Lignes directrices 07/2022 sur la certification en tant qu'outil au service des transferts

Version 2.0

Adoptées le 14 février 2023

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

HISTORIQUE DES VERSIONS

Version 1.0	14 juin 2022	Adoption des lignes directrices pour consultation publique
Version 2.0	14 février 2023	Adoption des lignes directrices après la consultation publique

RÉSUMÉ

L'article 46 du RGPD exige que les responsables du traitement/sous-traitants mettent en place des garanties appropriées pour les transferts de données à caractère personnel vers des pays tiers ou des organisations internationales. À cette fin, le RGPD diversifie les garanties appropriées qui peuvent être utilisées par les organisations au titre de l'article 46 pour encadrer les transferts vers des pays tiers en introduisant, entre autres, la certification en tant que nouveau mécanisme de transfert [article 42, paragraphe 2, et article 46, paragraphe 2, point f), du RGPD)].

Les présentes lignes directrices fournissent des orientations sur l'application de l'article 46, paragraphe 2, point f), du RGPD relatif aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales sur la base d'une certification. Le document est structuré en quatre sections avec une annexe.

La première partie du présent document («CONSIDÉRATIONS GÉNÉRALES») précise que les lignes directrices complètent les lignes directrices 1/2018 déjà existantes relatives à la certification et répondent aux exigences spécifiques du chapitre V du RGPD lorsque la certification est utilisée comme outil de transfert. Conformément à l'article 44 du RGPD, tout transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales doit remplir les conditions des autres dispositions du RGPD en plus de se conformer au chapitre V du RGPD. Par conséquent, dans un premier temps, le respect des dispositions générales du RGPD doit être assuré et, dans un second temps, les dispositions du chapitre V du RGPD doivent être respectées. Les acteurs concernés et leurs rôles essentiels dans ce contexte sont décrits, en accordant une attention particulière au rôle de l'importateur de données qui recevra une certification et de l'exportateur de données qui l'utilisera comme un outil pour encadrer ses transferts (étant donné que la responsabilité de la conformité du traitement des données incombe à l'exportateur de données). Dans ce contexte, la certification peut également inclure des mesures qui complètent les outils de transfert afin de garantir le respect du niveau de protection des données à caractère personnel de l'UE. La première partie des lignes directrices contient également des informations sur le processus d'obtention d'une certification à utiliser comme outil pour les transferts.

La deuxième partie des présentes lignes directrices («MISE EN ŒUVRE DES ORIENTATIONS SUR LES EXIGENCES EN MATIÈRE D'AGRÉMENT») rappelle que les exigences relatives à l'agrément d'un organisme de certification figurent dans la norme ISO 17065 et en interprétant les lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du RGPD et de son annexe dans le contexte du chapitre V. Toutefois, dans le contexte d'un transfert, les présentes lignes directrices expliquent plus en détail certaines des exigences en matière d'agrément applicables à l'organisme de certification.

La troisième partie des présentes lignes directrices («CRITÈRES DE CERTIFICATION SPÉCIFIQUES») fournit des orientations sur les critères de certification déjà énumérés dans les lignes directrices 1/2018 et établit des critères spécifiques supplémentaires qui devraient être inclus dans un mécanisme de certification à utiliser comme outil pour les transferts vers des pays tiers. Ces critères couvrent l'évaluation de la législation du pays tiers, les obligations générales des exportateurs et des importateurs, les règles relatives aux transferts ultérieurs, aux voies de recours et à l'exécution, aux procédures et aux actions dans les situations dans lesquelles la législation et les pratiques nationales empêchent le respect des engagements pris dans le cadre de la certification et les demandes d'accès aux données par les autorités de pays tiers.

La quatrième partie des présentes lignes directrices («ENGAGEMENTS CONTRAIGNANTS ET EXÉCUTOIRES À METTRE EN ŒUVRE») contient des éléments qui devraient être pris en compte dans les engagements contraignants et exécutoires que les responsables du traitement ou les sous-traitants qui ne sont pas soumis au RGPD devraient prendre afin de fournir des garanties appropriées aux données transférées vers des pays tiers. Ces engagements, qui peuvent être énoncés dans différents instruments, y compris des contrats, incluent notamment une garantie que l'importateur n'a aucune raison de croire que les lois et pratiques du pays tiers applicables au traitement en question, y compris toute obligation de divulguer des données à caractère personnel ou toute mesure autorisant l'accès des autorités publiques, l'empêchent de respecter ses engagements au titre de la certification.

L'ANNEXE des présentes lignes directrices contient quelques exemples de mesures supplémentaires conformes à celles énumérées à l'annexe II des recommandations 01/2020 (recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE) dans le contexte de l'utilisation d'une certification comme outil au service des transferts. Des exemples sont donnés en vue d'attirer l'attention sur les situations critiques.

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 notamment 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 12 et 22 de son règlement intérieur,

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES:

1 CONSIDÉRATIONS GÉNÉRALES

1.1 Objet et champ d'application

1. Le présent document vise à fournir des orientations sur l'application de l'article 46, paragraphe 2, point f), du RGPD relatif aux transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales sur la base d'une certification. Le comité européen de la protection des données a déjà publié des orientations générales sur la certification[2] et l'accréditation[3] au titre du RGPD. Ces nouvelles lignes directrices ne reflètent donc que les aspects spécifiques de la certification en tant qu'outil au service des transferts. Elles précisent l'application de l'article 46, paragraphe 2, point f) et de l'article 42, paragraphe 2, du RGPD en fournissant des orientations pratiques à cet égard et en introduisant de nouveaux éléments dans les lignes directrices déjà publiées.

