



AVIS DU CEPD SUR LA BASE JURIDIQUE DES TRANSFERTS DE DONNÉES À CARACTÈRE PERSONNEL VERS L'INSTITUT UNIVERSITAIRE EUROPÉEN (dossier 2020-0880)

1. INTRODUCTION

- Le présent avis porte sur la consultation de la Cour des comptes européenne (la «Cour des comptes») au sujet de la base juridique des transferts de données à caractère personnel vers l'Institut universitaire européen.
- Le CEPD émet le présent avis conformément à l'article 57, paragraphe 1, point g), et à l'article 58, paragraphe 3, point c), du règlement (UE) 2018/1725¹ (le «règlement»).

2. DESCRIPTION DES FAITS

La Cour des comptes souhaite signer un contrat avec l'Institut universitaire européen pour la dispense de formations. Le délégué à la protection des données de la Cour des comptes a demandé au CEPD quelle était la base juridique applicable et les éventuelles garanties en matière de protection des données pour les personnes concernées et les parties à un tel contrat.

3. ANALYSE JURIDIQUE

a) Relation entre responsable du traitement et sous-traitant ou entre responsables conjoints du traitement

Dans sa demande de consultation, le délégué à la protection des données (le «DPD») a indiqué que la Cour des comptes et l'Institut universitaire européen seraient des responsables conjoints du traitement conformément à un projet de contrat relatif à la dispense de formations. Cependant, dans les explications complémentaires fournies, il a été précisé que les formations seraient organisées par l'Institut universitaire européen, tandis que la Cour des comptes déciderait des membres du personnel qui participeront aux formations et des formations qui

¹ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

présentent un intérêt pour la Cour. Cela laisse à penser que la Cour des comptes déterminerait seule la finalité et les moyens du traitement des données à caractère personnel des membres de son personnel. En conséquence, le CEPD encourage la Cour des comptes à vérifier attentivement le rôle éventuel du responsable du traitement et du sous-traitant entre les deux parties.

Si, dans les faits, il s'agit plutôt d'une relation entre responsable du traitement et sous-traitant, cela doit être clairement stipulé dans un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie les parties. À la lumière de l'article 29² du règlement, la Cour des comptes, en tant que responsable du traitement, devrait veiller à ce que le contrat (ou un autre acte juridique) conclu avec l'Institut universitaire européen mentionne les obligations, les rôles et les tâches clairs et précis des parties respectives en ce qui concerne la protection des données, ainsi que toutes les exigences visées à l'article 29, paragraphe 3, du règlement.

Par ailleurs, s'il s'agit d'une relation entre responsables conjoints du traitement, la Cour des comptes et l'Institut universitaire européen doivent clairement recenser et définir leurs responsabilités respectives au regard de leurs obligations spécifiques au titre du règlement. À cette fin, ils doivent conclure un arrangement spécifique, dont les grandes lignes sont mises à la disposition des personnes concernées conformément à l'article 28 du règlement.

b) Transfert des données à caractère personnel vers une organisation internationale

L'Institut universitaire européen est une organisation internationale créée par la convention portant création de l'Institut universitaire européen³ signée par les États membres de l'UE. En tant qu'organisation internationale, l'Institut universitaire européen n'applique pas directement le cadre juridique européen en matière de protection des données, mais applique le règlement intérieur – la décision du président n° 10/2019 du 18 février 2019⁴, qui est rédigée conformément aux principes énoncés dans la convention portant création de l'Institut universitaire européen, signée le 19 avril 1972, et au protocole sur les privilèges et immunités qui y est annexé.

La coopération entre la Cour des comptes et l'Institut universitaire européen concernant la dispense de formations implique que certaines données à caractère personnel devraient être transférées d'une institution européenne vers une organisation internationale.

Le chapitre V du règlement prévoit des mécanismes et conditions spécifiques pour permettre les transferts de données à caractère personnel par des institutions et organes de l'UE vers un pays tiers ou une organisation internationale. Ces mécanismes et conditions visent à garantir que le niveau de protection des personnes physiques assuré par la législation de l'UE en matière de protection des données ne soit pas compromis.

