LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne

Document d'orientation

Bruxelles, le 14 juillet 2014

Synthèse

Le présent document offre une orientation aux institutions et organes de l'Union européenne concernant l'interprétation et l'application des règles fixées par le règlement (CE) n° 45/2001 dans le contexte des transferts internationaux de données à caractère personnel.

Les institutions et organes de l'Union ont de plus en plus souvent besoin de transférer des données à caractère personnel à des pays tiers ou à des organisations internationales pour diverses raisons, y compris aux fins de la coopération transfrontalière et de l'utilisation de services transnationaux.

Le «principe de protection adéquate» (article 9, paragraphes 1 et 2) doit être respecté dans le cadre des transferts internationaux de données. Ce principe exige que le droit fondamental à la protection des données soit garanti, y compris lorsque des informations à caractère personnel sont transférées en dehors de l'Union ou à des organismes qui ne sont pas soumis au droit de l'Union. Les responsables du traitement devraient analyser le niveau de protection offert par le destinataire des données; son caractère adéquat devrait être déterminé sur la base de la nature des règles applicables en matière de protection des données dans le lieu de destination et des moyens permettant de garantir leur application effective (supervision et mise en application).

Lorsque la Commission européenne adopte une «décision d'adéquation» (article 9, paragraphe 5), il n'est pas nécessaire de procéder à une nouvelle analyse du caractère adéquat de la protection. Les transferts sont également autorisés lorsque le responsable du traitement met au point des mécanismes spécifiques offrant des garanties suffisantes (article 9, paragraphe 7). Enfin, les transferts ne présentant pas de garanties spéciales sont autorisés dans des circonstances exceptionnelles, pour autant qu'une dérogation spécifique soit applicable (article 9, paragraphe 6).

Lorsque des institutions ou organes de l'Union sont tenus par la législation européenne ou par des accords bilatéraux d'effectuer des transferts internationaux, en agissant en qualité de responsables du traitement, et que le pays de destination n'est pas considéré comme adéquat par la Commission, l'instrument devrait, idéalement, prévoir les mesures suffisantes et nécessaires pour garantir la conformité avec l'article 9 du règlement. À cette fin, il convient de consulter le CEPD, conformément à l'article 28, paragraphe 2, du règlement, avant d'adopter ce type d'instrument juridique.

Le CEPD peut intervenir, dans le cadre d'une fonction de surveillance, en fonction des modalités du transfert, en particulier lorsqu'il n'est pas consulté ou ne donne pas d'autorisation préalable alors qu'il était raisonnable de s'attendre à ce que ces procédures aient lieu. Le CEPD peut également procéder à des contrôles ou faire usage de ses pouvoirs de mise en application, le cas échéant.

Sommaire

Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne

1. Introduction

Dans le cadre de leurs missions, les institutions et organes de l'Union européenne ont de plus en plus souvent besoin de transférer des données à caractère personnel à des pays tiers[1] ou à des organisations internationales pour diverses raisons, y compris aux fins de la coopération transfrontalière[2] et de l'utilisation de services transnationaux[3]. L'évolution rapide de la technologie, et notamment de l'informatique en nuage et des applications mobiles[4], crée de nouveaux défis, auxquels il convient d'apporter une réponse pour veiller à ce que les droits fondamentaux des individus soient pleinement respectés. L'article 9 du règlement (CE) n° 45/2001 (ci-après le «règlement») fixe les règles applicables à ce type de transfert, à la lumière des articles 25 et 26 de la directive 95/46/CE (ci-après la «directive»).

Le présent document a pour objectif d'apporter une orientation technique et pratique aux responsables du traitement des données des institutions et organes de l'Union concernant l'interprétation et l'application de ces règles de transfert.

L'actuel cadre juridique de l'Union en matière de protection des données, et notamment la directive, est en cours de révision. Dans la proposition de la Commission européenne, les règles relatives aux transferts internationaux sont considérablement étoffées. Le chapitre V de la proposition peut être considéré comme une avancée positive vers une protection des données plus globale[5], puisqu'il décrit non seulement le principe de «protection adéquate»[6], mais qu'il introduit également davantage de flexibilité en instaurant des garanties suffisantes pour les transferts de

[1] Les pays qui ne sont pas membres de l'Espace économique européen (EEE).

[2] Voir les avis du CEPD sur la notification d'un contrôle préalable ci-après: enquêtes relatives à des fraudes au sein de la BEI (2009-0459), communication de rapports d'enquête sur le thon rouge (2011-0615), gel de fonds par la Commission (2010-0426), enquêtes internes et externes de l'OLAF (2005-418, 2007-47, 2007-48, 2007-49, 2007-50, 2007-72), opérations de retour conjointes coordonnées par Frontex (2009-0281), disponibles à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/priorchecking/OpinionsPC.

[3] Voir la consultation concernant le transfert de données à caractère personnel à destination d'American Express Corporate Travel SA (AMEX) – EFSA (2009-390), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Consultations/2010/10-12-21_EFSA_AMEX_FR.pdf; voir aussi la consultation sur la communication de données personnelles du personnel de la BEI à l'OCDE (2013-0089), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Consultations/2013/13-03-21_Consultation_EIB_FR.pdf.

[4] Une orientation spécifique relative à l'informatique en nuage et aux dispositifs mobiles est actuellement en préparation.

[5] Pour des observations détaillées du CEPD, voir l'avis du Contrôleur européen de la protection des données du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données (ci-après «l'avis du CEPD sur le paquet de mesures pour une réforme»), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_FR.pdf).

[6] Voir les articles 40 et 41 de la proposition.

données[7]. Ces dispositions élargissent les possibilités de recours à des solutions spécifiques (par exemple, des règles d'entreprise contraignantes), permettant d'accomplir des progrès significatifs en direction de solutions plus pragmatiques pour garantir la protection des individus.

L'actuel régime fixé par le règlement n'est pas encore directement affecté par la révision du cadre juridique relatif à la protection des données, bien que le CEPD ait suggéré que celui-ci soit, au moins, modifié afin qu'il s'applique de manière concomitante[8]. Le règlement continuera donc d'établir les règles relatives aux transferts internationaux pour les quelques années à venir. Néanmoins, le présent document analyse les modifications qui ont été proposées, le cas échéant.

Par exemple, il est très probable que le principe de responsabilité, qui est implicite dans les règles existantes, soit renforcé dans le nouveau cadre de protection des données. À la lumière de ces éléments, nous appliquons déjà ce principe en apportant des conseils concernant les obligations des institutions et organes de l'Union, conformément à notre politique relative aux consultations dans le domaine de la supervision et de la mise en application[9].

De ce fait, lorsqu'une institution ou un organe de l'Union transfère des données à caractère personnel conformément à l'article 9 du règlement, ceux-ci devraient veiller à respecter pleinement leurs obligations en vertu du règlement avant de procéder au transfert ou à l'ensemble de transferts. Le cas échéant, les responsables du traitement devraient consulter leurs délégués à la protection des données (DPD) dès le départ et solliciter leur conseil. Parallèlement, le CEPD a mis au point des orientations concernant l'interprétation et l'application des règles existantes[10], qui ont été communiquées à des responsables du traitement dans un certain nombre de cas concrets. Le présent document s'appuie sur cette expérience pour fournir des outils pratiques à l'intention des responsables du traitement, afin de les aider à déterminer la meilleure solution.

2. Aperçu général

Comme décrit plus en détail ci-dessous, l'article 9 du règlement établit le principe général de «protection adéquate». Il s'agit du principe fondamental s'appliquant à la circulation internationale de données, qui est également inscrit aux articles 25 et 26 de la directive. L'article 9 décrit aussi la manière dont il convient d'apprécier le niveau de protection offert par un pays tiers ou une organisation internationale, les obligations auxquelles le responsable du traitement est tenu pour informer la Commission ou le CEPD, ainsi que les dérogations s'appliquant au principe général[11].

[7] Voir les articles 42 et 43 de la proposition.
[8] Avis du CEPD sur le paquet de mesures pour une réforme (voir la note de bas de page 5).
[9] Politique relative aux consultations dans le domaine de la supervision et de la mise en application, 23 novembre 2012, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/12-11-23_Policy_on_Consultations_FR.pdf.
[10] Voir la liste des demandes de consultation soumises au CEPD à l'annexe 3.
[11] Voir le texte complet de l'article 9 à l'annexe 1.

Le principe de protection adéquate exige que le droit fondamental à la protection des données soit garanti, y compris lorsque des données à caractère personnel sont communiquées à une partie ne relevant pas du champ d'application du règlement et de la directive. Malgré la cohérence et une convergence croissantes des principes et des pratiques en matière de protection des données à travers le monde, il n'est pas possible de présumer une adéquation complète dans tous les cas. Souvent, le niveau de protection des données offert par les pays tiers et les organisations internationales est bien inférieur à celui de l'Union européenne, voire inexistant. C'est pourquoi, avant de procéder à un transfert vers un pays tiers ou une organisation internationale, le responsable du traitement des données devrait veiller à ce que les personnes concernées soient protégées de manière adéquate.

L'article 9, paragraphe 1, autorise les transferts de données à caractère personnel à des pays tiers et à des organisations internationales lorsqu'un niveau de protection adéquat est garanti. Des transferts sont également autorisés lorsque le responsable du traitement met au point des mécanismes spécifiques offrant des garanties suffisantes (article 9, paragraphe 7). Enfin, les transferts n'offrant pas de garanties spéciales sont autorisés dans des circonstances exceptionnelles, pour autant qu'une dérogation spécifique soit applicable (article 9, paragraphe 6)[12].

3. Questions préliminaires

3.1. Notion de «transfert de données à caractère personnel»

La notion de «transfert de données à caractère personnel» n'est définie ni dans la directive ni dans le règlement. Dans ce dernier, cette formule est aussi utilisée dans d'autres dispositions relatives à la circulation de données entre des institutions ou organes de l'Union ou en leur sein et aux transferts à des destinataires au sein de l'Union qui relèvent également de la directive[13]. Dans ces circonstances, il est possible de partir du principe que cette formule est utilisée dans son acception initiale, c'est-à-dire que les données «circulent» ou que leur «circulation» est autorisée entre différents utilisateurs. Dans la pratique toutefois, cette question n'est pas toujours si simple à traiter.

Le CEPD demande une définition de cette notion dans le cadre de la réforme de la protection des données[14], puisque celle-ci s'est révélée problématique dans certains cas, qui ont pour l'instant été laissés à l'appréciation de la Cour de justice ou du législateur.