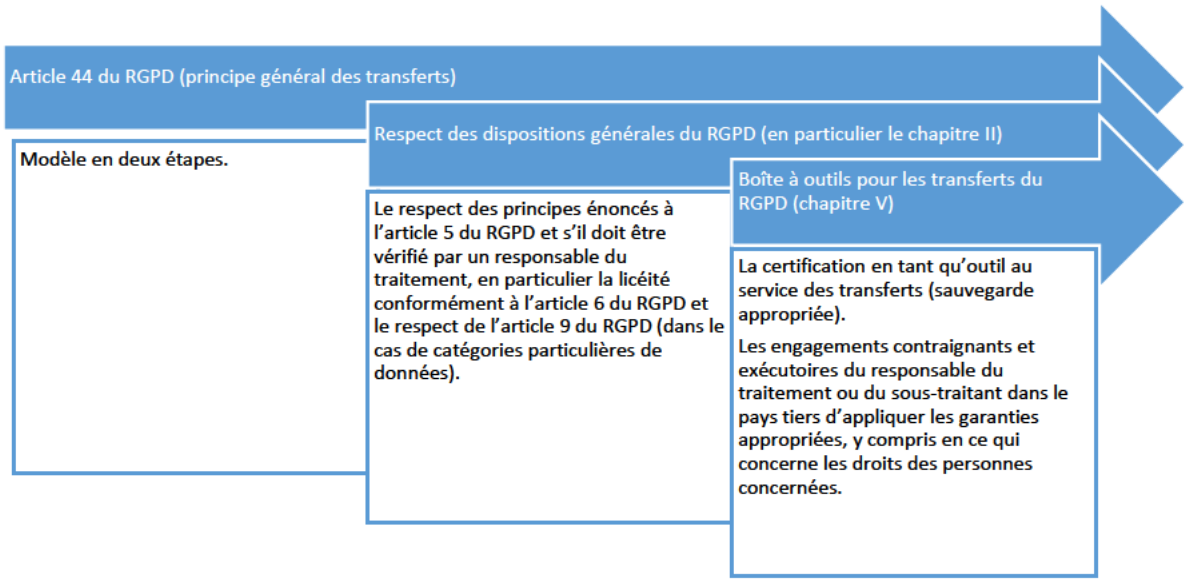
2. L'EDPB évaluera le fonctionnement des présentes lignes directrices à la lumière de l'expérience acquise dans le cadre de leur application pratique et fournira des orientations supplémentaires pour clarifier l'application des éléments énumérés ci-dessous, y compris le rôle de l'accord de certification en ce qui concerne les engagements contraignants et exécutoires visés à l'article 46, paragraphe 2, point f), du RGPD.

1.2 Règles générales applicables aux transferts internationaux

3. Conformément à l'article 44 du RGPD, tout transfert de données à caractère personnel vers des pays tiers[4] ou des organisations internationales doit remplir les conditions des autres dispositions du RGPD en plus de se conformer au chapitre V du RGPD. Par conséquent, chaque transfert doit notamment respecter les principes de protection des données définis à l'article 5 du RGPD, être licite en vertu de l'article 6 du RGPD et être conforme à l'article 9 du RGPD en cas de catégories particulières de données. La vérification se fait donc en deux étapes: dans un premier temps, il faut veiller au respect des

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
[2] Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement (UE) 2016/679
[3] Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données (2016/679)
[4] Lignes directrices 05/2021 sur l'interaction entre l'application de l'article 3 et les dispositions relatives aux transferts internationaux conformément au chapitre V du RGPD, p. 4.

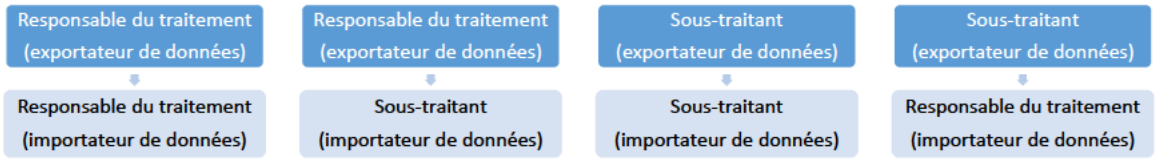
dispositions générales du RGPD, et, dans un second temps, à celui des dispositions du chapitre V du RGPD.



4. En son article 46, le RGPD dispose qu'«[e]n l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives». Conformément à l'article 46, paragraphe 2, point f), du RGPD, ces garanties appropriées peuvent être prévues par un mécanisme de certification approuvé ainsi que par les engagements contraignants et exécutoires du responsable du traitement ou du sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

5. En conséquence, l'exportateur de données peut décider de se fonder sur la certification obtenue par un importateur de données pour démontrer le respect de ses obligations, par exemple en vertu de l'article 24, paragraphe 3, ou de l'article 28, paragraphe 5, du RGPD. L'importateur de données peut décider de demander la certification afin de démontrer que des garanties appropriées sont en place.

6. Tant l'exportateur de données que l'importateur de données peuvent remplir différents rôles (par exemple en tant que responsable du traitement ou sous-traitant[5]), en fonction du traitement au titre du chapitre V, ce qui entraîne des responsabilités différentes:



7. Outre le recours à la certification ou à l'un des autres outils ou mécanismes de transfert visés aux articles 45 et 46, l'article 49 du RGPD dispose que, dans un nombre limité de situations spécifiques, les transferts internationaux de données peuvent avoir lieu lorsqu'aucun autre mécanisme du chapitre V

[5] Voir ci-dessous: MISE EN ŒUVRE DES ORIENTATIONS SUR LES CRITÈRES DE CERTIFICATION.

n'est respecté[6]. Cependant, comme expliqué dans de précédentes orientations publiées par l'EDPB, les dérogations prévues à l'article 49 du RGPD doivent être interprétées de manière restrictive et concernent principalement les activités de traitement qui sont occasionnelles et non répétitives[7].

1.3 Quels sont les acteurs concernés et quel est leur rôle pour la certification en tant qu'outil au service des transferts?

8. Le **comité européen de la protection des données (EDPB)** est habilité à approuver les critères de certification à l'échelle de l'EEE (label européen de protection des données) et à émettre des avis sur les projets de décisions des autorités de contrôle sur les critères de certification et les exigences en matière d'agrément des organismes de certification afin de garantir la cohérence. Il est également compétent pour dresser la liste de tous les mécanismes de certification et de tous les labels et marques en matière de protection des données, et pour mettre cette liste à la disposition du public[8].

9. Les **autorités de contrôle** approuvent les critères de certification lorsque le mécanisme de certification n'est pas un label européen de protection des données[9]. Elles peuvent également agréer l'organisme de certification, concevoir les critères de certification et délivrer la certification si le droit national de leur État membre le prévoit[10].

10. L'**organisme national d'accréditation** peut agréer des organismes tiers de certification en utilisant la norme ISO 17065 et les exigences supplémentaires en matière d'agrément des autorités de contrôle, qui devraient être conformes à la section 2 des présentes lignes directrices. Dans certains États membres, l'agrément peut également être proposé par l'autorité de contrôle compétente et être réalisé par un organisme national d'accréditation ou par les deux.

