Avis 4/2019

sur le projet d'arrangement administratif relatif au transfert de données à caractère personnel entre les autorités de surveillance financière de l'Espace économique européen (EEE) et les autorités de surveillance financière hors EEE

adopté le 12 février 2019

Table des matières

Le comité européen de la protection des données,

vu l'article 63, l'article 64, paragraphes 2 à 8, et l'article 46, paragraphe 3, point b), 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 relatif à 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,

vu les articles 10 et 22 de son règlement intérieur du 25 mai 2018, tel que modifié le 23 novembre 2018,

considérant ce qui suit:

(1) Conformément à l'article 46, paragraphe 1, paragraphe 3, point b) et paragraphe 4 du RGPD, en 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. Sous réserve de l'autorisation de l'autorité de contrôle compétente (ci-après l'«AC compétente»), les garanties appropriées peuvent être fournies, notamment, par des dispositions intégrées dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

(2) Compte tenu des caractéristiques spécifiques des arrangements administratifs prévus à l'article 46, paragraphe 3, point b)[1], qui peuvent varier considérablement, il convient d'examiner chaque cas individuellement, sans préjudice de l'évaluation de tout autre arrangement administratif.

(3) En application de l'article 70, paragraphe 1, du RGPD, le comité européen de la protection des données (ci-après le « CEPD ») veille à l'application cohérente du RGPD dans l'ensemble de l'Espace économique européen. En vertu de l'article 64, paragraphe 2, le mécanisme de contrôle de la cohérence peut être déclenché par une autorité de contrôle, le président du comité ou la Commission pour toute question d'application générale ou produisant des effets dans plusieurs États membres. Le CEPD émet alors un avis sur la question qui lui est soumise, à condition qu'il n'ait pas déjà émis un avis sur la même question.

(4) Conformément à l'article 64, paragraphe 3, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur du CEPD, l'avis du CEPD est adopté dans un délai de huit semaines après que le président a décidé que le dossier était complet. Sur décision de la présidente du CEPD, ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

(5) En vertu de l'article 65, paragraphe 1, point c), du RGPD, lorsqu'une AC compétente ne suit pas l'avis du CEPD émis en vertu de l'article 64, toute autorité de contrôle concernée ou la Commission peut saisir le CEPD, qui adopte alors une décision contraignante,

[1] Voir également le considérant 108 du RGPD.

A ADOPTÉ L'AVIS SUIVANT:

1 RÉSUMÉ DES FAITS

1. À la suite de plusieurs séries de discussions, l'Autorité européenne des marchés financiers (ESMA), agissant en qualité de facilitateur pour les autorités de surveillance financière (autorités nationales compétentes, ci-après «ANC») de l'EEE et en sa propre qualité, et l'Organisation internationale des commissions de valeurs (OICV) ont présenté, par lettre officielle, le projet d'arrangement administratif (ci-après le «projet d'AA») ci-joint, conformément à l'article 46, paragraphe 3, point b), du RGPD, afin de définir le cadre des transferts de données à caractère personnel des ANC de l'EEE (et de l'ESMA elle-même) vers leurs homologues hors EEE. Ce projet d'AA a été communiqué à la présidente du CEPD le 2 janvier 2019.

2. À la suite de cette transmission, la présidente du CEPD a demandé au comité d'émettre un avis en vertu de l'article 64, paragraphe 2, du RGPD. La décision relative au caractère complet du dossier a été prise le 15 janvier 2019.

2 ÉVALUATION

3. Le projet d'AA peut être utilisé par toutes les autorités de réglementation des marchés dans l'EEE et soumis aux AC compétentes pour autorisation. En conséquence, la question produit des effets dans plusieurs États membres au sens de l'article 64, paragraphe 2, du RGPD.

4. Le projet d'AA est nécessaire pour garantir une coopération internationale efficace entre ces autorités, agissant en leur qualité d'autorités publiques, d'autorités de réglementation et/ou de surveillance des marchés de valeurs mobilières et/ou d'instruments dérivés, afin de «protéger les investisseurs ou les clients et de renforcer l'intégrité des marchés de valeurs mobilières et d'instruments dérivés ainsi que la confiance dont ces marchés jouissent» conformément à leurs missions, telles que définies par la législation applicable.

5. Lors de l'évaluation des dispositions figurant dans ce projet d'AA précis, le CEPD a pris en considération un certain nombre d'éléments spécifiques pour apprécier les risques éventuels liés aux transferts de données à caractère personnel, dont le type de données à caractère personnel couvert par l'AA et les objectifs poursuivis.

