Avis 14/2026 sur les critères de certification Europrivacy en qui concerne leur approbation par le comité en tant que label européen de protection des données conformément à l'article 42, paragraphe 5, du RGPD

Adopté le 15 avril 2026

Table des matières

1 Résumé des faits 5

2 Évaluation 7

2.1 Champ d'application du mécanisme de certification et cible de l'évaluation 8

2.2 Opérations de traitement 8

2.3 Licéité du traitement 9

2.4 Principes du traitement des données 10

2.5 Obligations générales des responsables du traitement et des sous-traitants 10

2.6 Droits des personnes concernées 11

2.7 Risques pour les droits et la liberté 11

2.8 Mesures techniques et organisationnelles qui garantissent la protection 12

2.9 Critères aux fins de démontrer l'existence de garanties appropriées pour le transfert de données à caractère personnel 12

3 Critères supplémentaires pour un label européen de protection des données 13

4 Conclusions/recommandations 14

5 Observations finales 14

Le comité européen de la protection des données,

vu l'article 63, l'article 64, paragraphe 2, et l'article 42 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 (ci-après l'«EEE») 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[1],

vu les articles 10 et 22 de son règlement intérieur,

considérant ce qui suit:

1. Les États membres, les autorités de contrôle, le comité européen de la protection des données (ci-après l'«EDPB» ou le «comité») et la Commission européenne encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données (ci-après les «mécanismes de certification») et de labels et marques en matière de protection des données, afin de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le RGPD, en tenant compte des besoins spécifiques des micro, petites et moyennes entreprises. En outre, la mise en place de mécanismes de certification peut améliorer la transparence et permettre aux personnes concernées d'évaluer le niveau de protection des données des produits et services concernés.

2. Les critères de certification font partie intégrante d'un mécanisme de certification. Par conséquent, le RGPD exige l'approbation des critères d'un mécanisme de certification national par l'autorité de contrôle compétente [article 42, paragraphe 5, et article 43, paragraphe 2, point b), du RGPD] ou, dans le cas d'un label européen de protection des données, par l'EDPB [article 42, paragraphe 5, et article 70, paragraphe 1, point o), du RGPD].

3. Lorsqu'une autorité de contrôle a l'intention de soumettre à l'approbation de l'EDPB un label européen de protection des données conformément à l'article 42, paragraphe 5, du RGPD, elle devrait indiquer l'intention du propriétaire du système de certification de proposer le mécanisme de certification dans tous les États membres. Dans ce cas, le rôle principal de l'EDPB est de garantir l'application cohérente du RGPD, au moyen du mécanisme de contrôle de la cohérence visé aux articles 63, 64 et 65 du RGPD. Dans ce cadre, conformément à l'article 64, paragraphe 2, du RGPD, l'EDPB approuve les critères de certification.

4. Le présent avis vise à garantir l'application cohérente du RGPD, notamment par les autorités de contrôle, les responsables du traitement et les sous-traitants, à la lumière des éléments essentiels que doivent établir les mécanismes de certification. En particulier, l'évaluation de l'EDPB est effectuée sur la base des «lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement» (ci-après les «lignes directrices») et de leur addendum fournissant des «orientations sur l'évaluation des critères de certification» (ci-après l'«addendum»), pour lesquelles la période de consultation publique a expiré le 26 mai 2021.

5. Par conséquent, le comité reconnaît que chaque mécanisme de certification devrait être examiné individuellement, et ce, sans préjudice de l'évaluation de tout autre mécanisme de certification.

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».