11. Un **propriétaire de programme** est une organisation identifiable qui a établi des critères et des exigences en matière de certification permettant d'évaluer la conformité. Il est possible que l'organisation qui effectue les évaluations soit la même que celle qui a élaboré le programme et en est propriétaire, mais des modalités peuvent être fixées selon lesquelles une organisation est propriétaire du programme et une autre (ou plusieurs autres) effectue les évaluations en tant qu'organisme de certification.

12. En fonction de la législation nationale, l'**organisme de certification** accrédité comme indiqué ci-dessus peut, à défaut, délivrer les certifications[11]. Il peut concevoir des critères de certification et, partant, être propriétaires de système (voir point 11 ci-dessus). Il doit disposer d'un établissement dans l'EEE, en particulier pour permettre l'exercice effectif des pouvoirs correctifs consacrés à l'article 58, paragraphe 2, point f), du RGPD. Toutefois, l'organisme de certification peut sous-traiter des activités à des experts locaux ou à des établissements situés en dehors de l'EEE, qui effectueront des activités d'audit

[6] Pour de plus amples informations sur l'article 49 et son interaction avec l'article 46 en général, voir lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679.
[7] Voir lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, p. 5.
[8] Article 42, paragraphe 8, du RGPD.
[9] Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement (UE) 2016/679, point 2.2.
[10] Article 42, paragraphe 5, et article 43, paragraphe 1, du RGPD.
[11] Article 42, paragraphe 5, du RGPD.

pour son compte[12]. Néanmoins, un organisme de certification ne peut pas sous-traiter la décision d'octroi ou de non-octroi d'une certification.

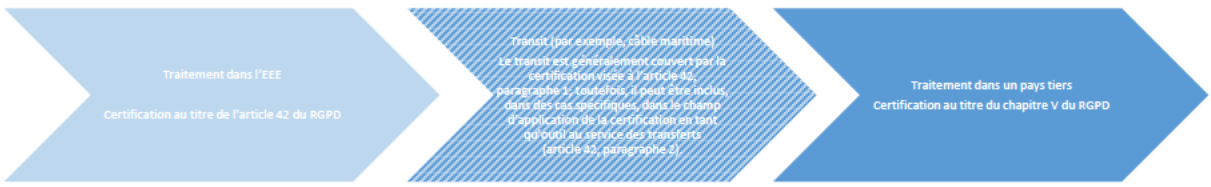
13. L'**importateur de données** est l'entité (responsable du traitement ou sous-traitant) du pays tiers qui reçoit des données d'un exportateur de données.

14. L'**exportateur de données** est l'entité (responsable du traitement ou sous-traitant) qui transfère des données de l'EEE à un importateur de données. L'exportateur de données doit veiller au respect des dispositions du chapitre V.

1.4 Quel est le champ d'application et l'objet de la certification en tant qu'outil au service des transferts?

15. Un mécanisme de certification en tant qu'outil de transfert au titre de l'article 42, paragraphe 2, doit viser à garantir des garanties appropriées pour le traitement des données à caractère personnel conformément à l'article 46, paragraphe 2, point f). La certification démontre l'existence de garanties appropriées fournies par des responsables du traitement ou des sous-traitants établis en dehors de l'EEE ou constituant une organisation internationale recevant des données de la part de responsables du traitement ou de sous-traitants de l'EEE pour contrer les risques spécifiques de transfert de données à caractère personnel.

16. En général, l'opération de transfert de données à caractère personnel d'un État membre vers un pays tiers constitue, en soi, un traitement de données à caractère personnel au sens de l'article 4, paragraphe 2, du RGPD, effectué dans un État membre[13] et qui peut donc être certifié en vertu de l'article 42, paragraphe 1, du RGPD. Toutefois, certaines situations, en fonction du contexte, pourraient inclure le transit dans le champ d'application de la certification en tant qu'outil au service des transferts. Par conséquent, l'objet de la certification, qui coïncide avec la cible d'évaluation lors de la certification[14], devrait généralement être le traitement des données reçues de l'EEE par l'importateur de données dans le pays tiers et le transit, s'il est sous le contrôle de l'importateur.



17. L'objet de la certification peut être une opération de traitement unique ou un ensemble d'opérations. Il peut s'agir de processus de gouvernance au sens de mesures organisationnelles, qui font donc partie intégrante d'une opération de traitement[15].

---

[12] Les organismes de certification doivent évaluer leurs experts locaux conformément à la norme ISO 17065 et aux exigences supplémentaires en matière d'agrément établies par l'autorité de contrôle [article 43, paragraphe 1, point b), du RGPD].

[13] Arrêt de la Cour de justice de l'Union européenne dans l'affaire C-311/18 — Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems, point 83.

[14] Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement (UE) 2016/679, p. 17.

[15] Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement (UE) 2016/679, p. 16 (mécanisme de traitement des plaintes, p. ex.).

18. L'entité présentant une demande serait donc l'importateur de données dans le pays tiers en ce qui concerne son objet de certification.

1.5 Quel devrait être le rôle de l'exportateur dans l'utilisation de la certification comme outil au service des transferts?

19. Le transfert par l'exportateur de données en tant que tel relève généralement directement du RGPD. Cela signifie que l'exportateur est tenu de respecter les obligations qui lui incombent en vertu du RGPD et, en particulier, de veiller à ce que les données soient transférées de manière sécurisée conformément à l'article 32 et au chapitre V, afin de veiller à ce que le niveau de protection des personnes physiques garanti par ce règlement ne soit pas compromis (article 44 du RGPD)[16]. Cela peut, bien entendu, être certifié en vertu de l'article 42, paragraphe 1.

20. En outre, l'exportateur de données qui souhaite utiliser une certification comme garantie appropriée conformément à l'article 46, paragraphe 2, point f), du RGPD est notamment tenu de vérifier si la certification sur laquelle il entend s'appuyer est efficace au regard des caractéristiques du traitement prévu. À cette fin, l'exportateur de données doit vérifier la certification délivrée afin de vérifier si le certificat est valide et non expiré, s'il couvre le transfert spécifique à effectuer et si le transit de données à caractère personnel relève du champ d'application de la certification, ainsi que s'il s'agit de transferts ultérieurs et si une documentation adéquate leur est fournie. En outre, l'exportateur doit vérifier que l'organisme de certification délivrant la certification est accrédité par un organisme national d'accréditation ou une autorité de contrôle compétente. En outre, l'exportateur de données devrait faire référence à l'utilisation de la certification comme outil au service des transferts dans le contrat de traitement des données conformément à l'article 28 du RGPD en cas de transferts du responsable du traitement à un sous-traitant ou d'un contrat de partage de données avec l'importateur de données en cas de transferts du responsable du traitement au responsable du traitement.

