EUROPEAN DATA PROTECTION SUPERVISOR

Avis nº 1/2016

Avis préliminaire relatif à l'accord entre les États-Unis d'Amérique et l'Union européenne concernant la protection des informations à caractère personnel afin de prévenir et de détecter les infractions pénales et de procéder aux enquêtes et poursuites en la matière

12 février 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée, en vertu de l'article 41, paragraphe 2, du règlement (CE) nº 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Le contrôleur européen et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'être constructifs et proactifs. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis découle de l'obligation générale exigeant que les accords internationaux conclus par l'Union soient conformes aux dispositions du traité sur le fonctionnement de l'Union européenne (TFUE) et respectent les droits fondamentaux qui forment le noyau du droit de l'Union. En particulier, l'évaluation vise à examiner la conformité du contenu de l'*Umbrella Agreement* (accord-cadre) avec les articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne et avec l'article 16 TFUE, qui garantissent la protection des données à caractère personnel.

SYNTHÈSE

Les enquêtes et poursuites d'infractions constituent un objectif politique légitime, et la coopération internationale, y compris l'échange d'informations, n'a jamais été aussi importante. Jusqu'à présent, l'Union a manqué d'un cadre commun robuste dans ce domaine, de sorte qu'il n'existe pas de garanties cohérentes pour les droits fondamentaux et les libertés des personnes. Comme le préconise le CEPD depuis longtemps, **l'Union doit conclure avec des pays tiers des accords viables concernant le partage de données à caractère personnel à des fins répressives, lesquels doivent être pleinement compatibles avec les traités et la Charte des droits fondamentaux de l'Union européenne**.

Par conséquent, **nous saluons et soutenons activement les efforts déployés par la Commission européenne en vue de conclure un premier *Umbrella Agreement* avec les États-Unis.** Cet accord répressif international a pour objectif de faire en sorte que le partage d'informations se base, pour la première fois, sur la protection des données. Si nous reconnaissons qu'il est impossible de reproduire entièrement la terminologie et les définitions du droit de l'Union dans un accord avec un pays tiers, les garanties pour les personnes doivent être claires et efficaces afin d'être pleinement conformes au droit primaire de l'Union.

Ces dernières années, la Cour de justice de l'Union européenne a confirmé les principes relatifs à la protection des données, y compris l'équité, l'exactitude et la pertinence des informations, la supervision indépendante et les droits individuels des personnes. **Ces principes sont importants tant pour les instances publiques que pour les sociétés privées, indépendamment de tout constat d'adéquation officiel de l'Union** par rapport aux garanties instaurées par des pays tiers à l'égard de la protection des données. En effet, ces principes deviennent sans cesse plus importants compte tenu de la sensibilité des données nécessaires aux enquêtes pénales.

Le présent avis vise à fournir des recommandations constructives et objectives aux institutions de l'Union alors que la Commission finalise cette tâche délicate, qui a de vastes conséquences non seulement en matière de coopération en matière répressive entre l'Union et les États-Unis, mais aussi pour les accords internationaux futurs. L'«Umbrella Agreement» est distinct du «EU-US Privacy Shield» (bouclier de protection des données UE-États-Unis), récemment annoncé, concernant le transfert d'informations à caractère personnel dans l'environnement commercial, mais doit être examiné en conjonction avec celui-ci. D'autres considérations peuvent s'avérer nécessaires pour analyser l'interaction entre ces deux instruments et la réforme du cadre de protection des données de l'Union.

Avant que l'accord ne soit soumis à l'approbation du Parlement européen, nous encourageons les parties à examiner de près les évolutions significatives intervenues depuis septembre dernier, moment auquel elles ont signalé leur intention de conclure l'accord dès l'adoption du *Judicial Redress Act* (loi américaine relative au recours juridictionnel). Nous saluons nombre de garanties déjà envisagées, mais celles-ci doivent être renforcées, notamment à la lumière de l'arrêt Schrems rendu en octobre, qui invalide la décision relative à la sphère de sécurité (*Safe Harbor*), et de l'accord politique de l'Union relatif à la réforme de la protection des données adopté en décembre, qui couvre les transferts de données et la coopération judiciaire et policière.