Le seul exemple de jurisprudence de la Cour de justice dans laquelle la notion de «transfert» a été évoquée, l'affaire Lindqvist[15], n'a qu'une portée limitée. Cette décision analyse notamment si le *simple fait* d'inscrire des données à caractère personnel sur une page internet stockée auprès d'un hébergeur établi dans le même État membre (comme M^me^ Lindqvist) ou dans un autre État membre constitue un

[12] Une liste de contrôle rapide figure à l'annexe 2.
[13] Voir les articles 7 et 8 du règlement.
[14] Avis du CEPD sur le paquet de mesures pour une réforme (voir la note de bas de page 5), page 21, point 108.
[15] Affaire C-101/01, Lindqvist, Rec 2003, p. I-12971.

transfert au sens de l'article 25 de la directive. La Cour a conclu, au point 71, qu'il n'existait «*pas de "transfert vers un pays tiers de données" au sens de l'article 25 de la directive 95/46 lorsqu'une personne qui se trouve dans un État membre inscrit sur une page Internet, stockée auprès de son fournisseur de services d'hébergement qui est établi dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à Internet, y compris des personnes se trouvant dans des pays tiers*».

Cette conclusion de la Cour doit être replacée dans le contexte de l'affaire. La Cour a rendu son évaluation en tenant compte «*des circonstances telles que celles de l'espèce au principal*». Elle ne s'est pas exprimée sur d'autres types d'opérations de traitement – pouvant différer, par exemple, au niveau de leur échelle, de leur intention, de leur objectif, de leurs risques, etc. – au-delà de la seule inscription de données à caractère personnel sur une page internet dans les circonstances de l'affaire, dont l'objectif visé était par ailleurs très local (le souhait de M^{me} Lindqvist d'informer les autres membres de sa paroisse). Il convient donc de ne pas appliquer simplement et automatiquement la conclusion de la Cour relative à la notion de «transfert» à des affaires présentant des caractéristiques différentes.

Dans d'autres affaires, des données à caractère personnel sont manifestement communiquées à un destinataire situé dans un pays tiers, dans *l'intention* de mettre cette information à sa disposition. De même, dans d'autres affaires encore, des données à caractère personnel sont publiées sur l'internet dans *l'objectif* d'informer le grand public, non seulement au niveau local ou au sein de l'Union, mais également dans des pays tiers, comme c'est le cas pour le répertoire du personnel de la Commission qui est disponible en ligne. Ces affaires peuvent faire l'objet de traitements différents, comme nous le verrons[16], mais elles ont en commun le fait que certaines informations sont *délibérément* mises à disposition de destinataires situés dans un pays tiers et qu'elles vont au-delà de la simple inscription de cette information à des fins plus limitées.

Dans ce contexte, et bien qu'il n'existe pas encore de définition formelle du «transfert de données à caractère personnel», les responsables du traitement devraient considérer que cette expression renvoie normalement aux éléments suivants: *la communication, la divulgation ou la mise à disposition par d'autres moyens de données à caractère personnel par un expéditeur relevant du règlement et conscient que le ou les destinataires y auront accès ou agissant dans cette intention*[17].

Cette formule couvrirait donc tant les «transferts délibérés» que l'«accès autorisé» aux données par le ou les destinataires[18]. Les conditions de «conscience» et d'«intention» excluraient les cas où l'accès est obtenu grâce à une action illicite (par exemple, le

[16] Voir ci-dessous, à partir du point 6.

[17] Ces éléments ne s'appliqueraient pas seulement aux transferts à des pays tiers ou à des organisations internationales (article 9), mais aussi aux transferts entre institutions ou organes de l'Union ou en leur sein (article 7) et aux transferts à des destinataires relevant de la directive (article 8).

[18] Systèmes *push* et *pull*: il s'agit de deux méthodes différentes de communication sur l'internet. Dans le système «*push*», la communication est amorcée par celui qui publie ou par un serveur (responsable du traitement des données). Cette opération peut être considérée comme un «transfert délibéré» de données à caractère personnel. Dans le système «*pull*», la demande de transmission d'informations est d'abord soumise par le destinataire. Cette opération peut être considérée comme un «accès autorisé» à des données à caractère personnel.

piratage). Par ailleurs, le simple fait que des informations traversent des frontières pour atteindre leur destination, ou soient susceptibles de le faire, en raison de la manière dont les réseaux sont structurés ne relèverait pas automatiquement de cette notion.

Des transferts internationaux de données à caractère personnel peuvent donc se produire dans différents environnements (physiques et numériques), à l'instar des exemples ci-après:

– l'envoi de données à caractère personnel par une institution ou un organe de l'Union (responsable du traitement des données) à un destinataire d'un pays tiers par courrier postal ou électronique;

– l'envoi «*push*» de données à partir de la base de données d'un responsable du traitement des données de l'Union à un destinataire d'un pays tiers;

– l'octroi de l'accès à la base de données d'un responsable du traitement des données de l'Union («*pull*») à un destinataire d'un pays tiers;

– la collecte en ligne directe de données relatives à un individu au sein de l'Union lorsque le traitement est effectuée par un sous-traitant d'un pays tiers agissant pour le compte d'un responsable du traitement des données de l'Union;

– la publication de données à caractère personnel sur l'internet par un responsable du traitement des données de l'Union.

Le terme «transfert» inclurait donc également, en tout état de cause, certaines opérations de traitement visées à l'article 2, point b), du règlement, comme la «communication par transmission» et la «diffusion ou toute autre forme de mise à disposition». Ainsi, le «transfert de données à caractère personnel» devrait non seulement être conforme à l'article 9, mais aussi à d'autres dispositions applicables du règlement, comme celles relatives à la qualité des données et aux traitements licites (voir également le point 3.3 ci-dessous).

Au regard de l'état des discussions concernant cette notion et de son incidence sur des cas concrets, il est recommandé aux responsables du traitement des données de consulter le CEPD en cas de doute sérieux.

3.2. Champ d'application de l'article 9

L'article 9 s'applique aux transferts de données à caractère personnel à des destinataires (autres que les institutions et organes de l'Union) qui ne relèvent pas de la directive. Par conséquent, il ne couvre pas les destinataires établis dans les pays de l'Espace économique européen (EEE)[19], à moins que les transferts ne concernent des domaines exclus de la directive (anciens deuxième et troisième piliers du droit de l'Union; voir le point 7 ci-dessous).

[19] Les pays de l'EEE sont les États membres de l'Union et l'Islande, le Liechtenstein et la Norvège.

Le règlement contient – comme nous l'avons brièvement évoqué ci-dessus – deux autres dispositions relatives aux transferts: les articles 7 et 8. Ces deux dispositions n'ont pas d'équivalents dans la directive. L'article 7 s'applique au transfert de données à caractère personnel entre institutions de l'Union ou en leur sein. Ce serait le cas, par exemple, pour un transfert entre deux directions générales de la Commission situées à Bruxelles. Ce serait également le cas pour un transfert entre le Service européen pour l'action extérieure (SEAE) et l'une des délégations de l'Union à travers le monde (même si ces délégations sont établies dans des pays tiers, elles font partie des institutions de l'Union et relèvent donc du règlement). L'article 8 s'applique aux transferts à des destinataires autres que les institutions et organes de l'Union et relevant de la directive 95/46/CE.

Il convient de noter qu'après l'adoption du traité de Lisbonne, les références aux institutions et organes communautaires dans le règlement doivent être lues comme des références à des institutions et organes de l'Union (par exemple, à l'article 3). Tel n'est pas le cas pour les institutions ou organes qui sont actuellement soumis à un cadre juridique spécifique en matière de protection des données, comme Europol et Eurojust (voir le point 7 ci-dessous).

3.3. Respect d'autres conditions juridiques

Les transferts de données sont considérés comme des opérations de traitement et doivent donc être licites, conformément au chapitre II du règlement.

L'article 5 établit les différents motifs de traitement de données à caractère personnel. Par conséquent, avant qu'un transfert n'ait lieu, le responsable du traitement devrait déterminer si l'un des fondements juridiques établis est applicable. Cet examen repose sur deux étapes distinctes: a) l'opération de traitement précédant le transfert doit être licite (collecte, stockage, etc.) et b) le transfert lui-même doit l'être également (il doit avoir un fondement juridique satisfaisant et être cohérent par rapport à la finalité initiale du traitement).

Les responsables du traitement devraient également se conformer au principe de qualité des données (article 4). Celui-ci inclut des exigences relatives à la limitation des finalités des données transférées, à leur réduction à un minimum, à la limitation dans le temps de leur conservation et à leur exactitude.

D'autres dispositions pertinentes du règlement devraient également être respectées, telles que:

- l'interdiction générale de traiter certaines catégories spéciales de données, sauf lorsqu'une dérogation s'applique;
- l'obligation de fournir à la personne concernée des informations sur les destinataires;
- la conformité avec les droits de la personne concernée à toutes les étapes du processus de transfert, notamment les droits d'accès, de rectification et d'effacement avant que le transfert n'ait lieu;
- la sécurité du traitement (en évaluant le niveau du risque associé aux transferts et en adoptant des mesures appropriées en matière de sécurité et d'organisation);

- l'examen de la nécessité d'un contrôle préalable (voir le point 8 ci-dessous).

3.4. Suivi des transferts dans le cadre des bonnes pratiques

De manière générale, et dans le cadre des bonnes pratiques, les institutions et organes de l'Union devraient créer un système interne de suivi et d'enregistrement des transferts relevant de l'article 9[20]. Celui-ci devrait non seulement inclure les transferts sur la base de leur caractère adéquat, mais aussi, et surtout, les transferts reposant sur des dérogations (article 9, paragraphes 6 et 7; voir le point 6 ci-dessous). Cette disposition serait notamment utile pour contribuer à la gestion interne des transferts internationaux et veiller à une responsabilisation et à une conformité effectives dans le cadre du règlement.

4. Protection adéquate

4.1. Applicabilité

L'article 9, paragraphe 1, du règlement dispose que le «*transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires, et qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, ne peut avoir lieu que pour autant qu'un niveau de protection adéquat soit assuré dans le pays du destinataire ou au sein de l'organisation internationale destinataire, et que ce transfert vise exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement*»[21].

Ce principe général indique que des données à caractère personnel ne peuvent être transférées par une institution ou un organe de l'Union à un pays tiers ou à une organisation internationale[22], à moins qu'un niveau de protection adéquat ne soit garanti. La disposition précise également que le transfert devrait viser «*exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement*». Il s'agit d'une approche plus restrictive que celle de la directive, qui repose sur la nature spécifique des institutions et des organes publics couverts par le règlement, lesquels ne sont pas habilités à agir au-delà de leurs compétences.

Par voie de dérogation, si un niveau de protection adéquat des données n'existe pas dans le pays du destinataire, ces transferts ne peuvent intervenir que si des garanties adéquates sont adoptées par le responsable du traitement (voir aussi le point 6.2) ou si

[20] Il pourrait être recommandé à certains institutions et organes de tenir un registre central des transferts. Par exemple, au regard de la sensibilité des données concernées et de la finalité du traitement, le CEPD a conseillé à l'OLAF de tenir un registre central des transferts (document de travail du 13 février 2006 intitulé «*OLAF Operations: International Transfers of Personal Data*» (opérations de l'OLAF: transferts internationaux de données à caractère personnel).

