CADRE DE PROTECTION DES DONNÉES UE-ÉTATS-UNIS

F.A.Q. POUR LES ENTREPRISES EUROPÉENNES[1]

Adopté le 16 juillet 2024

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

[1] Dans ce contexte, on entend par «entreprises européennes» les entreprises de l'EEE qui transfèrent ou peuvent transférer des données à caractère personnel à des entreprises établies aux États-Unis et certifiées au titre du CPD.

Adopté

Table des matières

Q1. QU'EST-CE QUE LE CADRE DE PROTECTION DES DONNEES UE-ÉTATS-UNIS?

Le cadre de protection des données UE-États-Unis («CPD») est un mécanisme d'autocertification pour les entreprises établies aux États-Unis. Les entreprises qui se sont autocertifiées au titre du CPD sont tenues de se conformer à ses principes, règles et obligations concernant le traitement des données à caractère personnel des citoyens de l'EEE. Pour de plus amples informations sur ces engagements, voir les principes du cadre de protection des données.[2]

La Commission européenne a estimé que les transferts de données à caractère personnel depuis l'EEE à des entreprises certifiées au titre du CPD bénéficient d'un niveau de protection adéquat.[3] Par conséquent, les données à caractère personnel peuvent être transférées librement à des entreprises certifiées établies aux États-Unis, sans qu'il soit nécessaire de mettre en place des garanties supplémentaires ou d'obtenir une autorisation. Voici quelques liens pertinents pour de plus amples informations:

- Questions et réponses:cadre de protection des données UE-États-Unis[4] de la Commission européenne
- Le site web du cadre de protection des données tel qu'il est géré par le ministère américain du commerce[5]
- Décision de la Commission européenne concernant le niveau de protection adéquat des données à caractère personnel en vertu du cadre de protection des données UE-États-Unis[6]

Le CPD s'applique à tout type de données à caractère personnel transférées de l'EEE vers les États-Unis, notamment les données à caractère personnel traitées à des fins commerciales ou de santé, et les données relatives aux ressources humaines collectées dans le cadre d'une relation de travail (ci-après dénommées: «données RH»), pour autant que l'entreprise destinataire aux États-Unis soit auto-certifiée au titre du CPD pour traiter ces types de données.[7]

Q2. QUELLES ENTREPRISES AMERICAINES PEUVENT BENEFICIER DU CADRE DE PROTECTION DES DONNEES UE-ÉTATS-UNIS?

Pour pouvoir s'autocertifier au titre du CPD, une entreprise établie aux États-Unis doit se soumettre aux pouvoirs d'enquête et d'exécution de la commission fédérale du commerce des États-Unis (U.S.

[2] https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles

[3] La décision relative au caractère adéquat du cadre de protection des données a été adoptée par la Commission européenne le 10 juillet 2023. Le CPD a été conçu par la Commission européenne et le ministère américain du commerce pour remplacer la décision (UE) 2016/1250 relative au bouclier de protection des données, qui a été déclarée invalide par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, *Commissaire à la protection des données/Facebook Ireland Limited et Maximillian Schrems (Schrems II)*.

[4] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

[5] https://www.dataprivacyframework.gov/s/

[6] https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

[7] Il convient de noter que toutes les autocertifications au titre du CPD ne couvrent pas les données RH. Il est donc important de vérifier si tel est le cas, le cas échéant. Voir également Q3.

Federal Trade Commission, «FTC») ou du ministère américain des transports (U.S. Department of Transportation, «DoT»). D'autres organes statutaires des États-Unis pourraient être inclus à l'avenir.[8]

Cela signifie, par exemple, que les organisations sans but lucratif, les banques, les compagnies d'assurance et les fournisseurs de services de télécommunications (en ce qui concerne les activités habituelles) qui ne relèvent pas de la compétence de la FTC ou du DoT ne peuvent pas s'autocertifier au titre du CPD.

Q3. QUE FAIRE AVANT DE TRANSFERER DES DONNEES A CARACTERE PERSONNEL A UNE ENTREPRISE ETABLIE AUX ÉTATS-UNIS QUI EST, OU PRETEND ETRE, CERTIFIEE AU TITRE DU CADRE DE PROTECTION DES DONNEES UE-ÉTATS-UNIS?

Avant de transférer des données à caractère personnel à une entreprise établie aux États-Unis qui prétend être autocertifiée au titre du CPD, un exportateur de données de l'EEE doit s'assurer que l'entreprise aux États-Unis détient une autocertification en cours de validité (les certifications doivent être renouvelées chaque année) et que cette certification couvre les données en question (notamment des données RH ou, selon le cas, des données non-RH).[9]

Afin de vérifier si une autocertification est valide et applicable, les exportateurs de données dans l'EEE doivent vérifier si l'entreprise aux États-Unis figure sur la liste du cadre de protection des données[10], publiée sur le site web du ministère américain du commerce. Cette liste comprend également un registre des sociétés qui ont été radiées de la liste («participants inactifs»), indiquant les raisons de leur radiation. Un exportateur de données de l'EEE ne peut se prévaloir du CPD pour transférer des données à caractère personnel à ces entreprises. Veuillez noter que les entreprises qui ont été radiées de la liste du cadre de protection des données doivent continuer d'appliquer les principes du cadre de protection des données aux données à caractère personnel qu'elles ont reçues pendant la période de leur participation au CPD aussi longtemps qu'elles conserveront ces données.