21. Étant donné que l'exportateur est responsable de l'application de toutes les dispositions du chapitre V, il doit également évaluer si la certification sur laquelle il entend s'appuyer en tant qu'outil au service des transferts est efficace à la lumière de la législation et des pratiques en vigueur dans le pays tiers qui sont pertinentes pour le transfert en question. Aux fins de cette évaluation et en tant qu'élément important pour démontrer le respect de sa responsabilité, l'exportateur de données peut s'appuyer sur la vérification effectuée par l'organisme de certification de l'évaluation documentée par l'importateur de la législation et des pratiques du pays tiers.

22. Si l'évaluation de l'importateur a révélé que lui-même et/ou l'exportateur de données peut avoir besoin de prévoir des mesures supplémentaires prévues par la certification pour assurer un niveau de protection substantiellement équivalent à celui prévu dans l'EEE, l'exportateur de données doit vérifier les mesures supplémentaires fournies par l'importateur de données titulaire d'une certification et s'il

[16] À cet égard, il est important de noter que l'article 44 du RGPD prévoit clairement qu'un transfert peut être effectué non seulement par un responsable du traitement, mais également par un sous-traitant. Par conséquent, il y a une situation de transfert lorsqu'un sous-traitant envoie des données à un autre sous-traitant, voire à un responsable du traitement dans un pays tiers, conformément aux instructions données par son responsable du traitement [article 28, paragraphe 3, point a), du RGPD]. Dans ces cas, le sous-traitant agit en tant qu'exportateur de données pour le compte du responsable du traitement et doit veiller à ce que les dispositions du chapitre V soient respectées pour le transfert en cause conformément aux instructions du responsable du traitement, y compris l'utilisation d'un outil de transfert approprié. Étant donné que le transfert est une activité de traitement effectuée pour le compte du responsable du traitement, le responsable du traitement est également responsable et pourrait être responsable en vertu du chapitre V, et doit également veiller à ce que le sous-traitant fournisse des garanties suffisantes au titre de l'article 28.

est en mesure de répondre aux mesures techniques et (le cas échéant) supplémentaires demandées par l'importateur de données.

23. Si ces dispositions ne sont pas respectées, l'exportateur de données devra exiger de l'importateur qu'il mette en place des mesures supplémentaires adaptées ou qu'il les établisse lui-même.

1.6 Quel est le processus de certification en tant qu'outil au service des transferts?

24. La certification est volontaire, mais lorsqu'elle est demandée, elle doit être accordée dans le cadre d'un processus transparent fondé sur des règles impératives. Le RGPD accorde une confiance considérable aux mécanismes de certification privés, dans le cadre d'une «autorégulation réglementée». Par conséquent, ces mécanismes doivent garantir que les certificats satisfont matériellement aux exigences de garanties appropriées telles que définies à l'article 46 du RGPD.

25. Par conséquent, la certification doit être fondée sur l'évaluation des critères de certification selon une méthode d'audit contraignante. Ces critères seront approuvés par les autorités de contrôle nationales ou par le comité européen de la protection des données, comme décrit à l'article 42, paragraphe 5, du RGPD. Les critères de certification comprennent des exigences relatives à une évaluation du traitement effectué par l'importateur de données, y compris les transferts ultérieurs, et du cadre juridique applicable au pays tiers, afin d'éviter que les règles et pratiques du pays tiers empêchent l'importateur de respecter les obligations qui lui incombent en vertu de la certification.

26. Au cours du processus de certification, la cible d'évaluation est vérifiée au regard des critères de certification par un organisme de certification accrédité par l'organisme national d'accréditation ou par l'autorité de contrôle compétente[17].

27. Conformément à l'article 43, paragraphe 1, du RGPD, les organismes de certification qui disposent d'un niveau d'expertise approprié en matière de protection des données délivrent et renouvellent la certification, après en avoir informé l'autorité de contrôle afin de lui permettre d'exercer ses pouvoirs en vertu de l'article 58, paragraphe 2, point h), du RGPD si nécessaire.

28. Conformément à l'article 43, paragraphe 5, du RGPD, les organismes de certification communiquent aux autorités de contrôle compétentes les raisons de l'octroi ou du retrait de la certification demandée. Cela ne signifie pas que l'organisme de certification a besoin de l'autorisation de l'autorité de contrôle pour délivrer la certification. L'organisme de certification contrôlera le respect des critères de certification par ses clients.

29. L'autorité de contrôle a le pouvoir correcteur de retirer une certification ou d'ordonner le retrait d'une certification délivrée en application des articles 42 et 43 du RGPD, ou d'ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont plus satisfaites.

30. Un label européen de protection des données pour les transferts internationaux de données peut servir d'outil pour couvrir les transferts vers des pays tiers, accompagné d'engagements contraignants et exécutoires[18].

---

[17] Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données (2016/679), p. 9.

[18] Voir l'article 42, paragraphe 5, du RGPD et le point 35 des lignes directrices 1/2018 de l'EDPB relatives à la certification et à la fixation des critères de certification conformément aux articles 42 et 43 du règlement.

31. Néanmoins, les certifications à utiliser comme outil au service des transferts peuvent également être délivrées conformément aux régimes de certification nationaux agréés dans les États de l'EEE. En tant que telles, elles ne sont valables que pour les transferts vers des pays tiers par des exportateurs de l'État membre de l'EEE où le système de certification a été approuvé, étant donné qu'il n'y a pas de reconnaissance mutuelle des différentes certifications des États de l'EEE. Toutefois, les autorités de contrôle de différents États de l'EEE sont libres d'approuver le même mécanisme de certification pour les transferts[19].

2 MISE EN ŒUVRE DES ORIENTATIONS SUR LES EXIGENCES EN MATIÈRE D'AGRÉMENT

32. Les exigences relatives à l'agrément d'un organisme de certification pour les certifications en tant qu'outil au service des transferts figurent dans la norme ISO 17065 et s'inspirent des lignes directrices 4/201820 dans le contexte du chapitre V, comme expliqué ci-dessous.

33. De l'avis du comité européen de la protection des données, les exigences supplémentaires en matière d'agrément élaborées sur la base des lignes directrices 4/2018 et ISO 17065 adoptées conformément à l'article 64, paragraphe 1, point c), du RGPD couvrent déjà les exigences spécifiques requises pour l'agrément d'un organisme de certification en ce qui concerne les certifications en tant qu'outil au service des transferts. Toutefois, dans un scénario de transfert, certaines exigences doivent être précisées au moyen de notes explicatives et d'interprétation.