[21] Voir également l'article 13, paragraphe 1, point d), de la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350/60 du 30.12.2008.

[22] Les articles 25 et 26 de la directive ne font pas référence aux transferts à des organisations internationales et mentionnent uniquement les transferts à des pays tiers.

l'une des exceptions prévues à l'article 9, paragraphe 6, s'applique (voir aussi le point 6.1).

4.2. Notion d'«adéquation»

L'article 9 ne donne pas de définition de l'«adéquation», ni du «niveau de protection adéquat». Cependant, l'article 9, paragraphe 2, prévoit certains éléments qui devraient être pris en considération pour apprécier l'«adéquation». Il précise que le niveau de protection offert par un pays tiers ou une organisation internationale s'apprécie au regard de «*toutes les circonstances entourant une opération ou un ensemble d'opérations de transfert de données*». Il exige également qu'il soit «*notamment tenu compte de la nature des données, de la finalité et de la durée du (ou des) traitement(s) envisagé(s), du pays tiers ou de l'organisation internationale destinataire, de la législation, tant générale que sectorielle, en vigueur dans le pays tiers ou applicable à l'organisation internationale en question ainsi que des règles professionnelles et des mesures de sécurité appliquées dans ce pays ou dans cette organisation internationale*». Cette liste n'est pas exhaustive, d'autres éléments pouvant également entrer en considération en fonction du cas d'espèce.

L'appréciation de l'adéquation exige donc une «évaluation du risque» de l'opération de traitement visée elle-même (par exemple, la nature des données, la finalité et la durée du (ou des) traitement(s) envisagé(s)) et une évaluation du système ou des mesures juridiques applicables aux destinataires (par exemple, la législation générale et sectorielle, les exigences professionnelles et les mesures de sécurité)[23]. L'«adéquation» est une notion pratique; par conséquent, toute appréciation de l'adéquation doit tenir compte des règles applicables dans le pays destinataire visé et des moyens permettant de garantir leur application effective. Ces principes sont «au cœur» de la protection des données et sont décrits comme suit par le groupe de travail «Article 29» sur la protection des données[24]:

«**1) Limitation des transferts à une finalité spécifique**
Les données doivent être traitées dans un but spécifique et n'être utilisées ou communiquées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité du transfert. Les seules exceptions à cette règle seraient celles qui sont nécessaires dans une société démocratique pour l'une des raisons énoncées à l'article 13 de la directive. *[Disposition analogue à l'article 20 du règlement]*.

[23] Il est particulièrement important de déterminer ces risques dans les cas où aucune décision d'adéquation n'est adoptée et où c'est le responsable du traitement des données qui apprécie l'adéquation ou offre des garanties complémentaires. Plus le risque est élevé, plus les exigences en matière d'analyse de la protection sont strictes.

[24] Voir le document de travail du groupe de travail «Article 29» intitulé «Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données», adopté le 24 juillet 1998, disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_fr.pdf.
Le groupe de travail «Article 29» sur la protection des données joue un rôle actif dans le recensement des éléments à évaluer dans le système juridique du destinataire. Ce document se trouve à la base de toutes les décisions d'adéquation adoptées par la Commission européenne ainsi que des instruments offrant des «garanties suffisantes» en l'absence d'adéquation, comme les clauses contractuelles types et les règles d'entreprise contraignantes.

2) Qualité et proportionnalité des données
Les données doivent être exactes et, au besoin, actualisées. Elles doivent être adéquates, pertinentes et non excessives au regard des finalités auxquelles obéit leur transfert ou leur traitement ultérieur.

3) Transparence
Les personnes physiques doivent recevoir des informations sur les finalités du traitement et sur l'identité du responsable de ce traitement dans le pays tiers ainsi que d'autres informations, dans la mesure où elles sont nécessaires pour assurer un traitement loyal. Les seules exceptions autorisées doivent être conformes à l'article 11, paragraphe 2, et à l'article 13 de la directive. *[Dispositions analogues à l'article 12, paragraphe 2, et à l'article 20 du règlement, respectivement]*.

4) Sécurité
Le responsable du traitement doit prendre des mesures de sécurité, sur le plan technique et au niveau de l'organisation, qui soient appropriées au regard des risques présentés par le traitement. Toute personne agissant sous l'autorité du responsable du traitement, y compris un sous-traitant, ne doit traiter les données que sur instruction du responsable.

5) Droits d'accès, de rectification et d'opposition
Toute personne concernée[25] doit avoir le droit de se voir communiquer toutes les données traitées qui la concernent et d'obtenir leur rectification lorsqu'il apparaît qu'elles sont inexactes. Dans certains cas, elle doit également pouvoir s'opposer au traitement des données qui la concernent. Les seules exceptions à ces droits doivent être conformes aux dispositions de l'article 13 de la directive. *[Disposition analogue à l'article 20 du règlement]*.

6) Restrictions aux transferts ultérieurs
Les transferts ultérieurs de données à caractère personnel effectués par le destinataire du transfert initial ne doivent être autorisés que lorsque le deuxième destinataire (c'est-à-dire le destinataire du transfert ultérieur) est également soumis à des règles offrant un niveau de protection adéquat. Les seules exceptions autorisées doivent être conformes aux dispositions de l'article 26, paragraphe 1, de la directive. *[Disposition analogue à l'article 9, paragraphe 6, du règlement]*.»

En outre, des mécanismes de procédure et de mise en application doivent être garantis. En ce sens, un système de protection des données ou une politique étoffée en matière de vie privée poursuit, pour l'essentiel, trois objectifs:

«1) assurer un **niveau satisfaisant de respect des règles**. (Aucun système ne peut garantir qu'elles seront respectées à 100 %, mais certains sont meilleurs que d'autres). On reconnaît en général la qualité d'un système à la conscience aiguë qu'ont les responsables du traitement de leurs obligations et les personnes concernées de leurs droits et des moyens de les exercer. L'existence de sanctions efficaces et dissuasives est importante pour garantir ce respect des règles, de même que, bien entendu, les

[25] D'après l'article 13 du règlement, le droit d'accès *peut* supposer un droit d'obtenir une copie des données (la présente note de bas de page ne fait pas partie du document du groupe de travail).

systèmes de vérification directe par les autorités, les commissions de contrôle ou les responsables indépendants chargés de la protection des données;

2) apporter **soutien et assistance aux personnes concernées** dans l'exercice de leurs droits. La personne physique doit être en mesure de faire valoir ses droits rapidement et efficacement sans avoir à subir des coûts prohibitifs. Pour ce faire, il faut qu'il existe une sorte de mécanisme institutionnel permettant l'instruction des plaintes par une instance indépendante;

3) fournir des **voies de recours appropriées** à la partie lésée en cas de non-respect des règles. Il s'agit là d'un élément primordial qui requiert notamment l'institution d'une instance d'arbitrage indépendante permettant le versement d'une indemnisation et, au besoin, l'adoption de sanctions.».

Pour résumer, un système adéquat reconnaît ces principes, tant dans leur esprit que dans leur mise en œuvre pratique, y compris sur le plan de leur mise en application le cas échéant. Ce point peut être garanti non seulement par l'existence de règles et de procédures juridiques, notamment par l'intermédiaire d'autorités judiciaires ou compétentes en matière de protection des données, de pouvoirs de réparation afin de rétablir la conformité dans l'intérêt des personnes concernées, mais aussi d'autres «mesures» instaurant un environnement plus sûr en matière de protection des données, par exemple des codes de conduite, des règles internes, des contrôles de sécurité ou des mécanismes de vérification, pour autant que tous les éléments essentiels susmentionnés soient couverts.

5. Appréciation de l'adéquation

L'appréciation du niveau de protection dans un pays ou un secteur donné peut être menée à différents niveaux et avoir différents effets juridiques, que ce soit par l'intermédiaire des responsables du traitement eux-mêmes, d'autorités compétentes en matière de protection des données ou de la Commission européenne. Cette dernière solution entraîne la prise de décisions relatives à l'adéquation ou à l'inadéquation qui sont contraignantes pour les États membres et les institutions et organes de l'Union (voir l'article 25, paragraphes 4 et 6, de la directive).

En l'absence d'une décision contraignante, la directive permet d'aboutir à différentes solutions: une majorité des États membres fait l'objet d'une évaluation centralisée menée par une autorité compétente en matière de protection des données, tandis que d'autres États membres s'attendent à ce que les responsables du traitement des données réalisent au moins une évaluation préliminaire, comme le prévoit également l'article 9 du règlement. Les institutions et organes de l'Union sont donc compétents, dans le cadre de leur mission de responsable de traitement, et doivent apprécier l'adéquation avant de procéder à un transfert de données. Ce point sera examiné plus en détail ci-dessous.

5.1. Décision d'adéquation adoptée par la Commission européenne

L'article 9, paragraphe 5, du règlement dispose que les «*institutions et organes communautaires prennent les mesures nécessaires pour se conformer aux décisions*

prises par la Commission constatant, en application de l'article 25, paragraphes 4 et 6, de la directive 95/46/CE, qu'un pays tiers ou une organisation internationale assure ou n'assure pas un niveau de protection adéquat».

D'après l'article 25, paragraphe 6, de la directive, la «*Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux [...]*». Une décision d'adéquation adoptée à la lumière de l'article 25, paragraphe 6, est contraignante pour l'ensemble des États membres, ce qui aboutit à la «libre circulation de données» vers le pays tiers en question. Ce type de décision s'applique également aux institutions et organes de l'Union.

La Commission européenne a déjà adopté plusieurs décisions d'adéquation; dès lors, les responsables du traitement des données qui souhaitent transférer des données vers un pays tiers devraient au préalable vérifier la liste des pays adéquats[26].

> Au moment de l'adoption du présent document, les pays concernés sont les suivants: Andorre, l'Argentine, le Canada (secteur privé), les États-Unis (sphère de sécurité; pour certaines activités dans le secteur privé), Guernesey, les Îles Féroé, l'Île de Man, Israël, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay.

Le champ d'application des décisions d'adéquation est variable. Elles couvrent parfois le système de protection des données d'un pays (comme en Argentine et en Suisse), tandis que d'autres portent uniquement sur certaines catégories de traitement des données à caractère personnel (à l'instar de la sphère de sécurité pour les États-Unis et du Canada). Il convient d'en tenir compte avant d'effectuer un transfert.

Pour résumer, si le niveau de protection dans le lieu de destination est «adéquat», les données à caractère personnel circulent librement et le responsable du traitement n'est pas tenu de prendre des mesures complémentaires en lien avec le transfert des données, pour autant que tous les autres aspects du règlement soient respectés.