Le premier mécanisme consiste en l'adoption par la Commission européenne d'une décision

² Voir les [lignes directrices du CEPD](#) du 7 novembre 2019 sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725 (les «lignes directrices du CEPD»).

³ Convention portant création de l'Institut universitaire européen:

<https://www.eui.eu/Documents/AboutEUI/Convention/Consolidated-Convention-following-UK-exit.pdf>

⁴ Décision n° 10/2019 du président:

<https://www.eui.eu/Documents/AboutEUI/Organization/DataProtection/PresDecision10-2019-DataProtection.pdf>

d'adéquation reconnaissant que le pays tiers ou une organisation internationale offre une norme en matière de protection des données qui est essentiellement équivalente à celle de l'UE⁵. Or, jusqu'à présent, la Commission européenne n'a adopté aucune décision d'adéquation concernant les organisations internationales.

En l'absence d'une décision d'adéquation, un transfert peut avoir lieu moyennant la fourniture de garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives⁶. Un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics peut prévoir de telles garanties appropriées⁷. Ces garanties peuvent aussi être fournies, sous réserve de l'autorisation du CEPD, par des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées⁸.

Si un transfert de données à caractère personnel est envisagé vers un pays tiers ou une organisation internationale qui ne fait pas l'objet d'une décision d'adéquation et si des garanties appropriées font défaut, un transfert peut être effectué sur la base d'un certain nombre de dérogations s'appliquant dans des situations particulières⁹. Toutefois, les exportateurs de données devraient tout d'abord s'efforcer d'encadrer le transfert par l'un des mécanismes offrant des garanties appropriées¹⁰. Qui plus est, l'institution de l'UE doit informer le CEPD des catégories de cas dans lesquels des dérogations ont été appliquées¹¹.

S'agissant des échanges récurrents et structurels de données à caractère personnel avec les autorités publiques, comme dans le cas du texte type envisagé, le CEPD estime que les accords internationaux contraignants¹² ou les arrangements administratifs constituent les instruments de transfert pertinents à utiliser¹³.

Une liste de garanties minimales figure dans les lignes directrices du comité européen de la protection des données adoptées le 18 janvier 2020 concernant l'article 46, paragraphe 2, point a), et l'article 46, paragraphe 3, point b), du RGPD¹⁴ pour les transferts de données à caractère personnel entre autorités et organismes publics de l'EEE et de pays tiers¹⁵. Il convient toutefois de noter que ces lignes directrices sont en cours de révision par le comité européen de la protection des données afin de tenir dûment compte de l'arrêt Schrems II¹⁶ de la Cour de justice de l'Union européenne. Le CEPD a également adopté une [décision](#)¹⁷ sur les garanties à

⁵ Article 47 du règlement.

⁶ Article 48, paragraphe 1, du règlement.

⁷ Article 48, paragraphe 2, point a), du règlement.

⁸ Article 48, paragraphe 3, point b), du règlement.

⁹ Article 50 du règlement.

¹⁰ Les dérogations ne devraient pas permettre les transferts récurrents, massifs et structurels (voir, par analogie, le considérant 72 du RGPD sur les transferts fondés sur des dérogations).

¹¹ Article 48, paragraphe 6, du règlement.

¹² Article 48, paragraphe 2, point a), du règlement.

¹³ Article 48, paragraphe 3, point b), du règlement.

¹⁴ Ces dispositions correspondent à l'article 48, paragraphe 2, point a), et à l'article 48, paragraphe 3, point b), du règlement.

¹⁵ [Lignes directrices 02/2020 du comité européen de la protection des données](#) concernant l'article 46, paragraphe 2, point a), et l'article 46, paragraphe 3, point b), du règlement 2016/679 pour les transferts de données à caractère personnel entre autorités et organismes publics de l'EEE et de pays tiers (les «lignes directrices du comité européen de la protection des données»).

¹⁶ [Affaire C-31/18](#).

¹⁷ Décision du CEPD du 13 mars 2019 concernant le recours à l'arrangement administratif IOSCO-ESMA par l'Autorité européenne des marchés financiers (la «décision du CEPD»).

intégrer dans un arrangement administratif pour les transferts de données à caractère personnel entre une agence de l'UE et une organisation internationale, conformément à l'article 48, paragraphe 3, point b), du règlement. Veuillez également noter que le réseau des DPD travaille actuellement sur un projet de modèle d'arrangement administratif.