6. Le projet d'AA, dont le texte intégral figure en annexe, comprend les garanties mentionnées ci-dessous.

   - **Définitions de notions figurant dans le RGPD et droits des personnes concernées :** la section II de l'AA contient les définitions nécessaires pour établir le champ d'application de l'AA et son application cohérente. Parmi elles figurent certaines définitions de notions et droits clés du

cadre juridique européen en matière de protection des données, tels que «données à caractère personnel», «traitement», «violation de données à caractère personnel», «droit d'accès» et «droit à l'effacement», qui correspondent aux définitions contenues dans le RGPD.

- **Principe de limitation des finalités et interdiction de toute utilisation ultérieure :** la section III.1 de l'AA part du principe que les autorités ont des responsabilités et des missions réglementaires spécifiques, qui consistent notamment à protéger les investisseurs ou les clients et à renforcer l'intégrité des marchés de valeurs mobilières et d'instruments dérivés ainsi que la confiance dont ces marchés jouissent. Conformément au principe de limitation des finalités, les transferts ne peuvent donc avoir lieu que dans le cadre de ces missions et responsabilités, à savoir si cela est nécessaire pour soutenir leurs tâches institutionnelles, et l'autorité qui reçoit les données à caractère personnel (ci-après l'«autorité destinataire») ne sera pas autorisée à les traiter ultérieurement d'une manière incompatible avec ces finalités.

- **Principe de qualité et de proportionnalité des données :** conformément à la section III.2 de l'AA, l'autorité qui transfère les données à caractère personnel (ci-après l'«autorité de transfert») transférera uniquement des données à caractère personnel exactes et à jour qui sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont transférées et traitées ultérieurement. Si une autorité se rend compte que les données à caractère personnel transférées sont incorrectes, elle en avisera l'autre autorité. Eu égard aux finalités pour lesquelles les données à caractère personnel ont été transférées et traitées ultérieurement, chaque autorité complétera, effacera, bloquera, corrigera ou rectifiera d'une autre manière les données à caractère personnel, comme il conviendra.

- **Principe de transparence :** chaque autorité adressera aux personnes concernées un avis général contenant des informations relatives au traitement effectué (y compris le transfert), au type d'entités auxquelles les données peuvent être transférées, aux droits dont les personnes concernées disposent en vertu des exigences légales applicables (y compris la manière d'exercer ces droits), ainsi qu'à tout délai ou toute restriction applicable concernant l'exercice de ces droits, et précisant les coordonnées à utiliser pour la soumission d'un litige ou l'introduction d'une réclamation. Chaque autorité publiera cet avis sur son site internet, avec l'AA. En outre, les personnes concernées seront avisées individuellement par les autorités de l'EEE selon les modalités définies dans le RGPD et, dans le cas de l'ESMA, conformément à ce que prévoit le règlement 2018/1725.

- **Principe de conservation des données :** comme indiqué à la section III.7 de l'AA, les autorités conserveront les données à caractère personnel pendant une durée n'excédant pas celle nécessaire au regard de la finalité pour laquelle elles sont traitées, conformément à la législation applicable.

- **Mesures de sécurité et de confidentialité :** la section III.4 prévoit que chaque autorité destinataire dispose de mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel qui lui sont transférées contre l'accès, la destruction, la perte, la modification ou la divulgation non autorisée, de manière accidentelle ou illicite, comprenant, par exemple, le marquage d'informations en tant que données à caractère personnel et la restriction de l'accès aux données à caractère personnel.

  L'AA prévoit également que, si une autorité destinataire prend connaissance d'une violation de données à caractère personnel, elle en informe le plus rapidement possible l'autorité de transfert et utilise des moyens raisonnables et appropriés pour remédier à cette violation et réduire autant que possible les éventuelles conséquences négatives.

- **Garanties relatives aux droits des personnes concernées :** la section III.5 de l'AA prévoit des garanties relatives aux droits des personnes concernées. Les personnes concernées peuvent savoir si leurs données ont été transférées à une autre autorité de surveillance financière hors EEE (autorité compétente d'un pays tiers, ci-après «ACT»). Elles auront également accès, sur demande, à leurs données à caractère personnel. En outre, elles peuvent s'adresser directement à l'ANC ou à l'ACT concernée pour demander la rectification, l'effacement, la limitation ou le blocage de leurs données. Les informations relatives à ces garanties doivent être fournies sur le site web de l'ANC/ACT. Toute restriction à ces droits doit être prévue par la loi et n'est autorisée que dans la mesure où c'est nécessaire, et uniquement pendant la durée requise, pour protéger la confidentialité ou pour atteindre un objectif important d'intérêt public général. Lorsque l'autorité de transfert est une ANC de l'EEE, ledit objectif doit être reconnu par l'État membre de cette ANC (il peut s'agir, par exemple, de prévenir une atteinte aux fonctions de surveillance/d'exécution).