5.2. Appréciation de l'adéquation par le responsable du traitement

En l'absence d'une décision de la Commission concernant l'adéquation, le responsable du traitement devrait en principe mener une évaluation spécifique de l'adéquation du système de protection des données (règles juridiques et autres mesures), en tenant compte de l'ensemble des circonstances du cas d'espèce. L'analyse devrait se focaliser sur les caractéristiques spécifiques (garanties ou risques) du transfert ou de l'ensemble de transferts en question. Celles-ci incluent les types de données, leur finalité et la durée de l'opération de traitement proposée, ainsi que l'identité des destinataires dans le pays ou l'organisation internationale de destination.

[26] La liste des pays adéquats (ou des secteurs au sein d'un pays tiers, à l'instar de la sphère de sécurité pour les États-Unis) est disponible sur le site web ci-après: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

Comme il a été observé ci-dessus, l'appréciation de l'adéquation exige également de tenir compte tant de l'esprit que de la pratique effective (approche objective et fonctionnelle). Dès lors, certaines vérifications des mesures mises en œuvre doivent être effectuées avant de pouvoir déterminer si un niveau de protection adéquat est effectivement garanti. Ce point relève de la compétence du responsable du traitement. Cependant, dans la pratique, il ne lui est pas toujours possible de réaliser une appréciation complète de l'adéquation pour un pays tiers ou une organisation internationale. Le cas échéant, le responsable du traitement devrait présumer que le niveau de protection n'est pas adéquat et envisager d'autres options parmi celles décrites ci-dessous.

En tout état de cause, ces appréciations spécifiques de l'adéquation devraient être clairement différenciées des décisions d'adéquation adoptées par la Commission. En effet, les premières n'affectent pas les éventuelles évaluations ultérieures du cadre de protection des données ou de l'adéquation du pays tiers ou de l'organisation internationale réalisées par la Commission. En outre, elles ne s'appliquent pas de manière transversale.

À la lumière du principe de responsabilité, le responsable du traitement des données devrait, le cas échéant, documenter de manière exhaustive les mesures prises pour veiller à l'adéquation et envisager d'effectuer une évaluation des risques appropriée[27].

5.3. Rôle du CEPD dans l'appréciation de l'adéquation

- Décisions d'adéquation adoptées par la Commission européenne

Les responsables du traitement des données ne sont tenus à aucune procédure particulière lorsque la Commission a effectué une déclaration d'adéquation conformément à l'article 25, paragraphe 4, de la directive, et il n'est pas nécessaire d'informer le CEPD. Néanmoins, dans le cadre de nos missions de suivi et de supervision, et conformément à l'article 9, paragraphe 5, nous pourrions décider de solliciter des informations auprès des responsables du traitement des données au cas par cas.

- Appréciation de l'adéquation par le responsable du traitement des données

Toute analyse effectuée par le responsable du traitement devrait être clairement documentée et mise à disposition du CEPD à sa demande.

Au regard de la politique relative aux consultations dans le domaine de la supervision et de la mise en application, le DPD d'une institution ou d'un organe de l'Union devrait toujours être consulté et associé à l'analyse. Par ailleurs, les responsables du traitement des données sont encouragés à solliciter un avis du CEPD lorsque l'affaire a) présente une nature ou une complexité inédites (lorsque le DPD ou l'institution ont

[27] Le fait que les pouvoirs publics ou l'autorité compétente du pays tiers fournissent des explications ou des garanties concernant l'interprétation et la mise en œuvre de la législation (contraignante ou non) peut influer de manière déterminante sur l'appréciation de l'adéquation. Cependant cette dernière doit préciser qu'elle se fonde sur ces explications et garanties et est donc conditionnée à leur respect.

des doutes importants) ou b) qu'elle a une incidence claire sur les droits des personnes concernées (en raison notamment des risques liés aux opérations de traitement, etc.)[28].

6. Dérogations

Dans certains cas, même si le pays ou l'organisation internationale destinataire ne présente pas un niveau de protection adéquat, des transferts peuvent avoir lieu si l'une ou plusieurs des situations prévues à l'article 9, paragraphes 6 ou 7, du règlement s'appliquent.

Le premier type de dérogation est visé à l'article 9, paragraphe 6, et comprend une liste restrictive de situations spécifiques. Dans ce cas, aucune autre mesure n'est en principe exigée si l'une des situations répertoriées s'applique (voir le point 6.1 ci-dessous).

Le second type de dérogation est visé à l'article 9, paragraphe 7, et concerne les transferts vers une destination qui ne garantit pas un niveau de protection adéquat. Ces transferts ne peuvent avoir lieu que si le responsable du traitement offre des garanties adéquates (voir le point 6.2 ci-dessous).

6.1. Dérogations spécifiques (exceptions à l'exigence d'adéquation)

L'article 9, paragraphe 6, décrit différentes situations dans lesquelles un transfert vers une destination qui n'est pas adéquate pourrait avoir lieu. Ces situations devraient être interprétées et appliquées de manière restrictive.

Il convient de noter que le recours à des *exceptions* ne garantit pas, en soi, que les droits de la personne concernée sont protégés dans le pays ou l'organisation internationale destinataire. Dès lors, il est recommandé aux responsables du traitement de «*privilégier des solutions garantissant aux personnes qu'elles continueront à bénéficier des droits et garanties fondamentaux reconnus à l'égard du traitement de leurs données dans l'UE, une fois celles-ci transférées*»[29].

Les transferts de données à caractère personnel qui pourraient être qualifiés de «*répétés, massifs ou structurels*»[30] devraient notamment être effectués au sein d'un cadre juridique spécifique, plutôt que par voie d'exception, ces dernières ne devant être utilisées, en principe, que de manière ponctuelle.

En tout état de cause, le recours aux exceptions ne devrait jamais aboutir à une situation dans laquelle les droits fondamentaux des personnes concernées pourraient être violés. Pour cette raison, dans les cas limités pour lesquels le recours aux exceptions est légitime, le responsable du traitement devrait prendre des précautions pour veiller à ce que le destinataire respecte certains principes en matière de protection des données. Ces garanties pourraient prendre différentes formes (protocole

[28] Voir la note de bas de page 9 ci-dessus.
[29] Groupe de travail «Article 29» sur la protection des données, «Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995», page 10.
[30] Avis du CEPD sur le paquet de mesures pour une réforme, adopté le 7 mars 2012.

d'accord, échange de lettres, etc.). Le contenu des garanties dépend également des caractéristiques du transfert, par exemple les différents niveaux de risque.

Toutefois, dans certaines situations dans lesquelles le recours à d'autres solutions (comme l'adoption de décisions d'adéquation ou de garanties suffisantes) se révèle inapproprié ou impossible, le responsable du traitement des données doit recourir aux exceptions prévues à l'article 9, paragraphe 6, du règlement. Les dérogations spécifiques visées dans cette disposition ont clairement pour objectif de servir de solution de substitution et peuvent être présentées comme suit:

a) «la personne concernée a indubitablement donné son consentement au transfert envisagé»

Ce fondement, conjointement à l'article 5, point d), du règlement, reste normalement d'une utilité limitée pour les institutions et organes de l'Union. C'est pourquoi ces derniers devraient disposer de mandats juridiques spécifiques pour traiter les données à caractère personnel, qui ne devraient être transférées qu'aux fins des missions relevant de la compétence du responsable du traitement. Par conséquent, au regard de la définition du «consentement de la personne concernée» établie à l'article 2, point h), du règlement, la «manifestation de volonté, libre, spécifique et informée» par cette dernière ne serait exprimée que dans des circonstances exceptionnelles. Par ailleurs, dans le domaine de l'emploi, le consentement «librement manifesté»[31] doit être garanti sur la base de critères stricts. Cependant, cette exigence n'exclut pas complètement le recours à cette possibilité. Par exemple, la personne concernée pourrait elle-même demander à une institution ou à un organe de l'Union d'effectuer un transfert (par exemple, le transfert de rapports d'évaluation à un futur employeur situé en dehors de l'Union). Le caractère «spécifique» du consentement suppose que celui-ci ne peut couvrir plusieurs finalités de traitement en même temps. La personne concernée doit également être informée des modalités du transfert, conformément à l'article 11 du règlement, ainsi que de tout risque potentiel.

b) «le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée»

Les institutions et organes de l'Union (responsables du traitement) peuvent signer des contrats dans différents domaines, par exemple des projets de recherche, des stages, des prestations de traduction, une assistance technique, du conseil, des conférences ou des services de publicité. Ces contrats peuvent notamment être conclus avec des personnes physiques. Le cas échéant, des transferts à un pays tiers ou à une organisation internationale peuvent être nécessaires aux fins de l'exécution du contrat conclu avec la personne concernée. Par exemple, dans le cas d'un contrat avec un chercheur, un transfert peut avoir lieu dans le cadre d'une mission à l'étranger, lorsque

[31] Groupe de travail «Article 29» sur la protection des données, avis 8/2001 du 13 septembre 2001 sur le traitement des données à caractère personnel dans le contexte professionnel.

l'institution ou l'organe de l'Union a besoin d'envoyer des informations à caractère personnel à un partenaire de recherche établi dans un pays tiers. Un autre exemple pourrait être celui du versement de fonds à un individu sur un compte établi dans une banque étrangère. Des transferts similaires sont autorisés à un stade précontractuel, pour autant qu'ils soient nécessaires à la mise en œuvre des mesures prises à la demande de la personne concernée.

c) «le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers»

Ce pourrait être le cas, par exemple, de transferts de données dans le cadre d'un contrat ad hoc d'assurance de transport conclu avec une entreprise privée établie dans un pays tiers. Dans ce cas, la personne concernée n'est pas partie au contrat, mais ce dernier doit être signé dans son intérêt (par exemple, pour un fonctionnaire qui part en mission).

d) «le transfert est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêt public importants ou pour la constatation, l'exercice ou la défense d'un droit en justice»

Les «motifs d'intérêt public importants» devraient correspondre à un intérêt stratégique ou à une obligation légale de *l'expéditeur* (institution ou organe de l'Union) et non du seul destinataire. En l'absence d'obligation juridique spécifique, le motif d'intérêt public doit être «important» et le transfert doit être «nécessaire» pour que cette dérogation s'applique. Il convient de déterminer ces critères au cas par cas. Cette situation s'appliquerait, par exemple, lorsqu'un organe de l'Union tel que l'OLAF mène une enquête concernant une fraude et a besoin de transférer des données à caractère personnel (comme des éléments de preuve) à un pays tiers. Dans de tels cas, et étant donné le caractère sensible des données, le recours à cette exception resterait limité, en principe, à des transferts exceptionnels ou ponctuels. Si les transferts pourraient être qualifiés de «répétés, massifs ou structurels» (même s'ils sont liés à une seule enquête ou un seul dossier), une solution systémique et protectrice serait nécessaire pour prévenir des menaces disproportionnées pour les libertés et droits fondamentaux de la personne concernée. De fait, il pourrait être recommandé de fonder les transferts sur les «garanties suffisantes» visées à l'article 9, paragraphe 7 (voir le point 6.2 ci-dessous).

