *Exemple: un champ d'application (spécifique), le «label de protection de la vie privée pour les coffres-forts électroniques», concernant le stockage sécurisé, devrait décrire en détail quelles sont les exigences pour remplir les critères de ce champ d'application, p.ex. la définition des coffres électroniques, les exigences systèmes, les mesures techniques et organisationnelles obligatoires. Dans ce cas, le champ d'application peut définir clairement la cible d'évaluation.*

(1) Les critères exigent-ils de la cible d'évaluation qu'elle inclue un relevé de l'ensemble des opérations de traitement pertinentes, une illustration des flux de données et une détermination du champ d'application de la cible d'évaluation?

- *Exemple: un mécanisme de certification propose la certification des opérations de traitement assurées par les responsables du traitement au titre du RGPD, sans plus de précision sur le champ d'application (champ d'application général). Les critères utilisés par le mécanisme de certification exigent du responsable du traitement demandeur qu'il détermine l'opération de traitement ciblée (cible d'évaluation) en termes de types de données et de systèmes et de processus mis en œuvre.*

(2) Les critères exigent-ils du demandeur qu'il indique clairement où commence et finit le traitement soumis à évaluation? Les critères exigent-ils de la cible d'évaluation qu'elle inclue les interfaces alors que les opérations de traitement interdépendantes ne sont pas comprises dans la cible d'évaluation? Cela est-il justifié de manière satisfaisante?

- *Exemple: une cible d'évaluation décrivant de manière suffisamment détaillée les opérations de traitement d'un service en ligne, telles que l'enregistrement des utilisateurs, la prestation de services, la facturation, l'enregistrement des adresses IP, les interfaces pour utilisateurs et pour tiers, mais pas l'hébergement de serveurs (à l'exception toutefois des accords portant sur le traitement et les mesures techniques et organisationnelles obligatoires).*

g. Les critères garantissent-ils que chacune des cibles d'évaluation puisse être comprise par le public visé, et notamment les personnes concernées le cas échéant?

3 EXIGENCES GENERALES

a. L'ensemble des termes pertinents employés dans le catalogue des critères (autrement dit dans l'ensemble des critères de certification) sont-ils recensés, expliqués et définis?

b. L'ensemble des références normatives sont-elles indiquées?

c. Les critères comprennent-ils la définition des responsabilités, des procédures et du traitement en matière de protection des données couverts par le champ d'application du mécanisme de certification?

4 OPERATIONS DE TRAITEMENT, ARTICLE 42, PARAGRAPHE 1

S'agissant du champ d'application du mécanisme de certification (général ou spécifique), l'ensemble des composants des opérations de traitement (données, systèmes, et processus) est-il pris en compte par les critères?

a. Les critères exigent-ils que les bases juridiques du traitement soient identifiées en ce qui concerne la cible d'évaluation?

b. S'agissant de la cible d'évaluation, les critères tiennent-ils compte des phases importantes du traitement et du cycle de vie complet des données, y compris la suppression et / ou l'anonymisation?

c. S'agissant de la cible d'évaluation, les critères prévoient-ils la portabilité des données?

d. S'agissant de la cible d'évaluation, les critères permettent-ils d'identifier et de tenir compte de certains types particuliers d'opérations de traitement, p.ex. la prise de décision automatisée, le profilage?

e. S'agissant de la cible d'évaluation, les critères permettent-ils d'identifier les catégories particulières de données?

f. Les critères permettent-ils et exigent-ils l'évaluation du risque de chacune des opérations de traitement et des besoins en protection des droits et des libertés des personnes concernées?

g. Les critères permettent-ils et exigent-ils la prise en compte adéquate des risques pour les droits et les libertés des personnes physiques?

…

5 LICEITE DU TRAITEMENT

a. Les critères requièrent-ils de vérifier la licéité du traitement pour chacune des opérations de traitement, sur le plan de sa finalité et de sa nécessité?

b. Les critères requièrent-ils de vérifier l'ensemble des exigences d'une base juridique pour chacune des opérations de traitement?