34. En ce qui concerne les exigences en matière de ressources (voir l'exigence 6 des lignes directrices 4/2018 – annexe 1), l'organisme de certification veille à disposer des ressources nécessaires pour pouvoir vérifier que, comme l'exigent les critères de certification, l'importateur a dûment et correctement procédé à l'évaluation nécessaire de la situation juridique et des pratiques du ou des pays tiers où il est établi ou exerce ses activités[21]. Cette évaluation devrait être effectuée en ce qui concerne les activités de traitement à certifier dans le cadre du mandat d'évaluation en ce qui concerne les garanties appropriées prévues à l'article 46 du RGPD, et comprend les mesures supplémentaires recensées et mises en œuvre par l'importateur, le cas échéant. Cela inclut également, par exemple, une connaissance significative de la législation et des pratiques locales pertinentes et des compétences linguistiques adéquates en rapport avec le ou les pays tiers.

35. En ce qui concerne les exigences en matière de processus (voir l'exigence 7 des lignes directrices 4/2018, annexe 1), l'organisme de certification veille à ce que le processus de certification puisse être étayé par d'éventuels audits sur place, à ce qu'il soit effectué au regard du traitement qui aura lieu

[19] Si une autorité de contrôle dirige l'adoption des critères de certification X dans le cadre de son initiative nationale et que, par la suite, compte tenu des critères du système et des réglementations nationales spécifiques applicables, d'autres pays souhaitent adopter les mêmes critères de certification, ils peuvent les adopter sans déclencher un avis du comité européen de la protection des données au titre de l'article 64 du RGPD et s'appuyer sur l'avis rendu à la première autorité de contrôle, conformément à l'article 64, paragraphe 3, du RGPD [voir, à cet égard, référence aux orientations – addendum (annexe des lignes directrices 1/2018 sur la certification et l'identification des critères de certification conformément aux articles 42 et 43 du règlement), paragraphe 66].

[20] Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du RGPD et de son annexe.

[21] Voir point 12 ci-dessus.

dans le ou les pays tiers, et à ce que l'évaluation porte également sur la mise en œuvre pratique de la législation et des politiques en vigueur dans le ou les pays tiers.

36. En ce qui concerne les exigences relatives aux modifications ayant une incidence sur la certification (voir l'exigence 7.10 des lignes directrices 4/2018, annexe 1), l'organisme de certification surveille les modifications de la législation et/ou de la jurisprudence des pays tiers susceptibles d'avoir une incidence sur le traitement relevant du champ d'application de la cible d'évaluation.

3 CRITÈRES DE CERTIFICATION SPÉCIFIQUES

37. Dans le cadre de l'examen des critères de certification spécifiques, les présentes lignes directrices se fondent sur les 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), l'annexe 2 correspondante sur l'examen et l'évaluation des critères de certification visés à l'article 42, paragraphe 5, et l'addendum aux orientations sur l'évaluation des critères de certification.

38. De l'avis du comité européen de la protection des données, les critères de certification élaborés sur la base de l'annexe 2 des lignes directrices 1/2018 et de l'addendum aux orientations sur l'évaluation des critères de certification couvrent déjà la majorité des critères de certification qui doivent être pris en considération lors de l'élaboration d'un système de certification à utiliser comme outil au service des transferts. Toutefois, il pourrait être nécessaire de préciser davantage certains de ces critères existants afin de les adapter à un scénario de transfert spécifique (voir point 3.1). En outre, il pourrait être nécessaire de formuler des critères supplémentaires aux fins de l'application de garanties appropriées, y compris en ce qui concerne les droits des personnes concernées (voir point 3.2).

3.1 MISE EN ŒUVRE DES ORIENTATIONS SUR LES CRITÈRES DE CERTIFICATION

39. En ce qui concerne le champ d'application du mécanisme de certification et la cible de l'évaluation (voir annexe 2, section 2.a), il convient de décrire clairement dans la documentation pertinente, y compris en ce qui concerne le transfert de données à caractère personnel vers un pays tiers ou s'il est destiné à couvrir également leur transit.

40. En ce qui concerne le champ d'application du mécanisme de certification et la cible de l'évaluation (voir annexe 2, section 2.b), la documentation pertinente doit décrire concrètement pour quel type d'entité (par exemple: responsable du traitement et/ou sous-traitant) le mécanisme de certification est applicable.

41. En ce qui concerne le champ d'application du mécanisme de certification et l'objectif de l'évaluation (voir annexe 2, section 2.f), les critères devraient exiger que la cible d'évaluation soit définie concrètement afin d'éviter les malentendus. Ces informations doivent comprendre au moins:

42. le(s) traitement(s), y compris dans le cas où des transferts ultérieurs sont envisagés:

    a) la finalité;

    b) le type d'entité (ex: responsable du traitement et/ou sous-traitant);

    c) le type de données transférées, en tenant compte de l'existence ou non de catégories particulières de données à caractère personnel telles que définies à l'article 9 du RGPD;

    d) les catégories de personnes concernées;

e) les pays dans lesquels le traitement des données a lieu.

43. En ce qui concerne la transparence et les droits des personnes concernées (voir annexe 2, section 8), les critères de certification devraient:

a) exiger que des informations sur les activités de traitement soient fournies aux personnes concernées, y compris, le cas échéant, sur le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale (voir articles 12, 13 et 14 du RGPD);

b) exiger que les personnes concernées se voient garantir des droits d'accès, de rectification, d'effacement, de limitation, de notification concernant la rectification, l'effacement ou la limitation, d'opposition au traitement, de ne pas être soumises à des décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, essentiellement équivalentes à celles prévues aux articles 15 à 19, 21 et 22 du RGPD;

c) exiger qu'une procédure appropriée de traitement des réclamations soit mise en place par l'importateur de données titulaire d'une certification afin de garantir la mise en œuvre effective des droits des personnes concernées;

d) exiger d'évaluer si et dans quelle mesure ces droits sont opposables aux personnes concernées dans le pays tiers concerné et toute mesure supplémentaire appropriée qui pourrait devoir être mise en place pour les faire respecter, par exemple en exigeant que l'importateur accepte de se soumettre à la juridiction de l'autorité de contrôle compétente pour l'exportateur ou les exportateurs et de coopérer avec elle dans le cadre de toute procédure visant à garantir le respect de ces droits et, en particulier, qu'il accepte de répondre aux demandes de renseignements, de se soumettre aux audits et de se conformer aux mesures adoptées par l'autorité de contrôle susmentionnée, y compris les mesures correctives et compensatoires.