Le CEPD a reçu un avis de l'OLAF concernant un ensemble de clauses types devant être utilisées dans le cadre des accords de coopération administrative conclus avec les autorités de pays tiers ou les organisations internationales. Ces clauses types sont fondées sur les clauses contractuelles types adoptées par la Commission (voir le point 6.2 ci-dessous). Le CEPD a conclu que ces clauses types devraient également être utilisées, en principe, pour les transferts couverts par les exceptions visées à l'article 9, paragraphe 6, lorsqu'il existe des risques spécifiques pour les personnes concernées. Ce pourrait être le cas, par exemple, en raison de la nature des données concernées (comme dans le cas de données sensibles), de la finalité du traitement (par exemple, des enquêtes pouvant aboutir à des poursuites pénales) ou du cadre juridique dans

le pays destinataire (par exemple, en raison de l'absence de règles en matière de protection des données ou de leur insuffisance).

L'Agence européenne de la sécurité aérienne (AESA) mène certaines activités (en particulier des services dans le domaine de la certification) qui donnent lieu au paiement d'honoraires et de redevances par les demandeurs. Une partie de ces activités de certification peut être menée entièrement ou partiellement en dehors du territoire des États membres. Le paiement facturé au demandeur comprend aussi les frais de déplacement des experts. L'AESA est invitée par les demandeurs à leur fournir les noms et la date de déplacement des experts afin de leur permettre de relier les dépenses à chaque personne. Le CEPD a émis une recommandation selon laquelle, puisque l'exécution des services décrits ci-dessus est une des activités essentielles de l'AESA, les transferts réalisés aux fins du paiement de ces services pourraient être considérés comme nécessaires au fonctionnement de cet organe, de manière à pouvoir bénéficier d'une dérogation au titre de l'article 9, paragraphe 6, point d). Il convient toutefois de noter que, dans les cas où une exception est appliquée, aucune garantie n'est en principe assurée. C'est la raison pour laquelle le CEPD a recommandé l'inclusion d'une clause précisant que le destinataire a) est légalement autorisé à demander ces données et b) qu'il limitera l'utilisation des données aux seules fins justifiant le transfert[32].

La constatation, l'exercice ou la défense d'un droit en justice constituent également des fondements possibles pour une dérogation. Cette disposition pourrait s'appliquer, par exemple, lorsqu'une procédure judiciaire se déroule dans un pays tiers et que des éléments de preuve comprenant des données à caractère personnel sont sollicités auprès d'une institution d'un organe de l'Union. Le responsable du traitement doit être en mesure de démontrer la nécessité du transfert.

e) «le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée»

Cette dérogation serait applicable, par exemple, si un fonctionnaire subit un accident au cours d'une mission et qu'un hôpital d'un pays tiers demande au service médical de l'institution de l'Union de fournir certaines données médicales nécessaires pour soigner cette personne. Le responsable du traitement doit être en mesure de démontrer la nécessité du transfert.

Le Parlement européen gère une base de données, le «Security Support System» (système d'aide à la sécurité), qui offre une assistance aux missions extérieures en cas d'urgence médicale. Ce système peut nécessiter un éventuel transfert aux services sanitaires d'un pays tiers. Les données à caractère

[32] Voir, par exemple, la lettre du CEPD du 4 octobre 2010 au délégué à la protection des données de l'Agence européenne de la sécurité aérienne concernant les transferts internationaux, disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2010/10-10-04_Letter_DPO_EASA_FR.pdf.

personnel traitées comprennent notamment des informations médicales (en cas d'urgence, si le participant est retrouvé inconscient, il peut s'agir d'informations relatives au traitement médicamenteux nécessaire, aux allergies ou au groupe sanguin). Le CEPD a considéré que cette opération de traitement relèverait de l'article 9, paragraphe 6, point e) [ainsi que de l'article 9, paragraphe 6, point a)], compte tenu du fait que les informations sont volontairement fournies par la personne concernée[33].

f) «le transfert est effectué à partir d'un registre qui, conformément à la législation communautaire, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime [...]»

Cette disposition s'appliquerait, par exemple, à une demande d'accès à un registre public géré par une institution ou un organe de l'Union, qui serait soumise par un citoyen européen depuis un pays tiers[34]. Cependant, ce serait plus généralement le cas aussi de la publication en ligne de certaines données à caractère personnel aux fins de leur consultation par le public, à l'instar du répertoire de la Commission. Dans ce cas, l'analyse ne devrait dès lors pas se focaliser sur la notion de «transfert», mais sur l'examen du caractère légitime et proportionné de la publication des données à caractère personnel.

6.2. Garanties suffisantes

Comme il a été observé ci-dessus, dans certains cas, le niveau de protection dans le pays tiers ou l'organisation internationale destinataire n'est pas adéquat, ou présente en tout cas un caractère douteux. Dans certains de ces cas, des dérogations ne sont parfois pas applicables. Le cas échéant, le responsable du traitement des données devrait mettre en place des garanties pour veiller à la protection des données à caractère personnel, conformément à l'article 9, paragraphe 7, du règlement.

La notion de «garanties suffisantes» n'est définie ni dans la directive ni dans le règlement. Celles-ci devraient donc être interprétées au sens de garanties en matière de protection des données instaurées pour une situation spécifique et qui n'existent pas déjà dans le système juridique du destinataire. Parmi les exemples courants de garanties suffisantes figurent les clauses contractuelles types[35] adoptées par la

[33] Voir l'avis du CEPD sur la notification d'un contrôle préalable adopté le 29 septembre 2009 (affaire 2009-0225) concernant le «dispositif d'assistance en matière de sécurité» du Parlement européen.

[34] L'article 2, paragraphe 1, du règlement (CE) n° 1049/2001 dispose que tout «citoyen de l'Union et toute personne physique ou morale résidant ou ayant son siège dans un État membre a un droit d'accès aux documents des institutions, sous réserve des principes, conditions et limites définis par le présent règlement».

[35] Décisions 2001/497/CE et 2004/915/CE de la Commission (transferts entre responsables du traitement) et décision 2002/16/CE de la Commission (transferts des responsables du traitement aux sous-traitants). La décision 2004/915/CE est une version révisée de la décision 2001/497/CE. La dernière version a été présentée par un regroupement d'associations professionnelles et présente plusieurs différences par rapport au texte initial. Elle prévoit, par exemple, des exigences d'audit plus flexibles et des règles plus détaillées concernant le droit d'accès (voir également le préambule de la décision 2004/915/CE).

Commission ou les règles d'entreprise contraignantes[36]. La finalité de ces instruments consiste à instaurer la protection qui fait défaut dans le lieu de destination des données.

6.2.1. Contenu des garanties suffisantes

Même si l'article 9, paragraphe 7, ne décrit pas les éléments qui permettraient de qualifier des garanties de «suffisantes», les critères d'adéquation énumérés au point 4.2 ci-dessus devraient faire l'objet d'un examen attentif. Tout instrument créé dans le but de servir de «garantie suffisante» devrait clairement inclure une description des principes en matière de protection des données qui doivent être respectées par l'importateur (destinataire), ainsi que des moyens permettant d'assurer la mise en place des mécanismes nécessaires pour rendre cette protection effective.

Les mécanismes de surveillance et de mise en application potentiels pourraient inclure les dispositions ci-après (dont certaines ne sont pertinentes que dans le domaine du droit privé – voir le point 6.2.2.):

- une clause de tiers bénéficiaire (pour permettre à la personne concernée de donner suite à toute violation des obligations contractuelles de l'importateur ou de l'exportateur);
- une clarification des obligations de l'importateur et de l'exportateur (par exemple, une obligation de répondre aux demandes, la communication d'un exemplaire des clauses à la personne concernée, l'obligation de se soumettre à des examens, à des audits, etc.);
- une clause de responsabilité (différentes solutions sont prévues dans les clauses contractuelles types adoptées par la Commission, selon que les contrats sont conclus entre deux responsables du traitement ou entre un responsable du traitement et un sous-traitant);
- l'obligation pour l'importateur d'informer l'exportateur de toute violation de la sécurité;
- les modalités en matière de médiation et de juridiction en cas d'absence de résolution à l'amiable d'un litige;
- les dispositions détaillées du droit applicable (les clauses sont régies par le droit du pays dans lequel l'institution ou l'organe de l'Union est établi. Ce type de clause est inclus pour régir les litiges de droit civil susceptibles d'apparaître entre les parties dans le cadre de la mise en application);
- les informations concernant la coopération avec les autorités de surveillance;
- le pouvoir de l'autorité compétente en matière de protection des données de bloquer ou de suspendre les transferts.

En outre, comme dans le cas des clauses contractuelles types, une clause décrivant les modalités du transfert ou de l'ensemble des transferts doit être incluse. Celle-ci

[36] Voir l'aperçu général des règles d'entreprise contraignantes, disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

devrait préciser les catégories de données, leur finalité, leur période de conservation, des mesures de sécurité détaillées, des mécanismes de notification des informations et les modalités d'exercice des droits des personnes concernées (accès, suppression, objection, etc.).

En fonction du type de transfert ou de destinataire, lorsqu'un contrat ne constitue pas un instrument approprié[37] (voir le point 6.2.2. ci-dessous), d'autres engagements en matière de supervision et de mise en application doivent être adoptés et associer tant le responsable du traitement que le destinataire, par exemple:

- une vérification directe par les autorités (par exemple, des inspections conjointes, des audits réalisés par des organismes indépendants, etc.) ou par le responsable du traitement (par exemple, des audits);
- l'obligation de désigner un délégué à la protection des données indépendant;
- une enquête indépendante concernant les plaintes (en désignant des points de contact pour les enquêtes);
- des sanctions dissuasives, des réparations appropriées et une conduite conforme aux décisions de la Cour;
- une clause de responsabilité (obligation de soumettre au CEPD des éléments de preuve de la conformité, soit à sa demande, soit à intervalles réguliers);
- la transparence des garanties (par exemple, la publication des instruments sur l'internet);
- la résiliation de l'accord ou du dispositif, par exemple, en cas d'infraction.

Lorsque le destinataire est un organisme public, celui-ci pourrait être invité à adopter des règles internes contraignantes pour veiller au respect des engagements pris.