- **Restrictions concernant les transferts ultérieurs :** les transferts ultérieurs vers un tiers d'un autre pays qui n'est pas une autorité participant à l'AA et ne fait pas l'objet d'une décision d'adéquation de la Commission européenne auront lieu uniquement avec le consentement écrit préalable de l'autorité de transfert et si le tiers donne des assurances appropriées qui sont compatibles avec les garanties prévues par l'AA.

  Les mêmes garanties sont prévues pour la communication de données à caractère personnel à un tiers situé dans le même pays que l'autorité destinataire sauf si, dans des cas exceptionnels, le tiers en question ne peut pas donner les assurances susmentionnées. Dans ce cas, le transfert ne peut avoir lieu que si la communication des données répond à «des motifs importants d'intérêt public». Lorsque l'autorité de transfert est une ANC de l'EEE, cet intérêt public doit être reconnu par l'État membre de cette ANC.

  La communication de données à caractère personnel à un tiers situé dans le même pays que l'autorité destinataire (organismes publics, juridictions, organismes d'autoréglementation, parties à une procédure d'exécution, etc.) en l'absence de consentement de l'autorité de transfert ou d'assurances appropriées n'est possible que dans les deux cas suivants :

  i) si la finalité pour laquelle les données à caractère personnel sont communiquées puis utilisées est compatible avec la finalité pour laquelle les données ont été initialement transférées ou avec le cadre général d'utilisation défini dans la demande spécifique initiale de l'autorité destinataire, et que la communication des données est nécessaire pour que l'autorité destinataire et/ou le tiers puisse s'acquitter de ses missions et de ses responsabilités ;

  ii) lorsque la communication de données à caractère personnel fait suite à une demande juridiquement exécutoire ou est requise par la loi. L'autorité destinataire avisera l'autorité de transfert avant la communication des données, en lui transmettant des informations sur les données demandées, l'organe demandeur et la base juridique de la communication des données. L'autorité destinataire fera tout ce qui est en son pouvoir pour limiter la communication des données à caractère personnel reçues au titre de l'AA, notamment en faisant valoir l'ensemble des prérogatives et dérogations juridiques applicables.

- **Voies de recours :** la section III 8. de l'AA prévoit un mécanisme de recours. Ce mécanisme est mis en place pour garantir le droit d'obtenir réparation et, le cas échéant, une indemnisation. En cas de non-respect de l'AA, y compris de violation des droits des personnes concernées, un recours peut être exercé devant une instance compétente (par exemple, une juridiction). Le

recours formé devant une telle instance compétente sera conforme aux exigences légales applicables, de telle manière que la personne concernée puisse effectivement faire valoir les droits liés aux principes et aux garanties prévus par l'AA. L'autorité de transfert sera informée de tout litige ou réclamation, et les autorités des deux parties mettront tout en œuvre pour régler le litige ou la réclamation à l'amiable. Si le problème ne peut pas être résolu de la sorte, il sera recouru à d'autres méthodes, notamment des mécanismes de médiation ou de règlement des litiges non contraignants. Si l'autorité de transfert estime qu'une autorité destinataire n'a pas agi en conformité avec les garanties énoncées dans l'AA, par exemple parce qu'elle n'a pas suivi la décision prise dans le cadre du mécanisme de médiation ou d'un autre mécanisme non contraignant de règlement des litiges, elle suspendra tout transfert de données au titre de l'AA à l'autorité destinataire jusqu'à ce que la question soit réglée de manière satisfaisante. En outre, la question sera portée à la connaissance du «groupe d'évaluation» (ainsi que de toutes les autres autorités). Si celui-ci établit qu'il y a eu «une modification démontrée de la volonté ou de la capacité [de l'autorité destinataire] d'agir en conformité avec [l'AA]», il peut recommander qu'il soit mis fin à la participation de l'autorité destinataire à l'AA. Afin de permettre aux personnes concernées d'exercer leur droit de recours, l'AA sera rendu public.