Le CEPD a décelé trois améliorations essentielles qu'il recommande d'apporter au texte afin de garantir sa conformité avec la Charte et l'article 16 du traité:

- clarification selon laquelle toutes les garanties s'appliquent à tous, pas seulement aux ressortissants de l'Union;
- garantie que les dispositions en matière de recours juridictionnel soient efficaces au sens de la Charte;
- clarification selon laquelle les transferts massifs de données sensibles ne sont pas autorisés.

L'avis offre des recommandations supplémentaires visant à clarifier les garanties envisagées en joignant à l'accord un document explicatif. Nous nous tenons à la disposition des institutions pour des conseils complémentaires et un dialogue à ce sujet.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7, 8 et 47,

vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 41, paragraphe 2, et son article 46, point d),

A ADOPTÉ LE PRÉSENT AVIS:

I. Contexte de l'accord paraphé

1. Le 3 décembre 2010, le Conseil a adopté une décision autorisant la Commission à engager des négociations entre l'Union européenne (UE) et les États-Unis en vue de la conclusion d'un accord relatif à la protection des données à caractère personnel lorsqu'elles sont transférées et traitées afin de prévenir et de détecter les infractions pénales, dont les actes terroristes, et de procéder aux enquêtes et poursuites en la matière, dans le cadre de la coopération policière et judiciaire en matière pénale (ci-après, l'«accord»)[1].

2. Les négociations entre la Commission et les États-Unis ont été engagées officiellement le 29 mars 2011[2]. Le 25 juin 2014, le procureur général des États-Unis a annoncé que des mesures législatives allaient être prises afin de prévoir un recours juridictionnel concernant le droit au respect de la vie privée aux États-Unis pour les citoyens de l'UE[3]. Au terme de plusieurs cycles de négociations, qui se sont étalés sur plus de quatre ans, l'accord a été paraphé le 8 septembre 2015. D'après la Commission, l'objectif est de signer et de conclure officiellement l'accord uniquement après l'adoption du *Judicial Redress Act* américain (loi sur le recours juridictionnel)[4].

3. Le Parlement européen doit approuver le texte paraphé de l'accord tandis que le Conseil doit le signer. Tant que cela n'est pas fait et que l'accord n'a pas été officiellement signé, nous signalons que les négociations peuvent être rouvertes sur des points spécifiques. C'est dans ce contexte que le CEPD rend le présent avis, basé sur le texte paraphé, publié sur le site internet de la Commission[5]. Il s'agit d'un avis préliminaire basé sur une première analyse d'un texte juridique complexe, qui est sans préjudice d'éventuelles recommandations supplémentaires qui pourraient être formulées sur la base de nouvelles informations disponibles, y compris les avancées législatives aux États-Unis, comme l'adoption du *Judicial Redress Act*. Le CEPD a identifié trois points essentiels qui doivent faire l'objet d'améliorations et met également en évidence d'autres aspects pour lesquels d'importantes clarifications sont recommandées. S'il intègre ces améliorations, l'accord peut être considéré comme conforme au droit primaire de l'Union.

II. Normes du droit de l'Union concernant les transferts internationaux de données et le respect des droits fondamentaux

4. Conformément à l'article 216, paragraphe 2, TFUE, les accords internationaux auxquels l'Union est partie, comme l'accord concerné, «*lient les institutions de l'Union et les États membres*». En outre, conformément à une jurisprudence constante de la Cour de justice de l'Union européenne (CJUE), les accords internationaux «*forment partie intégrante*», dès leur entrée en vigueur, «*de l'ordre juridique [européen]*»[6] et bénéficient de la primauté sur les actes de droit dérivé de l'Union[7].

5. La CJUE a constaté à l'égard des accords internationaux conclus par l'Union que «les obligations qu'impose un accord international *ne sauraient avoir pour effet de porter atteinte aux principes constitutionnels du traité CE, au nombre desquels figure le principe selon lequel tous les actes communautaires doivent respecter les droits* fondamentaux, ce respect constituant une condition de leur légalité qu'il incombe à la Cour de contrôler dans le cadre du système complet de voies de recours qu'établit ce traité»[8]. L'analyse ultérieure prend pour point de départ l'exigence selon laquelle les accords internationaux doivent être conformes au système de l'Union pour la protection des droits fondamentaux.