6. Les mécanismes de certification devraient permettre aux responsables du traitement et aux sous-traitants de démontrer qu'ils respectent le RGPD. Par conséquent, leurs critères devraient dûment tenir compte des exigences et principes relatifs à la protection des données à caractère personnel énoncés dans le RGPD et contribuer à l'application cohérente de ce dernier.
7. Par ailleurs, le propriétaire du système de certification devrait garantir la cohérence et la conformité du mécanisme de certification avec les normes ISO et pratiques de certification incluses ou utilisées.
8. En conséquence, les certifications devraient apporter une valeur ajoutée aux responsables du traitement et aux sous-traitants en contribuant à la mise en œuvre de mesures organisationnelles et techniques normalisées et déterminées qui facilitent et renforcent manifestement la conformité des opérations de traitement avec le RGPD, en tenant compte des exigences sectorielles.
9. Le comité salue les efforts consentis par les propriétaires de systèmes pour élaborer des mécanismes de certification, qui sont des outils pratiques et présentant potentiellement un bon rapport coût-efficacité, afin d'assurer une plus grande cohérence avec le RGPD et de favoriser le droit au respect de la vie privée et à la protection des données des personnes concernées en renforçant la transparence.
10. Le comité rappelle que les certifications sont des outils de responsabilisation volontaire et que l'adhésion à un mécanisme de certification ne minimise pas la responsabilité des responsables du traitement ou des sous-traitants en ce qui concerne le respect du RGPD et n'empêche pas les autorités de contrôle d'exercer leurs missions et pouvoirs en vertu du RGPD et des législations nationales pertinentes.
11. Dans le présent avis, le comité examine des questions telles que la portée, l'applicabilité et la pertinence des critères dans l'ensemble des États membres.
12. Le présent avis porte uniquement sur les critères de certification. Le comité peut avoir besoin d'informations de haut niveau sur les méthodes d'évaluation afin de pouvoir évaluer de manière approfondie le caractère vérifiable des critères dans le cadre de son avis. Toutefois, ce dernier n'emporte aucunement approbation desdites méthodes d'évaluation.
13. L'avis de l'EDPB est adopté conformément à l'article 64, paragraphe 2, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur du comité, dans un délai de huit semaines à compter du premier jour ouvrable suivant la date à laquelle le président du comité et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision du président, ce délai peut être prolongé de six semaines en fonction de la complexité de la question. Si le comité conclut dans son avis que les critères en cause ne peuvent pas être approuvés, l'autorité de contrôle peut soumettre à nouveau les critères pour approbation lorsque les préoccupations exprimées dans l'avis initial du comité ont été prises en considération.

A adopté le présent avis:

Résumé des faits

14. Conformément à l'article 42, paragraphe 5, du RGPD et aux lignes directrices, les critères de certification Europrivacy (version nº 82) (ci-après les « critères de certification ») ont été

élaborés par le Centre européen de certification et de protection de la vie privée (ci-après le «propriétaire du système»).

15. Le 29 janvier 2026, l'autorité de contrôle du Luxembourg (ci-après l'«autorité de contrôle luxembourgeoise») a soumis au comité européen de la protection des données les critères de certification Europrivacy (version nº 82) pour approbation, conformément à l'article 64, paragraphe 2, du RGPD.

16. La décision relative au caractère complet du dossier a été prise le 31 mars 2026.

17. Le comité rappelle qu'il a approuvé, par la publication de son avis 28/2022 le 10 octobre 2022, les critères de certification Europrivacy (version nº 60) en tant que label européen de protection des données conformément à l'article 42, paragraphe 5, du RGPD (ci-après l'«avis précédent de l'EDPB»).

18. Le présent avis porte sur la version modifiée des critères de certification Europrivacy (version nº 82). Tout d'abord, le comité relève que, dans cette version des critères de certification qui lui est actuellement présentée, le champ d'application a été étendu aux demandeurs soumis à l'article 3, paragraphe 2, du RGPD et, à cet égard, un critère relatif aux éventuels conflits avec des lois de pays tiers a été introduit. En outre, le comité constate que certains des critères de certification qu'il a approuvés en 2022 ont été adaptés, affinés et/ou clarifiés dans la version modifiée des critères de certification Europrivacy (version nº 82). Ces modifications concernent notamment: la désignation d'un représentant dans l'EEE et la coopération en cas de demande formulée par les autorités de protection des données compétentes dans l'EEE; le rapport d'évaluation du respect des obligations nationales, le traitement ultérieur, les garanties accompagnant le traitement de catégories particulières de données à caractère personnel, les droits des personnes concernées, le recours à des sous-traitants ultérieurs, le traitement des violations de données, l'évaluation des risques relatifs au traitement des données, ainsi que la politique et les exigences en matière de sécurité.