44. En ce qui concerne les mesures techniques et organisationnelles garantissant la protection (annexe 2, section 10.q), les critères de certification devraient exiger de l'importateur qu'il informe l'exportateur et, si l'importateur agit en qualité de responsable du traitement, qu'il informe l'autorité de contrôle de l'EEE compétente pour le ou les exportateurs de données des violations de données et qu'il les communique aux personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés, conformément aux exigences de l'article 34 du RGPD.

3.2 CRITÈRES DE CERTIFICATION SPÉCIFIQUES SUPPLÉMENTAIRES

45. Compte tenu des garanties recensées pour d'autres instruments de transfert au titre de l'article 46 du RGPD (telles que les règles d'entreprise contraignantes ou les codes de conduite) et afin d'assurer un niveau de protection cohérent, et compte tenu de l'arrêt Schrems II de la CJUE, l'EDPB estime que le mécanisme de certification devant être utilisé comme outil au service des transferts vers des pays tiers devrait également tenir compte des critères énumérés ci-dessous.

1 Évaluation de la législation du pays tiers

a) Les critères exigent-ils que l'importateur ait évalué les règles et pratiques du pays tiers dans lequel il opère et empêchent-ils l'importateur de respecter ses engagements au titre de la certification?

b) Les critères exigent-ils que l'importateur documente l'évaluation des règles et pratiques du pays tiers dans lequel il opère et tienne la documentation à la disposition de l'organisme de certification et, sur demande, à celle de l'autorité de contrôle de l'EEE compétente pour l'exportateur de données et de l'exportateur de données?

c) Les critères exigent-ils que l'importateur ait identifié et mis en œuvre les mesures organisationnelles et techniques pour fournir les garanties appropriées au titre de l'article 46 du RGPD en tenant compte des «recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE»?

d) Les critères imposent-ils à l'importateur de documenter les mesures organisationnelles et techniques effectivement mises en œuvre afin de fournir les garanties appropriées au titre de l'article 46 du RGPD et de tenir la documentation à la disposition de l'organisme de certification et, sur demande, des autorités compétentes en matière de protection des données et de l'exportateur de données?

e) Les critères exigent-ils que l'importateur ait identifié et mis en œuvre les mesures organisationnelles et techniques visant à garantir la sécurité des données à caractère personnel transférées, compte tenu des «recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE» si le transit est inclus dans le champ d'application de la certification en tant qu'outil au service des transferts?

f) Les critères exigent-ils une garantie à l'organisme de certification et à l'exportateur que l'importateur n'a aucune raison de croire que la législation et les pratiques qui lui sont applicables peuvent l'empêcher de remplir les obligations qui lui incombent en vertu de la certification?

2 Obligations générales des exportateurs et des importateurs

a) Les critères exigent-ils d'établir dans des accords contractuels (par exemple dans un contrat de services existant) entre exportateurs et importateurs une description du transfert spécifique auquel s'applique la certification ainsi que la création de droits de tiers bénéficiaire pour les personnes concernées?

b) Dans la mesure où les critères exigent un contenu spécifique pour ces accords ou instruments contractuels et où un modèle est fourni, les critères exigent-ils qu'ils fassent également l'objet de l'évaluation?

3 Règles relatives aux transferts ultérieurs

a) Les critères exigent-ils que les transferts ultérieurs soient soumis à des garanties spécifiques conformément aux exigences du chapitre V du RGPD afin de garantir que le niveau de protection assuré dans l'EEE ne soit pas compromis et que des documents appropriés soient tenus à la disposition de l'organisme de certification et de l'autorité de contrôle de l'EEE compétente pour le ou les exportateurs de données et à celle de l'exportateur de données sur demande?

4 Voies de recours et exécution

a) Les critères prévoient-ils que les personnes concernées peuvent faire valoir leurs droits en tant que tiers bénéficiaires à l'encontre de l'importateur de données devant la juridiction de l'EEE de la résidence habituelle de la personne concernée, ou auprès d'une organisation internationale, y compris en ce qui concerne la réparation du préjudice subi par la personne concernée en cas de non-respect par l'importateur du système de certification concerné?

b) Les critères permettent-ils d'évaluer de manière adéquate qu'un importateur est responsable dans l'EEE du préjudice subi par la personne concernée en cas de non-respect du système de certification concerné?
c) Les critères exigent-ils que les personnes concernées puissent introduire une réclamation contre l'importateur auprès d'une autorité de contrôle de l'EEE, en particulier dans l'État de l'EEE où il a sa résidence habituelle ou son lieu de travail, ou dans l'État compétent pour le ou les exportateurs de données?
d) Les critères exigent-ils que l'importateur coopère avec l'autorité de contrôle de l'EEE compétente pour le ou les exportateurs de données et accepte d'être audité et d'être inspecté par celui-ci, qu'il tienne compte de ses conseils et qu'il se conforme à ses décisions?

5 Processus et actions pour les situations dans lesquelles la législation nationale empêche le respect des engagements pris dans le cadre de la certification

a) Les critères exigent-ils un engagement selon lequel, lorsque l'importateur de données dans un pays tiers ou une organisation internationale a des raisons de croire que des modifications de la législation et des pratiques qui lui sont applicables peuvent l'empêcher de remplir ses obligations au titre de la certification, il le notifiera rapidement à l'organisme de certification et à l'exportateur de données, afin que ce dernier puisse évaluer s'il convient d'arrêter immédiatement les transferts?
b) Les critères exigent-ils une description des mesures à prendre (y compris la notification à l'exportateur dans l'EEE et la prise de mesures supplémentaires appropriées) si l'importateur de données a connaissance de la législation ou des pratiques d'un pays tiers qui empêchent le respect des obligations découlant de la certification, ainsi que des mesures à prendre en cas de demandes d'informations émanant d'autorités de pays tiers (y compris l'obligation de réexaminer et, le cas échéant, de contester la légalité de la demande et de réduire au minimum toute information divulguée)?

6 Traitement des demandes d'accès aux données introduites par les autorités de pays tiers

a) Les critères exigent-ils que l'importateur de données informe rapidement l'exportateur de données en cas de demande d'accès de la part des autorités de pays tiers et qu'il prenne des mesures supplémentaires appropriées?
b) Les critères exigent-ils que les transferts résultant de demandes d'accès disproportionnées émanant d'autorités publiques de pays tiers n'aient pas lieu, en particulier si ces demandes nécessitent des transferts généralisés et indifférenciés de données à caractère personnel?