6. À la lecture des différents instruments juridiques en vigueur dans les différents domaines d'application, nous pouvons conclure que le régime juridique de l'Union applicable à la protection des données, qui doit aujourd'hui être interprété à la lumière de l'article 8 de la Charte et de l'article 16 TFUE, prévoit en principe que les transferts internationaux de données vers un pays tiers ne peuvent avoir lieu sans exigence supplémentaire que lorsque ce pays garantit un niveau de protection adéquat[9]. Lorsqu'il est établi que le pays tiers ne garantit pas un niveau de protection adéquat, des exceptions s'appliquent aux transferts *spécifiques*, pour autant que des garanties appropriées soient produites.

7. Le dernier cycle de négociations concernant l'accord s'est achevé avant qu'interviennent deux évolutions importantes dans l'Union: l'accord politique relatif au train de réformes sur la protection des données, y compris le règlement général sur la protection des données[10] et la directive relative à la protection des données en matière pénale, et l'arrêt de la Cour de justice dans l'affaire Schrems[11], invalidant la décision relative à la sphère de sécurité.[12] Bien que cet arrêt ne concerne pas directement les transferts internationaux de données dans le domaine répressif, nous recommandons d'en tenir compte dans l'évaluation du rôle que jouera l'accord dans le système juridique de protection des données de l'Union. En effet, les constatations principales[13] de la Cour interprètent ou appliquent directement les articles 7, 8 et 47 de la Charte en rapport avec les transferts[14], lesquels s'appliquent tous également dans le domaine répressif.

8. Le cadre juridique de l'Union pour la protection des données dans le domaine répressif est en cours de modernisation. Le cadre actuel se compose de plusieurs sources juridiques différentes, telles que:

a) la décision-cadre 2008/977/JAI du Conseil[15] (ci-après, la «décision-cadre»), qui s'applique aux transferts de données internationaux dans le domaine répressif lorsque les données transférées ont été initialement mises à la disposition de l'État membre qui procède au transfert par les autorités compétentes d'un autre État membre;

b) le règlement (CE) nº 45/2001[16], qui s'applique aux transferts de données internationaux lorsque les données sont transférées par une institution ou un organe de l'Union;
c) une série d'actes de droit dérivé de l'Union - *lex specialis*, qui s'appliquent aux transferts spécifiques de données dans le domaine répressif, interdisant soit complètement les transferts[17], soit avec des exceptions très strictes[18], soit en exigeant des garanties comme l'existence d'un niveau de protection adéquat dans l'état réceptionnant les données[19];
d) des accords internationaux spécifiques conclus tant au niveau de l'Union qu'au niveau des États membres, qui servent de bases juridiques pour les transferts[20];
e) des actes législatifs des États membres en matière de protection des données, qui régissent d'autres transferts dans le domaine répressif.

Si les instruments de transfert sont très variés, leur cohérence est assurée par l'application horizontale de la Charte et du TFUE susmentionnés. Il convient également de souligner que tous les États membres sont signataires de la Convention nº 108 du Conseil de l'Europe[21], qui s'applique dans le domaine répressif et qui est également en cours de modernisation.

9. L'évaluation ci-après de l'accord proposé tiendra compte des normes actuelles du droit de l'Union susmentionnées, qui ont trait aux transferts internationaux de données à caractère personnel, telles qu'elles sont interprétées par la CJUE, et de leur modernisation prévue.

III. Objet, champ d'application et effets de l'accord

1. Niveau élevé de protection

10. Conformément à l'article 1er, paragraphe 1, de l'accord, l'accord vise à «*garantir un niveau élevé de protection des informations à caractère personnel*» et à «*renforcer la coopération entre les États-Unis et l'Union européenne au niveau de la prévention et de la détection des infractions pénales, dont les actes terroristes, ainsi que des enquêtes ou des poursuites en la matière*». Les deux parties contractantes reconnaissent au premier paragraphe du préambule qu'elles sont toutes deux «*résolues à garantir un niveau élevé de protection des informations à caractère personnel échangées dans le cadre de la prévention et de la détection des infractions pénales, ainsi que des enquêtes et poursuites en la matière*». Par conséquent, l'accord reconnaît la nécessité d'un seuil de protection élevé en vue de son application future. Le CEPD salue cette conclusion, qui est conforme au cadre juridique général de l'Union en matière de protection de données[22] et à la jurisprudence de la CJUE en matière d'interprétation et d'application du droit à la protection des données à caractère personnel, inscrit à l'article 8 de la Charte[23]. Toutefois, le CEPD souligne que pour que le niveau élevé de protection soit efficace et conforme au droit primaire de l'Union, il est nécessaire qu'il se reflète pleinement dans les dispositions de l'accord et dans leur application ultérieure.