19. Le comité souligne que la modification des critères de certification déjà approuvés en 2022 aura une incidence sur les certifications délivrées jusqu'à présent, ainsi que sur les procédures de certification en cours. Par conséquent, une période de transition entre les labels européens de protection des données délivrés conformément aux critères de certification approuvés dans l'avis précédent de l'EDPB (version nº 60) et ceux délivrés conformément aux critères de certification (version nº 82) évalués dans le présent avis devrait être gérée de manière appropriée et transparente. À cet égard, le comité comprend, sur la base de la documentation transmise par le propriétaire du système, que toutes les procédures de certification en cours doivent être achevées d'ici la fin de 2026 et qu'après cette date, les critères de certification approuvés dans l'avis précédent de l'EDPB (version nº 60) ne seront plus utilisés pour délivrer de nouveaux certificats. Les certificats délivrés jusqu'à présent resteront valables jusqu'à la fin de leur période de validité de trois ans et seront renouvelés conformément aux critères de certification (version nº 82). Par conséquent, après la fin de 2029, les critères de certification approuvés dans l'avis précédent de l'EDPB (version nº 60) seront entièrement remplacés par les critères de certification (version nº 82). En outre, les informations relatives à ce plan de transition seront rendues publiques par le propriétaire du système. Certains ajustements sont peut-être nécessaires concernant l'accréditation des organismes de certification, mais le présent avis n'aborde pas cette question, car elle ne relève pas de la compétence du comité.

20. Le système général de certification Europrivacy n'est pas destiné à être utilisé comme outil au service des transferts conformément à l'article 42, paragraphe 2, et à l'article 46, point f), du RGPD. Le 29 janvier 2026, l'autorité de contrôle luxembourgeoise a également soumis au comité, pour approbation conformément à l'article 64, paragraphe 2, du RGPD, un ensemble supplémentaire de critères de certification (l'«extension du système de certification

Europrivacy pour la certification des importateurs de données au titre de l'article 46»), dont le champ d'application vise les responsables du traitement et les sous-traitants établis en dehors de l'EEE qui ne sont pas directement soumis au RGPD conformément à l'article 3, paragraphe 2, du RGPD, mais qui traitent des données à caractère personnel reçues d'un autre responsable du traitement ou sous-traitant soumis au RGPD. En ce qui concerne cet ensemble de critères de certification destiné à être utilisé comme outil au service des transferts conformément à l'article 46, paragraphe 2, point f), du RGPD, le comité a adopté l'avis 15/2026.

Évaluation

21. Le comité a procédé à son évaluation des critères de certification pour leur approbation au titre de l'article 42, paragraphe 5, du RGPD, conformément à la structure prévue à l'annexe 2 des lignes directrices (ci-après l'«annexe») et à son addendum.

22. Dans le cadre du présent avis et en vue d'approuver les critères de certification, le comité a examiné les vérifications et contrôles préliminaires relatifs à la demande et à la cible d'évaluation (A), les critères essentiels du RGPD d'Europrivacy (G), les vérifications et contrôles des mesures technologiques et organisationnelles (T), fournis en même temps que les critères de certification.

23. En outre, le comité fait remarquer, à cet égard, que les «vérifications et contrôles contextuels complémentaires»[2], transmis avec les critères de certification approuvés dans son avis précédent (version nº 60), qui visent à garantir que les opérations de traitement de données comprises dans la cible d'évaluation sont conformes aux exigences spécifiques au domaine et à la technologie[3], n'ont pas été approuvés dans son avis précédent et que ces «vérifications et contrôles contextuels complémentaires» ne figurent plus dans la documentation mise à jour fournie dans le cadre du présent avis.

24. Le comité relève que, comme précisé dans les définitions du système, les références aux «autorités compétentes en matière de protection des données» figurant dans l'ensemble du système désignent les autorités chargées de la protection des données dans l'EEE[4].