Par ailleurs, les mesures devraient inclure une référence au pouvoir du CEPD d'interdire ou de suspendre la circulation de données vers des pays tiers ou des organisations internationales, afin de protéger les individus:

> a) lorsque le droit auquel l'importateur des données est soumis l'oblige à déroger aux garanties applicables en matière de protection des données, au-delà des restrictions nécessaires dans une société démocratique, conformément à l'article 20 du règlement, et lorsque ces exigences sont susceptibles d'avoir des répercussions négatives importantes sur la protection offerte par les «garanties suffisantes»[38], ou
> b) lorsqu'il existe des éléments de preuve convaincants ou une forte probabilité que les «garanties suffisantes» ne soient pas, ou ne seront pas,

[37] Ce qui peut notamment être le cas pour les organisations internationales dont les privilèges et immunités peuvent ne pas les autoriser à s'engager à se soumettre à des vérifications directes par les autorités, à se conformer aux décisions des juridictions de l'Union, etc. La mise au point de «garanties suffisantes» exige dès lors de faire preuve de créativité, la plupart des instruments élaborés jusqu'à présent l'ayant été dans un cadre commercial.

[38] Voir, par exemple, l'enquête de la commission LIBE sur la surveillance électronique de masse des citoyens de l'Union européenne, audience publique, Strasbourg, 7 octobre 2013, contribution de Peter Hustinx (CEPD), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_FR.pdf.

respectées et que la poursuite du transfert créerait un risque imminent de préjudice grave pour les personnes concernées.

Ces mesures s'appliquent sans préjudice des pouvoirs du CEPD de faire appliquer le règlement pour ce qui concerne les institutions ou les organes de l'Union concernés (voir le point 9).

6.2.2. Forme et nature des instruments reflétant les garanties suffisantes

Le règlement n'exige pas que l'instrument reflétant les garanties prenne une quelconque forme particulière. En fonction des circonstances, les garanties pourraient, par exemple, être intégrées à un contrat ou à une déclaration ou décision contraignante. La nature de l'instrument juridique varie selon que l'institution ou l'organe de l'Union agit dans le cadre du droit privé ou public.

Si l'institution ou l'organe de l'Union agit dans le cadre du droit privé (par exemple, en externalisant la gestion des voyages pour des missions, les services informatiques ou la formation) et que le destinataire des données est établi dans un pays tiers qui n'a pas été déclaré adéquat, l'institution ou l'organe de l'Union pourrait conclure avec le destinataire un contrat prévoyant des garanties suffisantes[39]. L'un des modèles de clauses contractuelles types de la Commission pourrait être utilisé. Le cas échéant, la référence à la directive doit être remplacée par une référence au règlement[40].

Initialement, les clauses contractuelles types ont été élaborées pour le secteur professionnel; leur application par les autorités publiques pourrait dès lors être limitée. Si l'institution ou l'organe de l'Union agit dans un domaine de droit public (par exemple, en créant un système d'échange de données avec des pays tiers ou en transférant des données en matière répressive ou douanière), un contrat ne constitue pas un instrument juridique approprié. Il convient donc d'envisager un mécanisme différent. Cette disposition devrait permettre de garantir le respect de principes d'adéquation et de veiller à ce que les garanties soient contraignantes pour le destinataire et puissent effectivement être mises en application.

La première étape devrait consister à inclure les garanties suffisantes dans le texte du principal accord international si celui-ci crée le mandat ou le transfert (voir le point 8).

Dans certains cas, en raison de la nature de l'organisation internationale ou de l'instrument juridique concerné, il n'est pas possible d'adopter des «garanties suffisantes» sous la forme d'un «instrument contraignant». Le cas échéant, un autre type d'instrument de protection devrait être envisagé. Par exemple, un protocole d'accord pourrait se révéler approprié dans certaines circonstances exceptionnelles.

---

[39] Outre un contrat, d'autres moyens pourraient également être utilisés (par exemple, le destinataire pourrait adopter une politique relative à la vie privée et publier une déclaration unilatérale instaurant une obligation juridique auto-contraignante, soit *per se* en vertu du droit national, soit par l'effet du principe d'attente légitime).

[40] À l'instar, par exemple, de la clause contractuelle type adoptée le 15 juin 2001 (décision 2001/497/CE de la Commission), et notamment: référence dans la clause 1, point a); appendice 2, référence dans les paragraphes d'introduction et les principes 5, 6, 7 et 9. Concernant la clause 10, «Droit applicable», celle-ci doit être complétée par une référence à l'État membre dans lequel l'institution ou l'organe de l'Union est établi.

Le CEPD a déjà précisé que «*[...] la possibilité de recourir à des instruments qui ne soient pas juridiquement contraignants pour offrir des garanties appropriées doit être clairement justifiée et limitée uniquement aux cas où la nécessité de se fier à ce type de mesure non contraignante a été démontrée. [...] La nécessité d'avoir recours à des garanties non légalement contraignantes dans le secteur public doit être analysée avec soin, au vu de la finalité du traitement et de la nature des données. [...]*»[41]. Indépendamment du type d'instrument adopté, les mesures en place doivent être suffisantes pour garantir la mise en œuvre appropriée (et la mise en application le cas échéant) des garanties décrites au point 6.2.1 ci-dessus.

6.3. Rôle du CEPD dans le traitement des dérogations

L'article 9, paragraphe 8, du règlement dispose que les «*institutions et organes communautaires informent le contrôleur européen de la protection des données des catégories de cas dans lesquels ils ont appliqué les paragraphes 6 et 7*». La communication d'informations prend différentes formes en fonction de la nature des dossiers, comme il est expliqué ci-dessous.

- Dérogations de l'article 9, paragraphe 6

Lorsqu'une institution ou un organe de l'Union a besoin de recourir à l'une des dérogations visées à l'article 9, paragraphe 6, ils ne sont pas tenus d'en informer le CEPD ex ante (avant que le transfert ne soit effectué). Cependant, le responsable du traitement devrait communiquer des informations au CEPD à sa demande, dans le contexte des opérations de supervision ou de mise en application. En tout état de cause, le DPD de l'institution ou de l'organe de l'Union devrait toujours être consulté et associé à la prise de décision visant à déterminer si une dérogation doit être appliquée.

En outre, à la lumière de la politique relative aux consultations dans le domaine de la supervision et de la mise en application, les responsables du traitement des données sont encouragés à présenter un avis au CEPD dans certaines circonstances déjà décrites au point 5.3 (deuxième puce) ci-dessus.

- Dérogations de l'article 9, paragraphe 7

De même, le DPD de l'institution ou de l'organe de l'Union doit être associé à la procédure d'analyse conduite avant l'adoption de mesures adéquates.

Pour l'association du CEPD ex ante, trois scénarios doivent être pris en considération pour déterminer si cette participation est nécessaire:

- <u>aucune autorisation ou consultation préalable nécessaire</u>:
  lorsque des clauses contractuelles types sont utilisées;

[41] Avis du CEPD sur le paquet de mesures pour une réforme (voir note de bas de page 5).

- aucune autorisation préalable nécessaire, mais une consultation pourrait l'être: (vérifier la politique du CEPD en matière de consultation dans le domaine de la supervision et de la mise en application); par exemple, lorsqu'un instrument contraignant spécifique (par opposition aux clauses contractuelles types) est mis au point par l'institution ou l'organe de l'Union en vue de son utilisation dans le cadre du droit tant privé que public;

- une autorisation préalable est nécessaire:
  dans certains cas exceptionnels, lorsque les transferts s'appuient sur des garanties spécifiques et ne sont pas intégrés à un instrument juridiquement contraignant[42].

Lorsqu'un instrument contenant des garanties spécifiques est soumis pour consultation ou autorisation préalable, une description exhaustive de l'analyse d'«adéquation» devrait être présentée au CEPD, conjointement à la documentation pertinente et à la confirmation des projets d'instrument(s) ou de mesures prévus pour instaurer les garanties suffisantes.

Après avoir reçu l'avis ou la demande d'autorisation, le CEPD évalue les aspects factuels et juridiques du dossier et émet des recommandations lorsque c'est nécessaire. Si une autorisation est requise, nous pourrions adopter une décision autorisant le transfert ou l'ensemble de transferts si l'adéquation des garanties offertes par le responsable du traitement des données est satisfaisante. Si nous ne considérons pas que les garanties proposées soient pleinement adéquates, nous émettons des recommandations en vue d'instaurer une conformité avec le règlement. Une phase de suivi est ensuite amorcée.

7. Transferts ne relevant pas de la directive 95/46/CE

L'article 9 est intitulé «Transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires et ne relevant pas de la directive 95/46/CE». Ces destinataires peuvent être établis dans les pays de l'EEE mais peuvent mener des types d'opérations exclus du champ d'application de la directive. En effet, l'article 3, paragraphe 2, de la directive dispose que la «*présente directive ne s'applique pas au traitement de données à caractère personnel: – mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal [...]*». Tel serait le cas, par exemple, pour des transferts aux autorités policières ou judiciaires.

[42] Voir la décision du CEPD du 13 février 2014 concernant les transferts de données à caractère personnel effectués par l'OLAF à travers la plate-forme de consultation des données relatives aux enquêtes conformément à l'article 9, paragraphe 7, du règlement (CE) n° 45/2001, disponible à l'adresse suivante:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_EN.pdf

Ces exceptions étaient nécessaires avant l'adoption du traité de Lisbonne, mais elles sont désormais, en principe, incompatibles avec son article 16[43], ainsi qu'avec l'article 8 de la charte des droits fondamentaux de l'Union européenne.

Les États membres sont tenus par la convention 108[44], qu'ils appliquent souvent au-delà du champ d'application de la directive[45]. Cette dernière s'applique à l'ensemble du système juridique, et pas seulement aux domaines relevant des deux premiers piliers. Dans ces cas, il peut être estimé qu'un niveau de protection «adéquat» (ou même «équivalent») existe au niveau national dans les domaines relevant des anciens deuxième et troisième piliers du droit européen. Par conséquent, les transferts peuvent avoir lieu conformément à l'article 9 pour autant qu'ils respectent l'article 8 du règlement.

Comme exposé ci-dessus, tous les États membres ont ratifié la convention 108 du Conseil de l'Europe. Cette ratification prévoit une présomption d'adéquation, qui doit être vérifiée, dans la pratique, auprès de l'État membre[46]. Cette mesure suppose de vérifier les mesures concrètes qui sont exigées du destinataire[47]. Par exemple, la police est-elle soumise à des obligations en matière de protection des données, conformément à la convention 108? Est-elle suffisamment sensibilisée à ses obligations en la matière? Des mécanismes répressifs sont-ils appliqués en cas d'infraction? Cette analyse doit être documentée par le responsable du traitement.

Cette vérification est également recommandée car: a) l'instrument de protection des données de l'Union actuellement applicable aux autorités policières et judiciaires (décision-cadre 2008/977/JAI) ne couvre pas l'ensemble des éléments pertinents pour une appréciation de l'adéquation telle que décrite dans le document de travail WP12 du groupe «Article 29», ni les situations purement nationales[48]; b) il n'existe

[43] Voir l'avis du Contrôleur européen de la protection des données du 14 janvier 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», point 33.

[44] La convention 108 (convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel) est en cours de révision. De plus amples informations sur cette procédure sont disponibles à l'adresse suivante: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_fr.asp.