7 Garanties supplémentaires concernant l'exportateur

46. Les critères exigent-ils que, lorsque cela est envisagé, l'importateur de données veille, également au moyen d'exigences contraignantes à cet égard pour l'exportateur de données, à ce que les mesures supplémentaires qu'il a identifiées soient accompagnées de mesures supplémentaires correspondantes de la part de l'exportateur de données, compte tenu des recommandations 01/2020 du comité européen de la protection des données et des utilisations, afin de garantir une mise en œuvre effective des mesures supplémentaires de l'importateur?

4 ENGAGEMENTS CONTRAIGNANTS ET EXÉCUTOIRES À METTRE EN ŒUVRE

47. L'article 42, paragraphe 2, du RGPD exige que les responsables du traitement et les sous-traitants non soumis au RGPD qui adhèrent à un mécanisme de certification destiné aux transferts prennent l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants[22], d'appliquer les garanties appropriées prévues par le mécanisme de certification, notamment en ce qui concerne les droits des personnes concernées.

48. Comme le précise le RGPD, de tels engagements peuvent être pris au moyen d'un contrat, ce qui apparaît comme la solution la plus simple. D'autres instruments peuvent également être utilisés, à condition que les responsables du traitement/sous-traitants adhérant au mécanisme de certification soient en mesure de démontrer leur caractère contraignant et exécutoire.

49. En tout état de cause, ce caractère doit être garanti par le droit de l'Union et les engagements devraient également être contraignants et exécutoires par les personnes concernées en tant que tiers bénéficiaires.

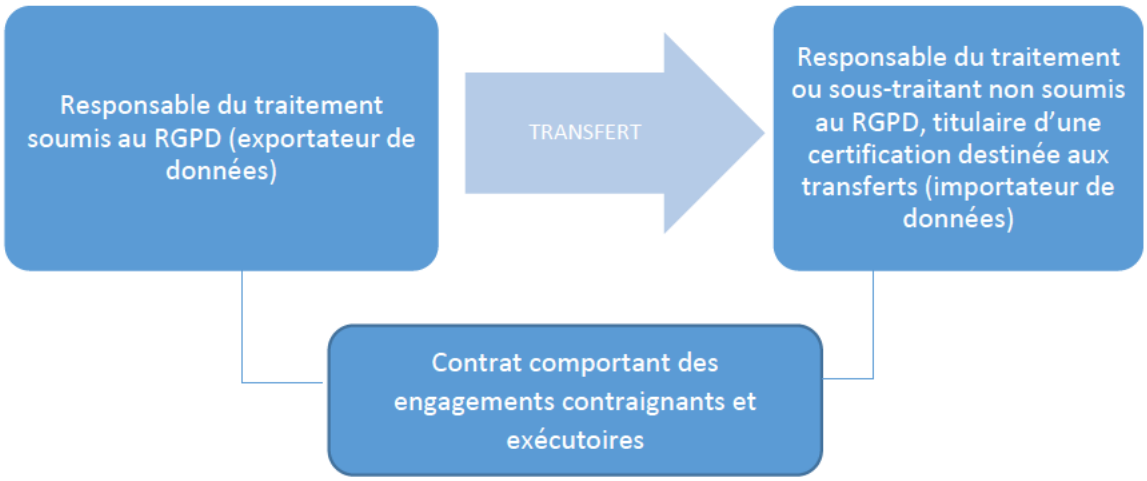
50. Une option simple consisterait à inclure les engagements contraignants et exécutoires dans le contrat entre l'exportateur de données et l'importateur de données. Dans la pratique, les parties pourraient utiliser un contrat existant (par exemple, un accord de service entre l'exportateur et l'importateur de données, le contrat d'accord sur le traitement des données conformément à l'article 28 du RGPD entre les responsables du traitement et les sous-traitants, ou un accord de partage de données entre responsables du traitement distincts) dans lequel les engagements contraignants et exécutoires pourraient être inclus. Ces engagements devraient être clairement distingués de toute autre clause. Une autre option pourrait consister à recourir à un contrat distinct en ajoutant au mécanisme de certification destiné aux transferts un contrat type qui devrait ensuite être signé par les responsables du traitement/sous-traitants dans le pays tiers et tous ses exportateurs de données.

51. Il convient de prévoir une certaine souplesse pour choisir l'option la plus appropriée en fonction de la situation spécifique.

52. Lorsque le mécanisme de certification est destiné à être utilisé pour les transferts et les transferts ultérieurs d'un sous-traitant à un autre sous-traitant, une référence au mécanisme de certification et à l'instrument prévoyant des engagements contraignants et exécutoires devraient également figurer dans l'accord de sous-traitance signé par le sous-traitant et son responsable du traitement.

Exemple d'engagements contraignants et exécutoires inclus dans le contrat entre l'exportateur de données et l'importateur de données:

[22] Cet instrument juridiquement contraignant ne constitue pas un autre instrument du chapitre V (tel que, par exemple, le CCT), étant donné que ces engagements contraignants et exécutoires visés à l'article 46, paragraphe 2, point f), doivent être conçus de manière à garantir que l'importateur respectera les critères de certification.



53. D'une manière générale, le contrat ou tout autre instrument juridiquement contraignant doit spécifier que le responsable du traitement/sous-traitant titulaire d'une certification agissant en tant qu'importateur s'engage à respecter les règles spécifiées dans la certification destinée aux transferts lors du traitement des données pertinentes reçues de l'EEE et déclare qu'il n'a aucune raison de croire que les lois et pratiques du pays tiers applicables au traitement en question, y compris toute obligation de divulguer des données à caractère personnel ou toute mesure autorisant l'accès des autorités publiques, l'empêche de respecter ses engagements au titre de la certification et qu'il informe l'exportateur de toute modification pertinente de la législation ou de la pratique à cet égard.

54. Le contrat ou l'autre instrument choisi doit également prévoir des mécanismes permettant de faire respecter ces engagements en cas de violation par le responsable du traitement/sous-traitant, notamment en ce qui concerne les droits des personnes concernées dont les données seront transférées dans le cadre de la certification.