25. En ce qui concerne la définition du droit du pays tiers, le comité comprend qu'il fait référence au droit applicable au demandeur et/ou aux données à caractère personnel traitées dans la cible d'évaluation, dans la mesure où ce droit ne prévoit pas de restrictions des droits en matière de protection des données allant au-delà de ce qui est nécessaire et proportionné dans une société démocratique pour garantir l'un des objectifs visés à l'article 23, paragraphe 1, du RGPD, et dans la mesure où il est proportionné à l'objectif poursuivi,

[2] Le comité n'a pas approuvé les «vérifications et contrôles contextuels complémentaires» dans son avis précédent.
[3] Avis précédent du comité, points 7 et 8.
[4] Voir la définition proposée dans les critères Europrivacy pour l'«autorité de contrôle compétente»: «*On entend par "autorité compétente en matière de protection des données" une autorité chargée de la protection des données dans l'EEE. Dans l'ensemble, il s'agit des autorités nationales chargées de la protection des données qui sont compétentes pour faire respecter la conformité de la protection des données à caractère personnel traitées par la cible d'évaluation. Dans le cas d'une certification au titre du RGPD délivrée à un importateur de données en vertu de l'article 46 du RGPD, l'autorité compétente en matière de protection des données est celle de l'exportateur de données dans l'EEE, sauf lorsqu'il s'agit d'introduire une réclamation pour laquelle toute autorité dans l'EEE est compétente*».

respecte l'essence du droit à la protection des données et prévoit des mesures particulières pour protéger les droits fondamentaux et les intérêts des personnes concernées.

Champ d'application du mécanisme de certification et cible de l'évaluation

26. Le comité rappelle[5] que le système de certification Europrivacy est un système général en ce sens qu'il cible un large éventail d'opérations de traitement différentes effectuées par des responsables du traitement et les sous-traitants de différents secteurs d'activité.

27. Le comité salue le fait que, dans la documentation relative au champ d'application de ce système de certification qui a été transmise par l'autorité de contrôle luxembourgeoise, le système Europrivacy modifié s'applique: **i)** aux responsables du traitement et aux sous-traitants établis dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE); **ii)** aux responsables du traitement et aux sous-traitants établis en dehors de l'EEE qui sont soumis au RGPD en vertu de l'article 3, paragraphe 2, du RGPD, soit parce qu'ils proposent des biens ou des services à des personnes concernées dans l'EEE, soit parce qu'ils effectuent un suivi du comportement des personnes concernées dans l'EEE[6]. L'applicabilité des critères est définie en fonction du rôle et des responsabilités du demandeur.

28. En ce qui concerne les demandeurs visés par l'article 3, paragraphe 2, du RGPD, établis dans un pays tiers et qui ne font pas l'objet d'une décision d'adéquation englobant la cible d'évaluation, le critère A.2.1.6 précise les conditions à remplir concernant la définition de la cible d'évaluation lors de l'examen de leur demande de certification. En particulier, avant d'envisager un audit de certification, l'organisme de certification est tenu de vérifier que le demandeur est en mesure de démontrer que la législation et les pratiques nationales du pays tiers ne l'empêchent pas de respecter les exigences en matière de certification. Dans le cas contraire, la procédure de certification s'arrêtera au cours de la phase de demande.

29. Le comité note qu'un responsable du traitement des données peut soumettre à la procédure de certification Europrivacy une cible d'évaluation qui fait l'objet d'un contrôle conjoint (critère A.2.1.5). Si la cible d'évaluation fait l'objet d'un contrôle conjoint, le comité tient à souligner que l'organisme de certification agréé devra mener consciencieusement la procédure de demande afin de s'assurer que la cible d'évaluation est significative et que le demandeur assume l'entière responsabilité de la conformité de la cible d'évaluation avec toutes les obligations prévues par le RGPD que le mécanisme de certification vise à démontrer. En conséquence, l'accord conclu entre le demandeur et les autres responsables conjoints du traitement participant à la cible d'évaluation en ce qui concerne leurs responsabilités respectives en matière de respect des obligations au titre du RGPD pourrait, en fonction du contexte des activités de traitement de la cible d'évaluation, empêcher le demandeur de remplir les critères de certification.

Opérations de traitement

30. Comme indiqué par le comité dans son avis précédent, les critères portent sur les éléments pertinents des opérations de traitement (données, systèmes et traitement) en ce qui concerne le champ d'application général du mécanisme de certification. En particulier, les critères permettent de déterminer des catégories particulières de données telles que définies à l'article 9 du RGPD (section G.2 des critères relative au traitement de données particulières).