Sur la base des lignes directrices susmentionnées du comité européen de la protection des données et de la décision du CEPD, l'arrangement administratif entre la Cour des comptes et l'Institut universitaire européen devrait prévoir les garanties suivantes:

- **les définitions des concepts et droits fondamentaux** du cadre juridique européen en matière de protection des données, par exemple, les données à caractère personnel, les transferts ultérieurs, le partage de données à caractère personnel, la violation de données à caractère personnel, le traitement, le secret professionnel, le profilage, les droits des personnes concernées mentionnant le droit d'accès, le droit de rectification, le droit à l'effacement, le droit à l'information, le droit d'opposition ou le droit de limitation du traitement, qui sont conformes aux définitions exposées dans le règlement;
- **le principe de limitation de la finalité et d'interdiction de toute utilisation ultérieure:** une partie destinataire ne devrait traiter des données qu'aux fins pour lesquelles les données ont été échangées et tout traitement ultérieur incompatible avec la finalité initiale de l'échange de données devrait être interdit;
- **le principe de qualité et de proportionnalité des données:** une partie qui transfère ne devrait transférer que des données à caractère personnel exactes et à jour qui sont adéquates, pertinentes et limitées à ce qui est nécessaire pour atteindre la finalité pour laquelle elles sont transférées et traitées ultérieurement. Chaque partie devrait informer l'autre partie si elle constate que les données à caractère personnel transférées sont incorrectes. En tenant compte des finalités pour lesquelles les données à caractère personnel ont été transférées et traitées ultérieurement, chaque partie devrait compléter, effacer, verrouiller, corriger ou rectifier de toute autre manière les données à caractère personnel, selon le cas;
- **le principe de transparence:** un avis général devrait être communiqué aux personnes concernées en ce qui concerne le traitement effectué, y compris le transfert, le type d'entités auxquelles les données sont susceptibles d'être transférées, les droits dont elles disposent en vertu des exigences légales applicables, y compris les modalités d'exercice de ces droits et les informations sur toute restriction applicable à l'exercice de ces droits, les mécanismes de recours disponibles et les coordonnées pour introduire un litige ou une réclamation. L'arrangement administratif devrait expliquer la manière dont cette notification devrait être transmise aux personnes concernées et si une notification individuelle doit être fournie;
- **le principe de conservation des données:** les données à caractère personnel ne devraient pas être conservées plus longtemps que nécessaire à la finalité pour laquelle elles sont traitées conformément à la législation, aux règlements et/ou à la réglementation applicables régissant la conservation de ces données;
- **les mesures de sécurité et de confidentialité:** des mesures de sécurité administratives, techniques et physiques appropriées devraient être prises, y compris, par exemple, le marquage des informations en tant que données à caractère personnel, la limitation de l'accès aux données à caractère personnel, la fourniture d'un stockage sécurisé des données à caractère personnel ou la mise en œuvre de politiques visant à garantir la sécurité et la confidentialité des données à caractère personnel. L'arrangement devrait également prévoir des procédures pour les cas de violation des données à caractère personnel et disposer que si une partie destinataire a connaissance d'une violation des données à caractère personnel, elle doit en informer une partie à l'origine du transfert dans les meilleurs délais et utiliser des moyens raisonnables et appropriés pour remédier à la violation des données à caractère personnel et réduire au minimum les effets néfastes potentiels;