6 PRINCIPES, ARTICLE 5

a. Les critères intègrent-ils dans une mesure adéquate l'ensemble des principes de protection des données visés à l'article 5?

b. Les critères exigent-ils la preuve de la minimisation des données pour la cible d'évaluation concernée?

…

7 OBLIGATIONS GENERALES DES RESPONSABLES DU TRAITEMENT ET DES SOUS-TRAITANTS

a. Les critères exigent-ils la preuve de l'existence d'accords contractuels entre sous-traitants et responsables du traitement?

b. Les contrats entre responsables du traitement et sous-traitant sont-ils soumis à évaluation?

c. Les critères rendent-ils compte des obligations du responsable du traitement visées au chapitre IV?

d. Les critères exigent-ils la preuve de l'examen et de l'actualisation des mesures techniques et organisationnelles mises en œuvre par le responsable du traitement, conformément à l'article 24, paragraphe 1?

e. Les critères vérifient-ils que l'organisation a évalué s'il convenait de désigner un délégué à la protection des données en vertu de l'article 37? Le cas échéant, le délégué à la protection des données répond-il aux exigences des articles 37 à 39?

f. Les critères vérifient-ils si un registre des activités de traitement doit être tenu, selon les dispositions de l'article 30, paragraphe 5, et, dans l'affirmative, s'il est tenu conformément aux exigences de l'article 30?

8 DROITS DES PERSONNES CONCERNEES

a. Les critères tiennent-ils compte de manière adéquate du droit de la personne concernée d'être informée et exigent-ils que des mesures soient mises en place?

b. Les critères exigent-ils que les personnes concernées se voient garantir un accès et un contrôle adéquats, voire plus larges, à/sur leurs données, y compris la portabilité des données?

c. Les critères exigent-ils la mise en place de mesures permettant d'intervenir dans l'opération de traitement afin de garantir les droits des personnes concernées, et d'autoriser les rectifications, l'effacement de données ou la limitation du traitement?

…

9 RISQUES POUR LES DROITS ET LES LIBERTES DES PERSONNES PHYSIQUES

a. Les critères permettent-ils et exigent-ils l'évaluation des risques pour les droits et les libertés des personnes physiques?

b. Les critères prévoient-ils ou exigent-ils une méthodologie reconnue d'évaluation des risques? Si tel est le cas, est-ce proportionné?

c. Les critères permettent-ils et exigent-ils une étude d'impact des opérations de traitement envisagées sur les droits et les libertés des personnes physiques?

d. Les critères exigent-ils une consultation préalable concernant les risques qui n'ont pu être atténués, à la lumière des résultats de l'analyse d'impact relative à la protection des données?

10 MESURES TECHNIQUES ET ORGANISATIONNELLES QUI GARANTISSENT LA PROTECTION

a. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles qui assurent la confidentialité des opérations de traitement?

b. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles qui assurent l'intégrité des opérations de traitement?

c. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles qui assurent la disponibilité des opérations de traitement?

d. Les critères exigent-ils la mise en œuvre de mesures qui assurent la transparence des opérations de traitement s'agissant

e. de la responsabilité?

f. des droits des personnes concernées?

g. de l'évaluation de chacune des opérations de traitement, p.ex. la transparence algorithmique?

h. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles garantissant les droits des personnes concernées, p.ex. la capacité à fournir des informations ou la portabilité des données?

i. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles permettant d'intervenir dans l'opération de traitement afin de garantir le droit des personnes concernées, et d'autoriser les rectifications, l'effacement de données ou la limitation du traitement?

j. Les critères exigent-ils la mise en œuvre de mesures permettant d'intervenir dans l'opération de traitement afin de corriger ou de vérifier le système ou le processus?

k. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles pour garantir la minimisation des données, par exemple, en dissociant ou en séparant les données de la personne concernée, au moyen de procédés d'anonymisation ou de pseudonymisation, ou encore d'isolation de systèmes de données?

l. Les critères exigent-ils la mise en œuvre de mesures techniques destinées à activer la protection des données par défaut?

m. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles pour protéger les données dès la conception, p.ex. un système de gestion de la protection des données pour démontrer, informer, contrôler et appliquer les exigences en matière de protection des données?

n. Les critères exigent-ils la mise en œuvre de mesures techniques et organisationnelles pour assurer la formation et l'éducation périodiques appropriées du personnel ayant un accès permanent ou régulier à des données à caractère personnel?

o. Les critères exigent-ils des mesures d'examen?

p. Les critères exigent-ils une auto-évaluation/ un audit interne?

q. Les critères exigent-ils la mise en œuvre d'une mesure pour veiller à ce que les obligations de notification d'une violation de données à caractère personnel soient exécutées en temps voulu et dans la mesure attendue?

r. Les critères exigent-ils que des procédures de gestion d'incidents soient en place et qu'elles aient été vérifiées?

s. Les critères exigent-ils la mise en place d'une veille de l'évolution des questions de respect de la vie privée et technologiques, et l'actualisation du système s'il y a lieu?

…

11 AUTRES CARACTERISTIQUES PARTICULIERES RESPECTUEUSES DE LA PROTECTION DES DONNEES

a. Les critères exigent-ils la mise en place de techniques de renforcement de la protection des données? Celles-ci pourraient comprendre des critères qui demandent une protection renforcée des données en éliminant ou en réduisant les données à caractère personnel et/ou le risque pour la protection des données.

- *Exemple: les critères qui demandent une non-associativité renforcée en utilisant une technologie de gestion de l'identité axée sur l'utilisateur, telle que la technologie «attribute-based credentials» (ABC) plutôt qu'une méthode de gestion de l'identité axée sur l'organisation, iraient dans le sens d'une technique de renforcement de la protection des données.*

b. Les critères exigent-ils la mise en œuvre de contrôles renforcés des personnes concernées pour faciliter l'autodétermination et la liberté de choix?

…

12 CRITERES AUX FINS DE DEMONTRER L'EXISTENCE DE GARANTIES APPROPRIEES POUR LE TRANSFERT DE DONNEES A CARACTERE PERSONNEL

Ces critères seront traités dans les prochaines lignes directrices consacrées à l'article 42, paragraphe 2.

13 CRITERES SUPPLEMENTAIRES POUR LE LABEL EUROPEEN DE PROTECTION DES DONNEES

a. Les critères envisagent-ils de couvrir tous les États membres?

b. Les critères peuvent-ils tenir compte de la législation ou des scénarios en matière de protection des données des États membres?

c. Les critères exigent-ils une évaluation de chaque cible d'évaluation quant aux dispositions sectorielles de la législation des États membres en matière de protection des données?

d. Les critères exigent-ils du responsable du traitement ou du sous-traitant qu'il fournisse des informations aux personnes concernées et aux parties intéressées dans les langues des États membres

e. sur le traitement /la cible d'évaluation?

f. sur la documentation du traitement/de la cible d'évaluation?

g. sur les résultats de l'évaluation?

…

14 ÉVALUATION GENERALE DES CRITERES

a. Les critères couvrent-ils intégralement le champ d'application du mécanisme de certification (autrement dit, sont-ils exhaustifs), de sorte qu'ils fournissent des garanties suffisantes pour que la certification puisse être fiable?

- *Exemple: si le champ d'application du mécanisme de certification couvre spécifiquement des opérations de traitement de données de santé, il conviendra de garantir un niveau très élevé de protection des données en définissant des critères qui assurent, par exemple, une évaluation en profondeur et l'application des principes de protection des données dès la conception et de protection des données par défaut.*

b. Les critères sont-ils proportionnés à l'échelle de l'opération de traitement couverte par le champ d'application du mécanisme de certification, au caractère sensible des informations et au risque lié au traitement?

c. Les critères sont-ils susceptibles d'améliorer le respect par les responsables du traitement et les sous-traitants de l'obligation de protection des données?

d. Les personnes concernées en bénéficieront-elles en ce qui concerne leur droit d'être informées, et notamment de se voir expliquer les résultats attendus?