Avis du comité (article 64)

Avis 19/2024 sur les critères de certification EuroPrise en ce qui concerne leur approbation par le comité en tant que label européen de protection des données conformément à l'article 42, paragraphe 5 (RGPD)

Adopté le 16 juillet 2024

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Contenu

1. RÉSUMÉ DES FAITS 6
2. APPRÉCIATION 6
2.1 Champ d'application du mécanisme de certification et cible d'évaluation 6
2.2 Opérations de transformation 7
2.3 Licéité et principes du traitement des données 7
2.4 Obligations générales des responsables du traitement et des sous-traitants 7
2.5 Droits des personnes concernées 8
2.6 Risques pour les droits et la liberté 8
2.7 Mesures techniques et organisationnelles garantissant la protection 8
2.8 Critères aux fins de démontrer l'existence de garanties appropriées pour le transfert de données à caractère personnel 8
3. CRITÈRES SUPPLÉMENTAIRES POUR UN LABEL EUROPÉEN DE PROTECTION DES DONNÉES 8
CONCLUSIONS/RECOMMANDATIONS 9
OBSERVATIONS FINALES 9

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,

(1) Les États membres, les autorités de contrôle, le comité européen de la protection des données (ci-après le «comité européen de la protection des données» 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») ainsi que de labels et de marques en la matière, aux fins 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[2]. En outre, la mise en place de mécanismes de certification peut favoriser la transparence et permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question[3].

(2) Les critères de certification font partie intégrante d'un mécanisme de certification. Par conséquent, le RGPD exige que les critères d'un mécanisme national de certification soient approuvés 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 le comité européen de la protection des données [article 42, paragraphe 5 et article 70, paragraphe 1, point o) du RGPD].

(3) Lorsqu'une autorité de contrôle (ci-après, «AC») a l'intention de soumettre à l'approbation du comité européen de la protection des données 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 proposer le mécanisme de certification dans tous les États membres. Dans ce cas, le rôle principal du comité 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, le comité européen de la protection des données approuve les critères de certification.

(4) Le présent avis vise à garantir l'application cohérente du RGPD, y compris par les autorités de contrôle, les responsables du traitement et les sous-traitants à la lumière des éléments essentiels que doivent contenir les mécanismes de certification. En particulier, l'évaluation du comité européen de la protection des données est effectuée sur la base des «lignes directrices 1/2018 relatives à la

[1] Dans le présent avis, on entend par «États membres» les «États membres de l'EEE».
[2] Article 42, paragraphe 1, du RGPD.
[3] Considérant 100 du RGPD.

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 contenant des «orientations sur l'évaluation des critères de certification» (ci-après l'«addendum»), pour lequel la période de consultation publique a expiré le 26 mai 2021.

(5) En conséquence, 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.

(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 son application cohérente.

(7) Par ailleurs, le propriétaire du système 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 constituent des outils pratiques et ont potentiellement un bon rapport coût-efficacité, afin d'assurer une plus grande cohérence avec le RGPD et de promouvoir 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 plus particulièrement sur les critères de certification. Si le comité a 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, ce dernier n'emporte aucunement approbation desdites méthodes d'évaluation.

(13) L'avis du comité 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 la présidente et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision de la présidente, 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:

1. RÉSUMÉ DES FAITS

1. Conformément à l'article 42, paragraphe 5, du RGPD et aux lignes directrices, le projet de «Catalogue de critères EuroPriSe pour la certification d'opérations de traitement par des sous-traitants» (champ d'application: EU) v1.5» (ci-après le «projet de critères de certification», les «critères de certification» ou les «critères») a été rédigé par EuroPriSe Cert GmbH (ci-après le «propriétaire du système»), une entité juridique établie en Allemagne, et soumis à la Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, l'autorité de contrôle allemande compétente en Rhénanie-du-Nord-Westphalie (ci-après la «DE-NRW SA»).

2. Le 29 avril 2024, l'autorité de contrôle allemande (ci-après l'«AC DE») a soumis le projet de critères de certification au CEPD pour approbation conformément à l'article 64, paragraphe 2, du RGPD. La décision relative au caractère complet du dossier a été prise le 29 mai 2024.

3. Le mécanisme de certification EuroPrise n'est pas une certification au sens de l'article 46, paragraphe 2, point f), du RGPD, destinée aux transferts internationaux de données à caractère personnel et ne fournit donc pas de garanties appropriées dans le cadre des transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales dans les conditions visées à l'article 46, paragraphe 2, point f). En effet, tout transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si les dispositions du chapitre V du RGPD sont respectées.

2. APPRÉCIATION

4. Le comité européen de la protection des données a procédé à son évaluation des critères de certification en vue de 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.

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

5. Le mécanisme de certification EuroPrise contient les critères de certification d'un système de certification à l'échelle de l'UE destiné à la certification d'opérations de traitement par des sous-traitants. Les certifications auxquelles s'applique le catalogue de critères concernent des opérations de traitement effectuées dans des produits, processus et services ou à l'aide de produits et services (y compris plusieurs d'entre eux) et à l'égard desquels le demandeur de certification agit en tant que sous-traitant. Les principaux critères de ce mécanisme de certification sont divisés en trois ensembles d'exigences, à savoir: du point de vue juridique (ensemble 1), du point de vue des mesures techniques et organisationnelles (ensemble 2) et du point de vue des droits des personnes concernées (ensemble 3).

6. Les demandeurs de certification dans le cadre de ce système doivent être des sous-traitants. Cela inclut les sous-traitants qui sont directement chargés du traitement des données à caractère personnel par un responsable du traitement au sens de l'article 4, paragraphe 7, du RGPD. Toutefois, les demandeurs de certification peuvent également être des sous-traitants au sens de l'article 28, paragraphes 2 et 4, du RGPD (sous-traitants secondaires).