Pour le transfert de données à caractère personnel à des entreprises établies aux États-Unis qui ne sont pas (ou ne sont plus) autocertifiées au titre du CPD, d'autres motifs de transfert prévus au chapitre V du RGPD peuvent être invoqués, tels que des règles d'entreprise contraignantes ou des clauses contractuelles types.

Le fait que le destinataire aux États-Unis soit autocertifié au titre du CPD permettra aux exportateurs de données de l'EEE de se conformer au chapitre V du RGPD, mais toutes les autres exigences du RGPD et de toute autre législation nationale en matière de protection des données restent applicables.

3.1. Transferts à des filiales américaines d'entreprises certifiées au titre du cadre de protection des données UE-États-Unis

[8] Voir l'annexe I de la décision d'adéquation, principes du cadre de protection UE-États-Unis publiés par le ministère américain du commerce, point I.2.
[9] Voir Q1 pour la définition des données RH.
[10] https://www.dataprivacyframework.gov/list

Dans le cas de transferts à des entreprises aux États-Unis qui sont des filiales d'une société mère certifiée au titre du CPD, les exportateurs de données de l'EEE doivent vérifier si la certification de la société mère couvre également la filiale concernée.

Vous trouverez des informations supplémentaires sur les modalités de vérification de la portée de l'autocertification d'une organisation, afin de déterminer notamment si d'autres entités ou filiales américaines sont couvertes par cette autocertification, à l'adresse suivante: ici.[11]

3.2. Transferts à une entreprise aux États-Unis agissant en tant que responsable du traitement

Avant de transférer des données à caractère personnel à un responsable du traitement aux États-Unis, un exportateur de données de l'EEE doit s'assurer que le transfert est conforme à toutes les dispositions pertinentes du RGPD. Dans un premier temps, l'exportateur de données ne peut partager des données à caractère personnel avec une entreprise aux États-Unis que s'il existe une base juridique pour le traitement (article 6 du RGPD). De plus, toutes les autres exigences du RGPD doivent être respectées (par exemple, la limitation des finalités, la proportionnalité, l'exactitude et les obligations d'information à l'égard des personnes concernées). Il convient de noter que lorsque des données doivent être transférées à une entreprise auto-certifiée aux États-Unis, l'exportateur de données de l'EEE doit, conformément aux articles 13 et 14 du RGPD, informer les personnes concernées de l'identité des destinataires de leurs données et du fait que le transfert est couvert par la décision relative au caractère adéquat du cadre de protection des données UE-États-Unis.

3.3. Transferts à une entreprise aux États-Unis agissant en tant que sous-traitant

Lorsqu'un responsable du traitement de l'EEE transfère des données à un sous-traitant aux États-Unis, le responsable du traitement et le sous-traitant ont l'obligation de conclure un accord de traitement des données en application de l'article 28 du RGPD (ci-après: accord de traitement des données), indépendamment du fait que le sous-traitant soit autocertifié au titre du CPD.

Vous trouverez ici de plus amples informations sur les exigences contractuelles pour les transferts à un sous-traitant aux États- Unis.[12]

La conclusion d'un accord de traitement des données est nécessaire pour garantir que le sous-traitant américain s'engage à:

- ne traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;

[11] https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-(DPF)-Commitments

[12] https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor

- garantir que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou sont soumises à une obligation statutaire de confidentialité appropriée;

- mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à ce que prévoient l'accord de traitement des données (découlant de l'article 32 du RGPD) et les sections 4 et 10 du CPD;

- respecter les conditions visées dans l'accord de traitement des données (découlant de l'article 28, paragraphes 2 et 4, du RGPD) et à la section II.3.B du CPD pour recruter un autre sous-traitant;

- tenir compte de la nature du traitement, aider le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III du RGPD;

- aider le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant;

- selon le choix du responsable du traitement, effacer toutes les données à caractère personnel ou les renvoyer au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruire les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel;

- mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. En ce qui concerne ce dernier point, le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du CPD.

Lorsque le sous-traitant américain recrute un autre sous-traitant (un «sous-traitant ultérieur») pour effectuer des activités de traitement spécifiques pour le compte du responsable du traitement de l'EEE, le sous-traitant doit veiller à ce que les exigences énoncées à la section II.3.B du CPD soient remplies. Il s'agit notamment de veiller à ce que le sous-traitant ultérieur fournisse le même niveau de protection des données à caractère personnel que celui exigé par le RGPD et se conforme aux mêmes obligations en matière de protection des données que celles énoncées dans l'accord de traitement des données. Lorsqu'un sous-traitant ultérieur manque à ses obligations en matière de protection des données, le sous-traitant américain initial demeure entièrement responsable devant le responsable du traitement de l'exercice des obligations du sous-traitant ultérieur.

Q4. OU PUIS-JE TROUVER DES ORIENTATIONS CONCERNANT LA CERTIFICATION DES FILIALES AMERICAINES D'ENTREPRISES EUROPEENNES?

Les filiales américaines d'entreprises de l'EEE peuvent s'autocertifier au titre du CPD si elles relèvent de la compétence de la FTC ou du DoT.

Vous trouverez de plus amples informations sur les critères d'éligibilité ici,[13] ainsi qu'un guide sur le processus d'autocertification ici[14].

[13] https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-(DPF)-Program

[14] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931)