- **Mécanisme de surveillance :** la section IV de l'AA prévoit un mécanisme de surveillance externe assurant la mise en œuvre des garanties prévues par l'AA. Ce mécanisme de surveillance consiste en une combinaison d'examens périodiques réalisés par le «groupe d'évaluation» et d'examens périodiques effectués par chaque ANC/ACT sur le plan interne. La combinaison de la surveillance externe et de la surveillance interne ainsi que les éventuelles conséquences des conclusions négatives d'un examen – comme la recommandation de suspendre la participation d'une autorité à l'AA – assurent un niveau de protection satisfaisant.

7. Le CEPD salue les efforts ayant conduit à l'élaboration de cet AA multilatéral, qui comprend un certain nombre de garanties importantes en matière de protection des données. Pour que ces garanties permettent de faire en sorte qu'un niveau approprié de protection des données soit maintenu lorsque des données sont transférées vers un pays tiers au titre de cet AA et compte tenu du caractère particulier de tels accords non contraignants, le CEPD souligne ce qui suit :

8. Chaque AC compétente contrôlera l'AA et son application pratique – en particulier en ce qui concerne les sections III.5., III.6, III.8. et IV relatives aux droits des personnes concernées, aux transferts ultérieurs, aux voies de recours et au mécanisme de surveillance – afin de veiller à ce que les personnes concernées bénéficient de droits effectifs et opposables et de voies de recours appropriées et à ce que le respect de l'AA fasse l'objet d'une surveillance efficace.

9. Chaque AC compétente n'autorisera cet AA qu'à titre de garde-fou adéquat en matière de protection des données aux fins du transfert transfrontalier de données, sous réserve du respect intégral de toutes les dispositions de l'AA par les signataires.

10. Chaque AC compétente suspendra les flux de données effectués par l'ANC de son État membre conformément à l'autorisation, si l'AA n'offre plus de garanties appropriées au sens du RGPD.

3 CONCLUSIONS/RECOMMANDATIONS

11. Compte tenu de ce qui précède et des engagements que les ANC, l'ESMA et leurs homologues hors EEE s'engageront à respecter en signant cet AA afin de disposer «*de garanties appropriées pour le traitement de ces données à caractère personnel dans l'exercice de leurs responsabilités et de leurs missions réglementaires respectives*» et d'«*agir en conformité avec [cet] arrangement*», le CEPD estime que l'AA offre des garanties appropriées pour les transferts de données à caractère personnel, sur la base de cet AA, à des organismes publics de pays tiers qui ne font pas l'objet d'une décision d'adéquation de la Commission européenne.

12. Conformément au préambule de l'AA, reconnaissant l'importance d'un dialogue régulier entre les ANC de l'EEE et leurs AC compétentes, ou le contrôleur européen de la protection des données dans le cas de l'ESMA, et afin de permettre aux AC compétentes de mener à bien leur mission consistant, en application de l'article 57, paragraphe 1, point a), du RGPD, à contrôler l'application du RGPD et à veiller au respect de celui-ci, l'autorisation adoptée par l'AC compétente devrait prévoir que chaque signataire (ANC de l'EEE ou ESMA) informera l'AC compétente concernée de toute suspension des transferts de données à caractère personnel fondée sur les sections III 8. et IV de l'AA, ainsi que de toute révision ou cessation de la participation à l'AA reposant sur la section V.

13. En outre, le CEPD rappelle que, conformément au principe de responsabilité, chaque ANC et l'ESMA devront conserver les informations pour faciliter la mission de contrôle des AC. Ces informations devraient, en tout état de cause, être mises à disposition si l'AC compétente en fait la demande. Chaque AC peut également prévoir, dans son autorisation, que ces informations lui soient transmises chaque année par les ANC ou l'ESMA, sans demande préalable en ce sens. Ces informations devraient comprendre des indications sur le nombre de demandes et de réclamations introduites par des personnes concernées au niveau de l'UE, des renseignements sur les cas que les mécanismes de règlement des litiges proposés n'ont pas permis de résoudre, ainsi que sur les conclusions tirées par le «groupe d'évaluation» à la suite des examens périodiques et sur les mesures prises en conséquence, notamment celles relatives à la communication de données à caractère personnel au titre de la section III.6.2.(3) de l'AA. Il convient également de consigner des informations sur les notifications reçues par les ANC concernant la communication de données à un tiers par l'ACT, laquelle communication fait suite à une demande juridiquement exécutoire ou est requise par la loi.

4 REMARQUES FINALES

14. Le présent avis sera rendu public conformément à l'article 64, paragraphe 5, point b), du RGPD.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)