7. Lorsqu'un sous-traitant - certifié dans le cadre du système de certification EuroPrise - a recours à un sous-traitant secondaire, ce dernier ne peut pas prétendre qu'il a été certifié dans le cadre du système

de certification EuroPrise. Dans ce cas, seules les opérations de traitement effectuées par le sous-traitant initial et certifié sont couvertes par la certification. Toutefois, les sous-traitants peuvent également demander une certification, ce qui donnerait lieu à une procédure autonome et indépendante.

8. Le comité relève, dans la documentation relative au champ d'application du mécanisme de certification fournie par l'autorité de contrôle allemande, que le système EuroPrise s'applique aux sous-traitants établis dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE).

2.2 Opérations de transformation

9. Le champ d'application de ces critères ne se limite pas à certains types d'opérations de traitement. Il s'agit plutôt de la méthodologie sous-jacente à une évaluation EuroPrise, qui permet la certification de toute opération de traitement par des sous-traitants. Il s'agit donc d'une approche méthodologique universelle sur la base de laquelle un grand nombre d'opérations de traitement, de nature très différente, peuvent être certifiées. Par conséquent, il est fondamental que les exigences méthodologiques soient respectées, car il s'agit du seul moyen de garantir l'application uniforme des critères de certification et un niveau comparable de test dans les différentes procédures de certification. L'objectif est de garantir la comparabilité et la reproductibilité des certifications délivrées et de leurs résultats.

2.3 Licéité et principes du traitement des données

10. Les critères exigent d'examiner si les opérations de traitement à certifier sont conformes aux principes de protection des données dès la conception et de protection des données par défaut (section 1.5 des critères), ce qui implique la participation du demandeur à l'assistance fournie au responsable du traitement dans la mise en œuvre de ces principes. Cela permet d'évaluer le respect de l'article 25 du RGPD, lu conjointement avec l'article 5 du RGPD. Bien qu'aucun critère ne vise directement le respect de l'article 6 du RGPD - étant donné que le responsable du traitement est responsable de la licéité du traitement - les critères visent à garantir que les sous-traitants-demandeurs conçoivent les opérations de traitement à certifier de manière à faciliter la mise en œuvre par les responsables du traitement des principes de protection des données de l'article 5 du GDPR, y compris le principe de licéité du traitement.

2.4 Obligations générales des responsables du traitement et des sous-traitants

11. Les critères reflètent la relation entre le sous-traitant et le responsable du traitement. En particulier, les critères prévoient l'obligation pour le sous-traitant de mettre en place un modèle d'accord de traitement des données avec le responsable du traitement, qui inclut toutes les exigences de l'article 28 du GDPR (section 1.2 des critères).

12. Les critères imposent aux demandeurs de nommer un délégué à la protection des données (DPD) conformément à l'article 37 du RGPD, et de fournir la preuve de la nomination du DPD (p. ex. un certificat de nomination). Les critères permettent de vérifier que le DPD satisfait aux exigences visées aux articles 37 à 39 (ensemble 1, section 1.1 des critères).

13. Les critères permettent de vérifier le contenu des registres de traitement des activités conformément à l'article 30 du RGPD (ensemble 1, section 1.1 des critères).

2.5 Droits des personnes concernées

14. Les critères 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. Les critères exigent 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 (ensemble 3 des critères).

2.6 Risques pour les droits et la liberté

15. Les critères exigent que le sous-traitant soit conscient des risques potentiels pour les droits et libertés des personnes physiques en ce qui concerne le traitement de données faisant partie de la cible d'évaluation. Si le traitement de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, plusieurs critères garantissent que le demandeur démontre que les exigences de l'article 35 du RGPD sont remplies conformément à l'article 35 du RGPD (section 1.2.2 des critères, exigence nº 6, section 1.3.2 des critères, section 1.3.3 des critères, section 2.1.5.1 des critères, section 2.1.5.9 des critères).

2.7 Mesures techniques et organisationnelles garantissant la protection

16. Les critères 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 aux articles 25 et 32 du RGPD (section 1.5 des critères, section 2.1 des critères/autres documents).

17. Les critères 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 1.2.2. des critères, exigence nº 6).

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

18. Les critères 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 1.4 des critères).

3. CRITÈRES SUPPLÉMENTAIRES POUR UN LABEL EUROPÉEN DE PROTECTION DES DONNÉES

19. 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». La section 4 des critères exige que le demandeur se conforme à la législation nationale applicable et à la législation sectorielle pertinente en matière de protection des données. En outre, le comité comprend qu'un «rapport de conformité au droit national» - évaluant en particulier la conformité de la cible d'évaluation avec les exigences du droit national applicable en matière de protection des

données - doit être établi par des experts juridiques, à condition que ces experts aient fait la preuve de leur niveau d'expertise nécessaire en ce qui concerne le droit national applicable.

CONCLUSIONS/RECOMMANDATIONS

20. Pour conclure, le comité européen de la protection des données considère que les critères de certification 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).

21. Le comité européen de la protection des données consignera le mécanisme de certification «Catalogue de critères EuroPriSe pour la certification d'opérations de traitement par des sous-traitants» dans le registre public des mécanismes de certification et des labels et marques en matière de protection des données conformément à l'article 42, paragraphe 8.

OBSERVATIONS FINALES

22. Le présent avis est adressé à l'autorité de contrôle allemande de Rhénanie-du-Nord-Westphalie et il 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