[5] Avis précédent du comité, point 6.
[6] Lignes directrices du comité sur le champ d'application territorial du RGPD (article 3), version 2.1, adoptées le 12 novembre 2019, section 2.

Licéité du traitement

31. Comme indiqué par le comité dans son avis précédent sur les critères de certification déjà approuvés (version nº 60), les critères exigent de vérifier la licéité du traitement des données pour chaque opération de traitement individuelle dans la cible d'évaluation et de vérifier les exigences d'une base juridique telle que définie à l'article 6 du RGPD (section G.1 des critères relative à la licéité du traitement des données). Le comité salue notamment le fait que, selon les critères de certification actualisés, le consentement des personnes concernées porte sur chaque finalité pour laquelle le traitement est effectué et le retrait du consentement ne doit pas porter préjudice à la personne concernée.

32. En outre, comme indiqué dans l'avis précédent du comité, les critères de certification imposent au demandeur de vérifier les exigences spécifiques aux conditions dans lesquelles, conformément à l'article 9, paragraphe 2, du RGPD, le traitement de catégories particulières de données à caractère personnel est autorisé (section G.2.1 des critères relative au traitement de données particulières) et de prévoir des limitations et des garanties supplémentaires concernant les droits et libertés de la personne concernée. Les critères de certification comportent également l'obligation de vérifier les exigences des conditions définies à l'article 10 du RGPD pour le traitement des données à caractère personnel relatives aux condamnations et aux infractions pénales (section G.2.2 des critères), le cas échéant. À cet égard, le comité salue également le fait que, selon les critères de certification actualisés (critère G.2.1.3 sur les garanties supplémentaires pour le traitement de catégories particulières de données à caractère personnel), le demandeur est tenu de mettre en place des limitations et des garanties supplémentaires, adaptées à la nature particulière des données et aux risques correspondants, lorsque des catégories particulières de données à caractère personnel font l'objet du traitement.

33. En outre, en ce qui concerne les demandeurs visés par l'article 3, paragraphe 2, du RGPD, établis dans un pays tiers et qui ne font pas l'objet d'une décision d'adéquation englobant la cible d'évaluation, les critères de certification actualisés imposent au demandeur de présenter un rapport élaboré par un expert juridique qui détermine que le droit national et les pratiques du pays tiers n'empêchent pas le respect des obligations de protection des données qui lui incombent en vertu du RGPD. Le rapport doit établir également que le droit national du pays tiers ne prévoit pas de restrictions des droits en matière de protection des données allant au-delà de ce qui est nécessaire et proportionné dans une société démocratique pour garantir l'un des objectifs visés à l'article 23, paragraphe 1, du RGPD, que ledit droit est proportionné à l'objectif poursuivi, qu'il respecte l'essence du droit à la protection des données et qu'il prévoit des mesures particulières pour protéger les droits fondamentaux et les intérêts des personnes concernées. Il convient de réexaminer ce point chaque fois que des changements de réglementation ou d'organisation sont susceptibles d'entraver le respect des critères ou d'avoir une incidence sur la cible d'évaluation ou les droits des personnes concernées, et l'organisme de certification doit en être informé (critère G.1.1.5).

34. Dans ce contexte, les critères de certification actualisés précisent dans les orientations que «lorsqu'un demandeur est établi en dehors de l'EEE et bénéficie d'une décision d'adéquation concernant le traitement effectué dans la cible d'évaluation, le respect de cette exigence peut être démontré au moyen d'un rapport simplifié». Selon ces critères, un tel rapport aurait dû évaluer si la décision d'adéquation est entrée en vigueur et justifier les raisons pour lesquelles la cible d'évaluation relève du champ d'application de la décision d'adéquation (critère G.1.1.5, lettre F).

Principes du traitement des données

35. Le comité rappelle que les critères de certification tiennent dûment compte des principes de protection des données conformément à l'article 5 du RGPD. En particulier, les critères de certification actualisés élargissent et étoffent le principe de limitation de la finalité, par l'ajout d'un critère spécial exigeant de démontrer que les données à caractère personnel ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités, que la licéité de tout traitement ultérieur est évaluée séparément et qu'une évaluation de la compatibilité de la finalité est effectuée et dûment documentée en vue du traitement ultérieur des données (critère G.1.1.6).

