Avis 28/2022 sur les critères de certification Europrivacy 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 10 octobre 2022

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 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, l'autorité de contrôle 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 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 certification et à la définition des critères de certification conformément aux articles 42 et 43 du

[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.

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 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 de certification 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:

RÉSUMÉ DES FAITS

1. Conformément à l'article 42, paragraphe 5, du RGPD et aux lignes directrices, les critères Europrivacy v.60 (ci-après le «projet de critères de certification», les «critères de certification» ou les «critères») ont été élaborés par le Centre européen de certification et de protection de la vie privée (ci-après le «propriétaire du système»).

2. Le 28 septembre 2022, 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 pour approbation conformément à l'article 64, paragraphe 2, du RGPD. La décision relative au caractère complet du dossier a été rendue le 28 septembre 2022.

3. Le mécanisme de certification Europrivacy 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 ÉVALUATION

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.

5. Le comité note que les orientations de mise en œuvre et les moyens proposés pour vérifier le mécanisme de certification fournis par le propriétaire du système ne sont pas toujours cohérents dans l'ensemble du catalogue de critères. À titre d'exemple, la section T.2.3.2 exige que des règles, des politiques, des procédures ou des mécanismes soient en place pour détecter et signaler les intrusions (par exemple, un système de détection des intrusions qui surveille le trafic sur le réseau en vue de détecter des activités suspectes et qui émet une alerte lorsqu'une telle activité est découverte), tandis que les moyens de vérification proposés font référence à l'inspection et au test d'intrusion (requis à la section T.2.3.1). Bien que ces incohérences ne relèvent pas du champ d'application de son évaluation, le comité souligne qu'elles peuvent constituer un obstacle à l'agrément de l'organisme de certification, à moins qu'elles ne soient rectifiées par le propriétaire du système.

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

6. Le mécanisme de certification Europrivacy est un système général en ce sens qu'il cible un large éventail d'opérations de traitement différentes effectuées par les responsables du traitement et les sous-traitants de différents secteurs d'activité. Les principaux critères de ce mécanisme de certification se composent des «critères essentiels» et des «vérifications et contrôles des MTO» concernant les mesures technologiques et organisationnelles mises en place pour sécuriser les données à caractère personnel traitées. Un ensemble de critères relatifs aux «vérifications et

contrôles des MTO» ne s'applique que si la cible d'évaluation traite des catégories particulières de données, des données relatives à des infractions pénales ou des données à caractère personnel relatives à un enfant.

7. En outre, les critères comprennent des « vérifications et contrôles contextuels complémentaires», 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. Une matrice d'information fournie par le propriétaire du système décrit à quelles catégories d'opérations de traitement de données s'applique chaque ensemble de critères relatifs aux « vérifications et contrôles contextuels complémentaires».

8. Le comité se félicite des systèmes généraux qui incluent des critères spécifiques afin de les rendre modulables et applicables à des opérations de traitement ou à un secteur d'activité spécifiques. Toutefois, le comité souhaite également préciser que, dans le cadre d'un système général, le caractère exhaustif des critères relatifs à des opérations de traitement spécifiques n'est pas requis et n'a donc pas été évalué dans le cadre du présent avis. En outre, le comité rappelle que, lorsqu'il publie des documents relatifs à des activités de traitement spécifiques, ces documents sont à prendre en considération par le propriétaire du système et les organismes de certification agréés.

9. Les critères applicables à la spécification de la cible d'évaluation sont définis dans les exigences disponibles au point A.2.1.1. Les règles spécifiques applicables à la procédure à suivre par le demandeur et par l'organisme de certification pour définir la cible d'évaluation sont précisées par le système Europrivacy (10.2 - activités de pré-certification).

10. Le comité note dans la documentation relative au champ d'application du mécanisme de certification fournie par l'autorité de contrôle luxembourgeoise que le système Europrivacy s'applique aux responsables du traitement et aux sous-traitants établis dans l'Union européenne (UE) ou dans l'Espace économique européen (EEE). L'applicabilité des critères est définie en fonction du rôle et des responsabilités du demandeur.

11. Le comité note qu'un responsable du traitement peut soumettre à la procédure de certification Europrivacy une cible d'évaluation qui fait l'objet d'un contrôle conjoint (critère A.2.7.1). 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[4] pourrait, en fonction du contexte des activités de traitement de la cible d'évaluation, empêcher le demandeur de remplir les critères de certification.

[4] *La détermination de leurs responsabilités respectives doit notamment porter sur l'exercice des droits des personnes concernées et l'obligation d'information. En outre, la répartition des responsabilités devrait couvrir d'autres obligations incombant au responsable du traitement, notamment en ce qui concerne les principes généraux de la protection des données, la base juridique, les mesures de sécurité, l'obligation de notification des violations de données, les analyses d'impact relatives à la protection des données, le recours à des sous-traitants, les transferts vers des pays tiers et les contacts avec les personnes concernées et les autorités de contrôle* (lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD)

12. Le comité note que le traitement de données génétiques est exclu du champ d'application du mécanisme de certification Europrivacy. Par conséquent, l'évaluation des critères effectuée par le comité ne porte pas sur le caractère approprié des critères pour la cible d'évaluation qui inclurait un tel traitement de données.

2.2 Opérations de traitement

13. 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. Notamment, les critères permettent d'identifier des catégories particulières de données telles que définies à l'article 9 du RGPD (section G.2 des critères - traitement de données particulières).

2.3 Licéité du traitement

14. 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 - licéité du traitement des données).

2.4 Principes du traitement des données

15. Les critères tiennent dûment compte des principes de protection des données conformément à l'article 5 du RGPD. En particulier, les critères exigent du demandeur qu'il démontre que les données à caractère personnel sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).

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

16. Les critères tiennent compte des obligations incombant au responsable du traitement en vertu de l'article 24 du RGPD (G.4 - 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 - sous-traitants de données).

17. Les critères exigent de 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 désigner un DPD conformément à 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 - délégué à la protection des données).

18. Les critères permettent de vérifier le contenu des registres des activités de traitement conformément à l'article 30 du RGPD (section G.5.3 des critères - registre des activités de traitement).

2.6 Droits des personnes concernées

19. 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 (section G.3 des critères - droits des personnes concernées).

2.7 Risques pour les droits et la liberté

20. Les critères 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 - analyse d'impact relative à la protection des données).

2.8 Mesures techniques et organisationnelles garantissant la protection

21. 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 à l'article 25 et à l'article 32 du RGPD (section G.6 des critères - sécurité du traitement et protection des données dès la conception, section T.1/T.2 des critères - exigences essentielles de sécurité/exigences de sécurité étendues).

22. 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 G.7 des critères - gestion des violations de données).

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

23. 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 G.10 des critères - transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales).

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

24. 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 G.1.1.3 des critères exige du demandeur qu'il fournisse une telle évaluation dans un rapport d'évaluation du respect des obligations nationales. Le comité note que 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.

CONCLUSIONS/RECOMMANDATIONS

25. Pour conclure, le comité européen de la protection des données 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).

26. Le comité européen de la protection des données consignera le mécanisme de certification Europrivacy dans le registre public des mécanismes de certification et les labels et marques en matière de protection des données conformément à l'article 42, paragraphe 8.

OBSERVATIONS FINALES

27. 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