- **les garanties relatives aux droits des personnes concernées:** les personnes concernées devraient pouvoir obtenir la confirmation que leurs données ont été transférées. Les personnes concernées devraient également avoir accès, sur demande, à leurs données à caractère personnel. En outre, les personnes concernées peuvent demander à ce que leurs données soient corrigées, effacées, verrouillées ou limitées et, le cas échéant, devraient pouvoir exercer leur droit de s'opposer au traitement des données pour des motifs liés à leur situation particulière. Toute limitation de ces droits doit être prévue par la loi et n'est autorisée que dans la mesure où, et aussi longtemps que, cela est nécessaire pour protéger la confidentialité en vertu du secret professionnel ou d'autres obligations légales;
- **les restrictions applicables aux transferts ultérieurs:** les transferts ultérieurs à un tiers dans un autre pays qui n'est pas couvert par une décision d'adéquation adoptée par la Commission européenne ne peuvent avoir lieu qu'avec l'accord écrit préalable d'une partie qui transfère et si le tiers fournit des garanties appropriées compatibles avec les garanties prévues dans l'arrangement administratif;
- **les voies de recours:** les personnes concernées devraient être en droit d'obtenir réparation et, le cas échéant, de percevoir une indemnisation. L'arrangement administratif devrait prévoir des mécanismes alternatifs de règlement des différends en l'absence de recours juridictionnel pour une organisation internationale qui signe l'arrangement. Parmi ces autres méthodes peuvent figurer des procédures de médiation ou des procédures de règlement des différends. Des dispositions devraient également permettre la suspension des transferts de données dans le cas où une partie qui les transfère estime qu'une partie destinataire n'a pas agi, dans le cadre de réclamations ou de différends, conformément aux garanties énoncées dans l'arrangement de travail. L'arrangement administratif devrait prévoir que les parties s'informent mutuellement des litiges ou réclamations en lien avec l'arrangement et mettent tout en œuvre pour les régler à l'amiable en temps utile. Des mécanismes de recours devraient également être disponibles en cas de violations présumées des données. Les situations dans lesquelles une organisation internationale n'est pas en mesure de mettre en œuvre les garanties prévues par l'arrangement devraient également être couvertes. En pareils cas, l'institution de l'Union européenne devrait en être informée sans délai et les transferts devraient être suspendus jusqu'à ce que les garanties prévues par l'arrangement puissent être mises en œuvre;
- **le mécanisme de surveillance:** ce mécanisme devrait consister en une combinaison d'examen périodiques réalisés en externe et en interne par chaque partie. La combinaison de la surveillance externe et interne et des conséquences possibles adoptées à la suite d'un examen négatif – qui peut inclure une recommandation de suspendre la participation aux arrangements administratifs – garantit un niveau de protection satisfaisant. Le CEPD recommande également que l'arrangement administratif inclue l'engagement volontaire de la partie destinataire à coopérer avec le CEPD en tant qu'autorité de contrôle de la Cour des comptes. Si cela n'est pas possible, une surveillance indépendante pourrait être garantie au moyen de mécanismes autonomes sur le plan fonctionnel. Dans ce dernier cas, il doit s'agir d'un organisme qui, tout en n'étant pas extérieur, exerce ses fonctions de manière indépendante, c'est-à-dire exempt d'instructions et avec des ressources humaines, techniques et financières suffisantes.

Compte tenu du fait que la décision n° 10/2019 du président de l'Institut universitaire européen relative à la protection des données¹⁸ se fonde dans une large mesure sur le cadre juridique européen en matière de protection des données, il semble que la plupart des garanties énumérées ci-dessus (principes de protection des données, sécurité, droits des personnes

¹⁸ Décision n° 10/2019 du président:
<https://www.eui.eu/Documents/AboutEUI/Organization/DataProtection/PresDecision10-2019-DataProtection.pdf>

concernées, certaines définitions de concepts clés) y soient déjà mentionnées. Cependant, d'autres garanties doivent encore être établies, en particulier celles concernant les restrictions applicables aux transferts ultérieurs, les voies de recours (y compris des précisions supplémentaires sur le recours juridictionnel par l'organe de première instance) et le mécanisme de surveillance.

4. CONCLUSION

Compte tenu de ce qui précède, le CEPD recommande à la Cour des comptes et à l'Institut universitaire européen de clarifier les rôles respectifs des deux parties dans le traitement des données à caractère personnel et de rédiger l'arrangement administratif approprié en tenant compte des garanties exposées dans la présente lettre. Conformément à l'article 48, paragraphe 3, du règlement, l'arrangement administratif doit recevoir l'autorisation du CEPD.

Bruxelles, 12 novembre 2020

Wojciech Rafał WIEWIÓROWSKI

(e-signed)