2. Présomption de conformité et autorisations

11. En ce qui concerne l'effet de l'accord, l'article 5, paragraphe 3, de l'accord dispose que «*en donnant effet au paragraphe 2*», qui concerne la mise en œuvre en droit interne, «***le traitement d'informations à caractère personnel*** *par les États-Unis ou l'Union européenne et ses États membres, dans les matières relevant du champ d'application du présent accord,* ***est réputé conforme à leur législation respective en matière de protection des données*** *restreignant ou conditionnant les transferts internationaux d'informations à caractère*

personnel, et ***aucune autre autorisation prévue par cette législation n'est requise***». L'article 5, paragraphe 3, de l'accord semble établir que lorsque les parties ont mis en œuvre dans leur système juridique national les dispositions de l'accord, chaque traitement de données à caractère personnel relevant du champ d'application matériel de l'accord est supposé respecter les lois nationales en matière de protection des données des pays exportateurs qui régissent les transferts internationaux de données.

12. Le libellé de cette disposition est similaire à celui utilisé dans l'accord entre l'Union et les États-Unis sur les données PNR, qui établit le caractère adéquat du système de traitement et d'utilisation des données PNR du ministère américain de la sécurité intérieure (article 19 «Caractère adéquat»)[24]. Toutefois, l'accord ne constitue pas une décision sur le caractère adéquat[25] et ne constitue pas un instrument juridique autonome dans la mesure où il complète la base juridique spécifique pour les transferts.

13. Néanmoins, l'accord crée une présomption générale de conformité. Subordonnés à l'existence d'une base juridique spécifique, les futurs transferts ne nécessiteront aucune autorisation. Par conséquent, il est essentiel que cette «présomption» soit renforcée par toutes les garanties nécessaires dans le texte de l'accord.

14. L'«architecture» de l'article 5 de l'accord indique que le paragraphe 3 dudit article ne prendra effet que lorsque son paragraphe 2 sera pleinement appliqué. L'article 5, paragraphe 2, exige des parties qu'elles prennent toutes les mesures qui s'imposent pour mettre l'accord en œuvre, en particulier les dispositions relatives à l'accès, à la rectification et aux recours administratif et juridictionnel. Il dispose en outre clairement que «*les protections et recours établis dans le présent accord profitent aux personnes et aux entités* ***de la manière mise en œuvre dans la législation nationale applicable de chaque partie***», ce qui signifie que, pour être efficace («pour profiter aux personnes et aux entités»), l'accord doit être mis en œuvre dans les systèmes juridiques nationaux des parties. Une analyse plus approfondie est nécessaire afin de vérifier dans quelle mesure, à la lumière également de la jurisprudence Medellin[26], l'accord peut être considéré comme un accord d'application directe dans l'ordre juridique américain et quelles sont les dispositions fondamentales susceptibles de devoir être mises en œuvre par le Congrès américain pour en faire une loi nationale contraignante.

15. L'accord fait référence à des mesures à intégrer dans le cadre juridique applicable des parties. Toutefois, il ne semble pas fournir un mécanisme spécifique permettant d'évaluer le niveau de sa mise en œuvre dans le droit national des parties afin de donner effet à l'article 5, paragraphe 3, de l'accord. Le mécanisme conjoint d'évaluation périodique prévu à l'article 23 semble avoir pour objectif général d'évaluer l'efficacité «des politiques et procédures de mise en œuvre du présent accord» et oblige les parties à mener la première évaluation conjointe «au plus tard trois ans à compter de la date d'entrée en vigueur» de l'accord. Dans ce contexte, une question essentielle est de savoir «*quand les transferts de données dans des matières relevant du champ d'application de l'accord peuvent-ils* ***être réputés conformes*** *aux exigences de la législation européenne en matière de protection de données restreignant ou conditionnant les transferts internationaux, sans qu'aucune autorisation soit nécessaire*?».