Obligations générales des responsables du traitement et des sous-traitants

36. Le comité rappelle que les critères de certification[7] tiennent compte des obligations incombant au responsable du traitement en vertu de l'article 24 du RGPD (section G.4 relative à la responsabilité du responsable du traitement des données) et exigent l'évaluation des accords contractuels conclus entre le sous-traitant et le responsable du traitement conformément à l'article 28 du RGPD (section G.5 des critères relative aux sous-traitants de données).

37. En outre, le comité salue le fait que les critères de certification imposent désormais au demandeur visé par l'article 3, paragraphe 2, du RGPD, de désigner un bureau ou un représentant dans l'EEE conformément à l'article 27 du RGPD, dont les coordonnées sont indiquées sur le site web du demandeur (critère G.4.1.4). Le comité prend note de ces critères de certification et rappelle qu'il ne s'agit pas toujours d'une obligation pour les responsables du traitement et les sous-traitants en vertu du RGPD, de sorte qu'il convient de garder à l'esprit les conditions prévues à l'article 27 du RGPD.

38. En outre, le comité note, comme indiqué dans son avis précédent, que les critères de certification imposent à tous les demandeurs de désigner un délégué à la protection des données (DPD), même dans le cas où le demandeur n'est pas tenu de le faire en vertu de l'article 37 du RGPD. Les critères permettent de vérifier que le DPD satisfait aux exigences visées aux articles 37 à 39 (section G.9 des critères, relative au délégué à la protection des données).

39. De même, les critères de certification imposent de vérifier le contenu des registres des activités de traitement, conformément à l'article 30 du RGPD (section G.5.3 des critères, relative aux registres des activités de traitement). À cet égard, le comité salue le fait qu'en vertu des critères de certification actualisés, les demandeurs visés à l'article 3, paragraphe 2, du RGPD sont tenus de coopérer en cas de demande formulée par les autorités de protection des données compétentes dans l'EEE et de mettre à la disposition de celles-ci, sur demande, le registre des activités de traitement (critère G.5.3.5).

40. Dans le même ordre d'idées, le comité note que certains critères de certification supplémentaires ont été ajoutés en ce qui concerne le recrutement de sous-traitants ultérieurs par les demandeurs agissant en qualité de responsables du traitement ou de sous-traitants (section G.5.1.2 relative au recrutement de sous-traitants ultérieurs). Cette distinction permet de mieux tenir compte de la séparation des rôles et des responsabilités entre les acteurs de la chaîne de traitement.

[7] Avis précédent du comité, point 15.

Droits des personnes concernées

41. Comme dans son avis précédent, le comité rappelle que les critères de certification tiennent dûment compte du droit de la personne concernée d'être informée conformément au chapitre III du RGPD et exigent la mise en place de mesures correspondantes[8]. Les critères de certification demandent également la mise en place de mesures prévoyant la possibilité d'intervenir dans le traitement afin de garantir les droits des personnes concernées et notamment les droits à la rectification, à l'effacement ou à la limitation (section G.3 des critères relative aux droits des personnes concernées).

42. En outre, le comité salue les améliorations apportées aux critères de certification en ce qui concerne les informations à communiquer aux personnes concernées (section G 3.2 relative aux informations à communiquer lorsque des données à caractère personnel sont collectées auprès de la personne concernée et section G.3.3 relative aux informations à communiquer lorsque des données à caractère personnel ne sont pas collectées auprès de la personne concernée), les modalités de communication avec les personnes concernées[9] et les modalités d'exercice des droits des personnes concernées[10] (section G 3.1 relative à des informations transparentes, à la communication et aux modalités d'exercice des droits des personnes concernées), ainsi que le droit d'accès (section G 3.4 relative au droit d'accès de la personne concernée), le droit à l'effacement [section G.3.6 relative au droit à l'effacement («droit à l'oubli»)], le droit à la limitation du traitement (critère G 3.7.1 relatif au droit à la limitation du traitement), l'obligation de notification concernant la rectification ou l'effacement des données à caractère personnel ou la limitation de leur traitement (critère G.3.8.2 relatif au devoir d'informer les personnes concernées sur les destinataires si elles le demandent), le droit d'opposition (section G.3.10 relative au droit d'opposition) et le droit de ne pas faire l'objet d'une décision individuelle automatisée, y compris le profilage (section G.3.11 relative au droit de ne pas faire l'objet d'une décision individuelle automatisée, y compris le profilage).