[45] Voir l'examen et analyse d'impact sur la mise en œuvre de la directive 95/46/CE dans les États membres accompagnant le «premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)», COM(2003) 265 final, disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf. Voir également l'annexe 3 sur la protection des données dans les domaines de la coopération policière et judiciaire en matière pénale de l'analyse d'impact accompagnant le paquet de mesures pour une réforme de la protection des données, SEC(2012) 72 final, Bruxelles, 25.1.2012, p. 36, disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf.

[46] L'article 9, paragraphe 2, de la convention 108 prévoit qu'il est possible de déroger à certains principes de l'instrument «lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales».

[47] La convention 108 ne crée pas de droits subjectifs pour la personne concernée *per se*, et ne peut pas non plus être directement mise en application par la Cour européenne des droits de l'homme.

[48] Voir l'avis du Contrôleur européen de la protection des données du 14 janvier 2011 sur la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», point 35, disponible à l'adresse suivante:

actuellement pas d'instrument juridique de protection des données au niveau de l'Union couvrant la politique étrangère et de sécurité commune[49].

Pour ce qui concerne Europol et Eurojust, ils ne relèvent pas de la directive et disposent d'un système spécial de protection des données[50]. C'est pourquoi, bien que ces organismes soient désormais des institutions de l'Union, une appréciation de l'adéquation serait requise.

Néanmoins, et comme c'est souvent le cas pour les États membres dans le cadre des deuxième et troisième piliers, il existe une présomption d'adéquation car leur cadre juridique de protection des données est globalement conforme à la directive et au règlement. Dans ce cas, le responsable du traitement devrait apprécier l'adéquation (comme précisé au point 5.2 ci-dessus) pour s'assurer de la conformité effective.

8. Législation de l'Union et accords bilatéraux

Les institutions ou organes de l'Union peuvent être tenus par la législation de l'Union ou par des accords bilatéraux de procéder à des transferts internationaux, en agissant en qualité de responsables du traitement[51]. Le cas échéant, l'instrument devrait, idéalement, inclure le cadre approprié et nécessaire pour garantir la conformité avec l'article 9 du règlement.

Avant l'adoption de ce type d'instrument juridique, il convient de consulter le CEPD, conformément à l'article 28, paragraphe 2, du règlement.

Si le pays destinataire (dans le cas d'un accord bilatéral) n'a pas été déclaré adéquat par la Commission, l'instrument doit préciser si une adéquation existe (comme décrit au point 5.2 ci-dessus) ou si des «garanties suffisantes» ont été mises au point (comme décrit au point 6.2 ci-dessus). Dans ce dernier cas, les garanties suffisantes devraient former une partie intégrante de l'instrument, par exemple sous la forme d'une annexe. Il s'agit d'un exemple d'instrument juridique contraignant d'un type spécial, qui traite non seulement les aspects essentiels de l'accord lui-même, mais également les aspects pertinents relatifs à la protection des données à caractère personnel.

---

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_FR.pdf.

[49] Voir l'avis du Contrôleur européen de la protection des données du 24 novembre 2010 sur la communication de la Commission au Parlement européen et au Conseil intitulée «La politique antiterroriste de l'UE: principales réalisations et défis à venir», point 31, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-11-24_EU_counter-terrorism_FR.pdf.

[50] Décision du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) (2009/371/JAI), disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32009D0371&from=FR.
Dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel (2005/C 68/01), disponible à l'adresse suivante: http://eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection/Eurojust%20Data%20Protection%20Rules/Eurojust-Data-Protection-Rules-2005-02-24-FR.pdf.

[51] Voir, par exemple, les accords contenant des dispositions relatives à l'assistance mutuelle en matière douanière conclus avec des pays tiers (voir l'annexe 3).

Dans certains cas, la législation ou l'accord bilatéral en question est déjà en vigueur. Cependant, ces textes ne prévoient parfois pas le cadre approprié à une conformité avec l'article 9, ou n'incluent qu'une disposition très générale qui, même si elle contient quelques éléments positifs, est insuffisante pour procéder à un transfert licite[52].

Dans ces cas, une pratique courante consiste à inclure une clause type faisant référence à la confidentialité et à la protection des données à caractère personnel, en particulier pour certains types d'accords bilatéraux, par exemple dans le domaine de la coopération douanière. Ces clauses comprennent généralement une déclaration précisant que des données à caractère personnel ne peuvent être échangées que si le destinataire prend des mesures pour les protéger, de manière au moins équivalente par rapport à la partie exportatrice.

L'«équivalence» résulte notamment de l'harmonisation, à l'instar de la législation nationale en matière de protection des données après la transposition de la directive. Bien que le principe d'«adéquation» ne nécessite pas l'existence d'un système harmonisé, il exige toutefois le respect des principes fondamentaux tels que décrits au point 4.2. En outre, il ne peut être supposé que le niveau de protection «équivalent» sera garanti dans la pratique.

Par conséquent, la clause d'«équivalence» figurant dans ces accords bilatéraux ne garantit pas en soi la conformité avec l'article 9. Le cas échéant, le responsable du traitement devrait adopter des mesures complémentaires pour veiller à la conformité avec l'article 9, avant que le transfert ou l'ensemble de transferts n'aient lieu.

9. Supervision et mise en application

Comme décrit dans le document stratégique du CEPD intitulé «Contrôler et garantir le respect du règlement (CE) n° 45/2001»[53] (ci-après le «document stratégique sur la conformité»), le CEPD dispose de plusieurs outils de supervision et de mise en application, qui lui permettent de s'acquitter de sa mission de suivi de la conformité. Ces outils peuvent être utilisés dans les scénarios prévus à l'article 9, en fonction du type d'opération de traitement (en particulier le niveau de risque).

- Outils de supervision

– Contrôles préalables

[52] Voir par exemple l'article 17 de l'accord entre la Communauté européenne et la République de l'Inde relatif à la coopération et à l'assistance administrative mutuelle en matière douanière (JO L 304/25 du 30.9.2004), disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:22004A0930(01)&rid=8

[53] Document stratégique «Contrôler et garantir le respect du règlement (CE) n° 45/2001» adopté le 13 décembre 2010, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_FR.pdf.

Dans certains cas, le type d'opération de traitement associé au transfert peut relever des critères visés à l'article 27, paragraphe 2, du règlement. Le cas échéant, le responsable du traitement devrait présenter une notification de contrôle préalable au CEPD, décrivant clairement l'ensemble des aspects pertinents de la procédure.

Un contrôle préalable pourrait être requis le cas échéant, que le destinataire ait ou non été déclaré adéquat. Par exemple, si le traitement est lié à des données sanitaires devant être transférées vers un pays adéquat (comme la Suisse), le traitement doit tout de même être soumis à un contrôle préalable.

Dans d'autres cas, le CEPD peut avoir à traiter à la fois une demande d'avis (comme décrit au point 6.3) et un contrôle préalable, en raison de la nature de l'opération de traitement sous-jacente.

Il peut également être nécessaire de soumettre une notification de contrôle préalable à la lumière de l'article 27, paragraphe 1, du règlement, si les opérations de traitement sont susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées. Cette exigence pourrait s'appliquer, par exemple, aux informations traitées par voie de services d'informatique en nuage, dans certaines circonstances spécifiques à définir dans des lignes directrices ultérieures, en raison de la complexité et de la sensibilité des données[54]. Dans ce contexte, des données de clients sont souvent transférées vers des serveurs de prestataires de services en nuage et des centres de données situés dans diverses parties du monde. En l'absence d'emplacement stable des données, le CEPD pourrait avoir à vérifier s'il existe des garanties suffisantes effectivement conformes à l'article 9, et couvrant l'ensemble des destinataires potentiels susceptibles d'être associés à l'environnement en nuage. Cependant, cette exigence dépend également des conditions devant être convenues avec les prestataires de services d'informatique en nuage, de manière plus générale. À ce stade, il n'existe pas d'exigence supplémentaire de contrôle préalable.

– Consultations, traitement des plaintes, inspections

Le CEPD dispose d'autres outils de supervision pour garantir la conformité, par exemple la conduite de consultations, comme il est précisé ci-dessus. La politique en matière de consultation est pleinement applicable aux transferts relevant de l'article 9.

Toute personne concernée qui est affectée par un transfert peut soumettre une plainte au CEPD, conformément aux articles 32 et 33 du règlement, si elle considère que ses droits à la protection des données ont été violés.

Le CEPD pourrait également décider de procéder à des inspections pour vérifier la conformité avec l'article 9 du règlement ou recueillir des éléments de preuve dans le contexte de plaintes adressées.

[54] Voir l'avis du Contrôleur européen de la protection des données du 16 novembre 2012 relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_FR.pdf.

- Outils de mise en application

Les pouvoirs de mise en application du CEPD sont fixés à l'article 47 du règlement et sont commentés de manière exhaustive dans le document stratégique sur la conformité. La pratique du CEPD consiste à choisir l'action la plus efficace sur la base des objectifs visés. Pour ce qui concerne les transferts de données relevant de l'article 9, le CEPD a le pouvoir de:

* saisir le responsable du traitement en cas de violation alléguée du règlement et, le cas échéant, formuler des propositions tendant à remédier à cette violation;

* adresser un avertissement ou une admonestation au responsable du traitement;

* interdire temporairement ou définitivement un traitement;

* saisir l'institution ou l'organe de l'Union concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission;

* saisir la Cour de justice de l'Union européenne dans les conditions prévues par le traité;

* intervenir dans les affaires portées devant la Cour de justice de l'Union européenne.

Ces pouvoirs sont exercés au regard des circonstances spécifiques liées au système juridique du destinataire ou de toute pratique de traitement susceptible de menacer la protection des individus (voir le point 6.2.1 sur le pouvoir du CEPD d'interdire ou de suspendre la circulation de données).