55. Plus particulièrement, le contrat ou l'autre instrument choisi devrait inclure les points suivants:

- l'existence d'un droit pour les personnes concernées dont les données sont transférées dans le cadre de la certification de faire respecter en tant que tiers bénéficiaires les engagements pris par l'importateur de données certifié dans le cadre de la certification;

- la question de la responsabilité en cas de non-respect des règles prévues par la certification par un importateur de données titulaire d'une certification en dehors de l'EEE. Les personnes concernées ont la possibilité, en cas de non-respect des règles prévues par la certification par un importateur de données titulaire d'une certification en dehors de l'EEE, d'introduire un recours, en invoquant leurs droits de tiers bénéficiaire, y compris une indemnisation, contre cette entité devant une autorité de contrôle de l'EEE et une juridiction de l'EEE de la résidence habituelle de la personne concernée. Si une personne concernée décide de le faire, l'importateur titulaire d'une certification doit accepter sa décision. Les personnes concernées ont également la possibilité, si un manquement de l'importateur est susceptible d'engager la responsabilité de l'exportateur de données, d'introduire un recours contre l'exportateur de données devant l'autorité de contrôle ou devant la juridiction de l'établissement de l'exportateur de données ou de la résidence habituelle

de la personne concernée[23]. L'importateur de données et l'exportateur de données devraient également accepter que la personne concernée puisse être représentée par un organisme, une organisation ou une association à but non lucratif dans les conditions énoncées à l'article 80, paragraphe 1, du RGPD;

- l'existence d'un droit pour l'exportateur d'exiger le respect des règles de la certification par l'importateur de donnés titulaire d'une certification en tant que tiers bénéficiaire;
- l'existence d'une obligation pour l'importateur de données titulaire d'une certification de notifier à l'exportateur et à l'autorité de contrôle de l'exportateur de données toute mesure prise par l'organisme de certification en réponse à un manquement aux règles de certification constaté par le même importateur de données.

[23] Cette responsabilité devrait être sans préjudice des mécanismes à mettre en œuvre en vertu de la certification avec l'organisme chargé du suivi, qui peut également prendre des mesures correctives à l'encontre des responsables du traitement/sous-traitants conformément à la certification.

ANNEXE

A. EXEMPLES DE MESURES SUPPLÉMENTAIRES À METTRE EN ŒUVRE PAR L'IMPORTATEUR DANS LE CAS OÙ LE TRANSIT EST INCLUS DANS LE CHAMP D'APPLICATION DE LA CERTIFICATION

Utilisation 1: stockage de données à des fins de sauvegarde et à d'autres fins qui ne nécessitent pas l'accès aux données en clair

Des critères relatifs aux normes de cryptage et à la sécurité de la clé de décryptage, en particulier des critères relatifs à la situation juridique dans le pays tiers, doivent être établis. Si l'importateur peut être contraint de transmettre des clés de décryptage, la mesure supplémentaire ne peut être considérée comme efficace[24].

Utilisation 2: transfert de données pseudonymisées

Dans le cas de données pseudonymisées, des critères sont établis en ce qui concerne la sécurité des informations supplémentaires nécessaires pour attribuer les données transférées à une personne identifiée ou identifiable, en particulier:

— des critères relatifs à la situation juridique dans le pays tiers. Si l'importateur peut être contraint d'accéder à des données supplémentaires ou de les utiliser pour attribuer les données à une personne identifiée ou identifiable, la mesure ne peut être considérée comme efficace[25];

— des critères relatifs à la définition des informations supplémentaires mises à la disposition des autorités de pays tiers qui pourraient suffire à attribuer les données à une personne identifiée ou identifiable.

Utilisation 3: chiffrement de données afin de les protéger contre l'accès des autorités publiques du pays tiers de l'importateur lorsqu'elles transitent entre l'exportateur et son importateur

Dans le cas de données cryptées, tous les critères de sécurité du transit sont inclus. Si l'importateur peut être contraint de transmettre des clés cryptographiques pour le décryptage ou l'authentification ou de modifier un composant utilisé pour le transit de telle sorte que ses propriétés de sécurité soient compromises, la mesure supplémentaire ne peut être considérée comme efficace[26].

Utilisation 4: destinataire protégé

Dans le cas des destinataires protégés, les critères relatifs aux limites du privilège doivent être définis. Le traitement des données doit rester dans les limites du secret professionnel. Cela vaut également pour le traitement par les (sous-) sous-traitants et les transferts ultérieurs, dont les destinataires doivent également être privilégiés[27].

---

[24] Annexe 2, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE — Version 2.0 — Utilisation 1: Stockage de données à des fins de sauvegarde et à d'autres fins qui ne nécessitent pas l'accès aux données en, p. 85; https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[25] Voir les points 86 à 89 ci-dessus.

[26] Voir le point 90 ci-dessus.

[27] Voir le point 91 ci-dessus.

B. EXEMPLES DE MESURES SUPPLÉMENTAIRES DANS LE CAS OÙ LE TRANSIT N'EST PAS COUVERT PAR LA CERTIFICATION ET OÙ L'EXPORTATEUR DOIT GARANTIR CES MESURES

Utilisation 2: transfert de données pseudonymisées

Des critères sont fournis en ce qui concerne les informations supplémentaires dont disposent les autorités du pays tiers et qui pourraient être suffisantes pour attribuer les données à une personne identifiée ou identifiable.

Utilisation 3: chiffrement de données afin de les protéger contre l'accès des autorités publiques du pays tiers de l'importateur lorsqu'elles transitent entre l'exportateur et son importateur

Des critères sont fournis en ce qui concerne la fiabilité de l'autorité ou de l'infrastructure de certification des clés publiques utilisées, la sécurité des clés cryptographiques utilisées pour l'authentification ou le décryptage et la fiabilité de la gestion des clés, ainsi que l'utilisation de logiciels correctement entretenus sans vulnérabilités connues.

Si l'importateur peut être contraint de divulguer des clés cryptographiques adaptées au décryptage ou à l'authentification ou de modifier un composant utilisé pour le transit afin de porter atteinte à ses propriétés de sécurité, la mesure ne peut être considérée comme efficace[28].

Utilisation 4: destinataire protégé

Dans le cas des destinataires protégés, les critères relatifs aux limites du privilège doivent être définis. Le traitement des données doit rester dans les limites du secret professionnel. Cela vaut également pour le traitement par les sous-traitants et sous-traitants ultérieurs et pour les transferts ultérieurs, dont les destinataires doivent également être privilégiés[29].

[28] Voir les recommandations précitées, point 90.
[29] Voir les recommandations précitées, point 91.