Risques pour les droits et la liberté

43. Le comité a déjà indiqué dans son avis précédent que les critères de certification exigent d'évaluer le risque pour les droits et libertés des personnes physiques lié au traitement des données compris dans la cible d'évaluation conformément à l'article 35 du RGPD (section G.8 des critères relative à l'obligation d'évaluer si une analyse d'impact relative à la protection des données est nécessaire)[11].

44. Le comité salue les modifications apportées aux critères de certification, qui prévoient désormais que «le demandeur devra évaluer, au moyen d'une méthode répétable, les risques présentés par le traitement, qui peuvent avoir une incidence sur les droits et libertés des personnes physiques» (section G.6.2.4 relative à l'évaluation des risques du traitement des données).

[8] Avis précédent du comité, point 19.
[9] À titre d'exemple, le critère G.3.1.1 relatif à l'obligation d'informer la personne concernée dans un langage clair détaille les informations sur le traitement des données que doit communiquer le demandeur à la personne concernée, et ces informations doivent désormais i) être communiquées par écrit ou par d'autres moyens, ii) être disponibles dans la ou les langues officielles du demandeur et iii) être disponibles dans la langue des personnes concernées ciblées.
[10] À titre d'exemple, le critère G 3.1.3 relatif à une gestion et à un enregistrement appropriés des droits des personnes concernées impose désormais au demandeur de disposer d'une procédure ou d'un mécanisme permettant de confirmer la réception de la demande à la personne concernée et de tenir un registre des demandes des personnes concernées dans lequel figure la date de réception.
[11] Avis précédent du comité, point 20.

45. En outre, le comité salue les nouveaux ajouts et détails introduits par les critères de certification. À titre d'exemple, le comité prend note de l'ajout apporté à l'analyse d'impact relative à la protection des données, en ce qui concerne les situations dans lesquelles le demandeur n'est pas tenu de réaliser une telle analyse (section G.8.2.1 sur les exigences concernant l'analyse d'impact relative à la protection des données).

Mesures techniques et organisationnelles qui garantissent la protection

46. Comme indiqué dans l'avis précédent du comité, les critères de certification exigent l'application de mesures techniques et organisationnelles garantissant la confidentialité, l'intégrité et la disponibilité des opérations de traitement. Les critères exigent également l'application de mesures techniques pour mettre en œuvre la protection des données dès la conception et par défaut conformément à l'article 25 et à l'article 32 du RGPD (section G.6 des critères relative à la protection des données dès la conception et par défaut et à la sécurité du traitement, section G.6.2 des critères relative à la sécurité du traitement et section sur les critères T)[12]. À cet égard, le comité salue le fait que les critères de certification modifiés précisent davantage (section G.6.1.2 relative à la minimisation des données par défaut) les règles et procédures que le demandeur doit appliquer pour se conformer à ces critères.

47. Comme souligné dans l'avis précédent du comité, les critères de certification exigent l'application de mesures destinées à garantir que les obligations en matière de notification d'une violation de données à caractère personnel sont exécutées dans les meilleurs délais et dans les limites prévues, conformément aux articles 33 et 34 du RGPD (section G.7 des critères relative à la gestion des violations de données).

48. À cet égard, le comité note que les critères de certification ont été améliorés et étoffés. Plus précisément, les critères de certification comprennent désormais une liste plus détaillée (section G.7.1.1. relative à l'obligation de documenter les violations de données) des informations que le demandeur doit consigner en cas de violation de données (par exemple, les catégories de données à caractère personnel concernées ou susceptibles de l'être, le nombre approximatif de personnes concernées par la violation ou susceptibles de l'être, les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ou susceptibles de l'être, les conséquences probables de la violation de données à caractère personnel).