ANNEXE 1

Article 9 du règlement (CE) n° 45/2001

Transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires et ne relevant pas de la directive 95/46/CE

1. Le transfert de données à caractère personnel à des destinataires autres que les institutions et organes communautaires, et qui ne sont pas soumis à la législation nationale adoptée en application de la directive 95/46/CE, ne peut avoir lieu que pour autant qu'un niveau de protection adéquat soit assuré dans le pays du destinataire ou au sein de l'organisation internationale destinataire, et que ce transfert vise exclusivement à permettre l'exécution des missions qui relèvent de la compétence du responsable du traitement.
2. Le caractère adéquat du niveau de protection offert par le pays tiers ou par l'organisation internationale en question s'apprécie au regard de toutes les circonstances entourant une opération ou un ensemble d'opérations de transfert de données. Il est notamment tenu compte de la nature des données, de la finalité et de la durée du (ou des) traitement(s) envisagé(s), du pays tiers ou de l'organisation internationale destinataire, de la législation, tant générale que sectorielle, en vigueur dans le pays tiers ou applicable à l'organisation internationale en question ainsi que des règles professionnelles et des mesures de sécurité appliquées dans ce pays ou dans cette organisation internationale.
3. Les institutions et organes communautaires informent la Commission et le contrôleur européen de la protection des données des cas dans lesquels ils estiment que le pays tiers ou l'organisation internationale en question n'assure pas un niveau de protection adéquat au sens du paragraphe 2.
4. La Commission informe les États membres des cas visés au paragraphe 3.
5. Les institutions et organes communautaires prennent les mesures nécessaires pour se conformer aux décisions prises par la Commission constatant, en application de l'article 25, paragraphes 4 et 6, de la directive 95/46/CE, qu'un pays tiers ou une organisation internationale assure ou n'assure pas un niveau de protection adéquat.
6. Par dérogation aux paragraphes 1 et 2, l'institution ou l'organe communautaire peut transférer des données à caractère personnel si:
a) la personne concernée a indubitablement donné son consentement au transfert envisagé, ou
b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée, ou
c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, ou
d) le transfert est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêt public importants ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou
e) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou
f) le transfert est effectué à partir d'un registre qui, conformément à la législation communautaire, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions fixées par la législation communautaire pour la consultation sont remplies dans le cas particulier.
7. Sans préjudice du paragraphe 6, le contrôleur européen de la protection des données peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat au sens des paragraphes 1 et 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.
8. Les institutions et organes communautaires informent le contrôleur européen de la protection des données des catégories de cas dans lesquels ils ont appliqué les paragraphes 6 et 7.

ANNEXE 2

Liste de contrôle à vérifier avant d'effectuer un transfert

Les responsables du traitement devraient associer leurs délégués à la protection des données dès le départ et solliciter leurs conseils et leur orientation pour garantir la conformité. Les actions et les vérifications juridiques ci-après devraient être conduites avant qu'un ou plusieurs transferts internationaux n'aient lieu:

Q. 1) Un niveau de protection adéquat est-il garanti dans le pays ou au sein de l'organisation internationale destinataire?

Vérifier la liste des décisions d'adéquation adoptées par la Commission: Andorre, l'Argentine, le Canada (secteur privé), les États-Unis (sphère de sécurité; pour certaines activités du secteur privé), Guernesey, les Îles Féroé, l'Île de Man, Israël, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay.

R: **Oui** – le transfert peut avoir lieu pour autant que les autres règles fixées par le règlement (CE) n° 45/2001 soient respectées.

R: **Non ou peut-être** – voir la question 2.

Participation du CEPD: il n'est pas nécessaire d'informer ou de consulter le CEPD, ni de demander son autorisation.

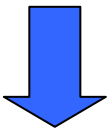
2) Existe-t-il d'autres raisons de penser qu'un niveau de protection adéquat est offert par le destinataire dans le pays tiers ou l'organisation internationale?

Le responsable du traitement doit procéder à une évaluation pour vérifier s'il existe un niveau de protection adéquat pour les transferts en question. Cette évaluation devrait se limiter aux finalités spécifiques et aux destinataires du pays tiers ou de l'organisation internationale de destination.

R: **Oui** – le transfert peut avoir lieu pour autant que l'évaluation de l'adéquation soit clairement documentée et que les autres règles fixées par le règlement (CE) n° 45/2001 soient respectées.

R: **Non** – voir la question 3.

Participation du CEPD: l'autorisation du CEPD n'est pas nécessaire. Nous pourrions être consultés dans certaines circonstances (vérifier la politique du CEPD relative aux consultations dans le domaine de la supervision et de la mise en application).



3) Une dérogation s'applique-t-elle?

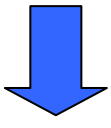
Le transfert n'est-il effectivement *pas* répété, massif ou structurel et l'un des critères ci-après s'applique-t-il?

a) la personne concernée a indubitablement donné son consentement au transfert envisagé, ou
b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou
c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, ou
d) le transfert est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêt public importants ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou
e) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou
f) le transfert est effectué à partir d'un registre qui est destiné à l'information du public.

R: **Oui** – le transfert peut avoir lieu pour autant qu'il ne soit pas répété, massif ou structurel. L'une des conditions visées à l'article 9, paragraphe 6, du règlement (CE) n° 45/2001 devrait également être remplie et toutes les autres règles fixées par le règlement (CE) n° 45/2001 devraient être respectées.

R: **Non** – voir la question 4.

Participation ex ante du CEPD: l'autorisation du CEPD n'est pas nécessaire. Nous pourrions être consultés dans certaines circonstances (vérifier la politique du CEPD relative aux consultations dans le domaine de la supervision et de la mise en application).



4) Le responsable du traitement offre-t-il des «garanties suffisantes»?

Les «garanties suffisantes» sont des garanties en matière de protection des données, instaurées sur une base ad hoc et qui n'existent pas déjà dans la pratique ou le système juridique du destinataire dans le lieu de destination. L'objectif de ces garanties est de créer une protection là où elle peut faire défaut dans le pays où l'organisation internationale de destination des données, dans les cas où des dérogations ne sont pas applicables.

R: **Oui** – le transfert peut avoir lieu pour autant que les autres règles fixées par le règlement (CE) n° 45/2001 soient respectées.

R: **Non** – le transfert ne peut pas avoir lieu.

Participation du CEPD: trois scénarios doivent être envisagé pour déterminer si le CEPD doit ou non être associé:

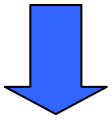
- aucune autorisation ou consultation préalable nécessaire:
  lorsque des clauses contractuelles types sont utilisées;

- aucune autorisation préalable nécessaire, mais une consultation pourrait l'être:
  (vérifier la politique du CEPD en matière de consultation dans le domaine de la supervision et de la mise en application); par exemple, lorsqu'un instrument contraignant spécifique (par opposition aux clauses contractuelles types) est mis au point par l'institution ou l'organe de l'Union en vue de son utilisation dans le cadre du droit tant privé que public;

- une autorisation préalable est nécessaire:
  dans certains cas exceptionnels, lorsque les transferts s'appuient sur des garanties spécifiques et ne sont pas intégrés à un instrument juridiquement contraignant.

Le CEPD pourrait également décider qu'une autorisation est nécessaire dans d'autres cas qui lui sont soumis pour consultation, en fonction du niveau de risque du système de transfert.

Lorsqu'une autorisation préalable est sollicitée, une analyse complète de l'«adéquation» (et du projet d'instrument(s)) devrait être présentée au CEPD.



5) Vérifier si l'opération de traitement sous-jacente a été soumise à un contrôle préalable et en informer le CEPD lorsque c'est nécessaire.

ANNEXE 3

Liste de demandes d'autorisation (article 9, paragraphe 7) et de consultation administrative [article 28, paragraphe 1, et article 46, point d)] et échantillon de demandes de consultation législative (article 28, paragraphe 2) soumises au CEPD en lien avec l'article 9.

Demandes d'autorisation (article 9, paragraphe 7)

- Décision du CEPD du 13 février 2014 concernant les transferts de données à caractère personnel effectués par l'OLAF par l'intermédiaire de la plateforme de consultation des données relatives aux enquêtes conformément à l'article 9, paragraphe 7, du règlement (CE) n° 45/2001, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_EN.pdf; annexe – projet de dispositif de coopération administrative entre l'«Office européen de lutte antifraude» (OLAF) et [le partenaire], disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2014/14-02-13_Letter_Kessler_Decision_Annex_EN.pdf.

Consultations administratives [article 28, paragraphe 1, et article 46, point d)]

- Réponse du 16 juillet 2012 à une consultation sur un modèle révisé de clauses contractuelles en matière de protection des données de l'OLAF à utiliser dans le cadre des accords de coopération administrative conclus avec les autorités de pays tiers ou des organisations internationales (dossier 2012-0086), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-07-16Model%20Data%20Protection%20Clauses_OLAF_D-1051_EN.pdf.
- Réponse du 3 avril 2012 à une consultation sur un modèle révisé de clauses contractuelles en matière de protection des données de l'OLAF à utiliser dans le cadre des accords de coopération administrative conclus avec les autorités de pays tiers ou des organisations internationales (dossier 2012-0086), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2012/12-04-03 %20Model%20Data%20Protection%20Clauses_OLAF_D-746_EN.pdf.
- Réponse du 4 octobre 2010 au délégué à la protection des données de l'Agence européenne de la sécurité aérienne concernant les transferts internationaux, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2010/10-10-04_Letter_DPO_EASA_FR.pdf.
- Réponse du 21 décembre 2010 à une consultation concernant le transfert par l'EFSA de données à caractère personnel d'experts externes de l'EFSA à destination d'American Express Corporate Travel SA (AMEX) (dossier 2009-

390), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Consultations/2010/10-12-21_EFSA_AMEX_FR.pdf.

- Réponse du 2 juillet 2009 à une consultation sur les transferts de données à caractère personnel dans des pays tiers: «adéquation» des signataires à la convention 108 du Conseil de l'Europe, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-07-02_OLAF_transfer_third_countries_EN.pdf.

- Réponse du 6 mai 2009 à une consultation sur des questions relatives au traitement des transferts de données à caractère personnel par l'OLAF, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/2009/09-05-06_OLAF_transfers_EN.pdf.

Exemples de consultations législatives (article 28, paragraphe 2)

- Avis du 14 mars 2014 sur la proposition de décision du Conseil sur la position à adopter, au nom de l'Union européenne, au sein du comité mixte de coopération douanière UE-Chine, en ce qui concerne la reconnaissance mutuelle du programme relatif aux opérateurs économiques agréés de l'Union européenne et des mesures relatives au programme de mesures de la République populaire de Chine sur la gestion par catégorie des entreprises, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-14_EU-China_Customs_FR.pdf.

- Avis du 20 février 2014 sur la communication de la Commission au Parlement européen et au Conseil relative au «rétablissement de la confiance dans les flux de données entre l'Union européenne et les États-Unis» et sur la communication de la Commission au Parlement européen et au Conseil relative au «fonctionnement de la sphère de sécurité du point de vue des citoyens de l'UE et des entreprises établies sur son territoire, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_FR.pdf.

- Avis du 9 février 2012 sur la proposition de décision du Conseil relative à une position à prendre par l'Union au sein du comité mixte de coopération douanière Union européenne-États-Unis concernant la reconnaissance mutuelle du programme relatif aux opérateurs économiques agréés de l'Union européenne et du programme de partenariat douane-commerce contre le terrorisme des États-Unis, JO C 160/01 du 6.6.2012, p. 1, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-02-09_EU_US_Joint_Customs_FR.pdf.

- Avis du 12 mars 2010 sur la proposition de décision du Conseil relative à une position à prendre par l'Union au sein du comité mixte de coopération

douanière UE- Japon concernant la reconnaissance mutuelle des programmes relatifs aux opérateurs économiques agréés dans l'Union européenne et au Japon, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-12_EU-Japan_FR.pdf.