Critères aux fins de démontrer l'existence de garanties appropriées pour le transfert de données à caractère personnel

49. Comme le comité l'a affirmé dans son avis précédent, les critères de certification exigent d'identifier tous les transferts de données à caractère personnel vers des pays tiers et à des organisations internationales faisant partie de la cible d'évaluation et de justifier le choix effectué en ce qui concerne le mécanisme de transfert de données prévoyant des garanties appropriées, conformément au chapitre V du RGPD (section G.10 – transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales).

[12] Avis précédent du comité, point 21.

50. Le comité reconnaît que, pour les demandeurs visés par l'article 3, paragraphe 2, du RGPD, ces critères de certification s'appliqueront en cas de transferts de données à caractère personnel comprises dans la cible d'évaluation vers des entités établies tant dans le même pays tiers que celui dans lequel le demandeur se trouve que dans un autre pays tiers.

51. En outre, le comité salue le fait que les critères de certification concernant les transferts de données à caractère personnel aient été étoffés et qu'ils indiquent plus clairement les obligations du demandeur en la matière (section G.10.1 relative aux obligations générales pour les transferts internationaux de données à caractère personnel vers des pays tiers ou à des organisations internationales).

Critères supplémentaires pour un label européen de protection des données

52. Selon les lignes directrices, l'évaluation doit inclure la question de savoir «si les critères peuvent tenir compte de la législation ou des scénarios en matière de protection des données des États membres». Comme indiqué par le comité dans son avis précédent, la section G.1.1.3 des critères de certification exige du demandeur qu'il fournisse une telle évaluation dans un rapport d'évaluation du respect des obligations nationales. Ce rapport comprendra une évaluation des obligations nationales applicables à la cible d'évaluation et documentera les mesures prises par le demandeur pour se conformer aux règles applicables et, éventuellement, les mesures correctrices en cours. Le demandeur n'utilisera pas la liste des principales exigences nationales complémentaires fournie par le propriétaire du système pour chaque pays comme une liste exhaustive des obligations nationales pertinentes pour la cible d'évaluation. La liste indicative des exigences minimales en matière de vérifications et de contrôles complémentaires fournie par le propriétaire du système ne constitue pas un critère de certification dans le cadre du présent avis.

53. Le comité salue les ajustements apportés au rapport d'évaluation du respect des obligations nationales dans les critères actualisés (section G.1.1.3 relative à l'évaluation du respect des obligations nationales). En particulier, il est désormais précisé que le demandeur doit documenter, dans un rapport d'évaluation du respect des obligations nationales, l'évaluation faite de la conformité du traitement des données «*avec les obligations nationales complémentaires de l'EEE en matière de protection des données à caractère personnel applicables au demandeur*». En particulier, le rapport d'évaluation du respect des obligations nationales doit comprendre, entre autres, une définition claire de la cible d'évaluation qui a été évaluée, la liste des obligations nationales complémentaires de l'EEE en matière de protection des données applicables à la cible d'évaluation, ainsi que l'évaluation de la conformité de la cible d'évaluation avec lesdites obligations. Le comité considère que si le demandeur est établi en dehors de l'EEE et est soumis à l'article 3, paragraphe 2, du RGPD, les obligations nationales de l'EEE en matière de protection des données applicables à la cible d'évaluation doivent être déterminées en fonction de l'endroit où se trouvent les personnes concernées auxquelles le demandeur propose des biens ou des services ou dont le comportement fait l'objet d'un suivi.

Conclusions/recommandations

54. Pour conclure, le comité considère que les critères de certification Europrivacy sont conformes au RGPD et les approuve conformément à la mission du comité définie à l'article 70, paragraphe 1, point o), du RGPD, ce qui donne lieu à une certification commune (label européen de protection des données).

55. Le comité considère que les critères de certification font partie intégrante du système de certification et consignera le système de certification Europrivacy dans le registre public des mécanismes de certification et les labels et marques en matière de protection des données, et mettra les critères à la disposition du public conformément à l'article 42, paragraphe 8, du RGPD.

Observations finales

56. Le présent avis est adressé à l'autorité de contrôle luxembourgeoise et sera publié conformément à l'article 64, paragraphe 5, point b), du RGPD.

Pour le comité européen de la protection des données

La présidente

Anu Talus