16. Considérant le fait que l'article 5, paragraphe 3, de l'accord soustrait aux autorités concernées (autorités de contrôle de la protection des données ou autres institutions, en fonction du système juridique de l'État membre de l'Union) le pouvoir d'autoriser les transferts, le CEPD rappelle que l'institution, dans les États membres de l'Union, d'autorités de contrôle nationales indépendantes est un élément essentiel[27] du respect de la protection des

personnes à l'égard du traitement de leurs données à caractère personnel[28]. Les autorités de contrôle nationales sont chargées du contrôle du respect de la législation de l'Union en matière de protection des données, conformément à l'article 8, paragraphe 3, de la Charte, et chaque autorité est investie de la compétence de vérifier si un transfert de données à caractère personnel depuis l'État membre dont elle relève vers un pays tiers respecte la législation en matière de protection des données même lorsque le système juridique d'un pays tiers a été jugé adéquat[29] ou qu'une présomption de conformité est introduite sur la base d'un accord. Par conséquent, le CEPD observe que l'absence de toute autre autorisation des transferts, conformément à l'article 5, paragraphe 3, de l'accord, ne préjuge pas des compétences et pouvoirs des autorités de contrôle indépendantes à surveiller la légalité des transferts et la conformité de ceux-ci avec la législation en matière de protection des données, également sur la base de l'article 21 de l'accord. Dès lors, l'article 5, paragraphe 3, de l'accord doit être interprété comme respectant ce rôle des autorités de contrôle, se conformant ainsi à l'article 8, paragraphe 3, de la Charte. Le CEPD recommande que, pour plus de clarté, cette conclusion soit insérée dans une déclaration explicative de l'accord.

3. Relation entre l'accord et les bases juridiques spécifiques des transferts

17. Il ressort du second paragraphe du préambule que l'accord vise «*à faciliter l'échange d'informations*» dans les domaines pertinents en matière pénale en établissant un «*cadre pour la protection des informations à caractère personnel lors de leur transfert*» entre les parties (article 1er, paragraphe 2). Il est en outre clairement indiqué à l'article 1er, paragraphe 3, que l'accord «*n'est en soi pas une base juridique pour les transferts d'informations à caractère personnel*» et qu'«*une base juridique sera toujours requise pour ces transferts*». Le cadre juridique complet fournissant les garanties pour les transferts couverts par l'accord se compose des dispositions de l'accord, de la manière dont elles sont mises en œuvre dans le droit national des parties et de la base juridique spécifique applicable aux transferts. Le rapport entre l'accord et les bases juridiques ultérieures pour les transferts entre les parties est très important. Nous lisons l'article 5, paragraphe 1, dans le sens que tous les instruments spécifiques fournissant la base juridique des transferts doivent se conformer aux exigences de l'accord, qui doivent être considérées comme fournissant un niveau de protection minimum pour les transferts. À des fins de sécurité juridique, le CEPD recommande aux parties d'envisager de confirmer, du moins dans les déclarations explicatives accompagnant l'accord, que les bases juridiques spécifiques des transferts doivent satisfaire pleinement aux garanties fournies dans l'accord et que, dans le cas de dispositions contradictoires entre la base juridique spécifique et l'accord, ce dernier prévaudra.

4. Transferts vers des autorités publiques

18. L'article 5, paragraphe 2, de l'accord précise que «*pour les États-Unis, leurs obligations s'appliquent de manière à être conformes à leurs principes de fédéralisme fondamentaux*». Cette disposition pourrait avoir une incidence sur les transferts en provenance d'autorités fédérales compétentes aux États-Unis qui sont les destinataires initiaux de données vers des autorités des États fédérés, qui ne sont pas liées par l'accord. En ce sens, l'article 2, paragraphe 5, définit l'«autorité compétente» aux États-Unis comme étant une «*autorité répressive nationale, responsable de la prévention et de la détection des infractions pénales, dont les actes terroristes, et des enquêtes et poursuites en la matière*», ce qui exclut donc les autorités au niveau des États fédérés[30]. En revanche, toutes les autorités de l'Union et ses États membres qui sont compétentes dans les mêmes domaines sont liées par l'accord, conformément à la définition de l'article 2, paragraphe 5.

19. Certaines incidences potentiellement négatives de la clause analysée à l'article 5, paragraphe 2, peuvent être atténuées par l'article 14, paragraphe 2, de l'accord, conformément auquel les transferts de données du niveau fédéral vers les États fédérés peuvent être interrompus si les États fédérés «*n'ont pas protégé efficacement les informations à caractère personnel, en tenant compte de l'objet du présent accord*». Le CEPD salue cette disposition, mais recommande de préciser, du moins dans les déclarations explicatives accompagnant l'accord, qu'en cas de protection inefficace des données transférées vers les États fédérés, les mesures pertinentes au titre de l'article 14, paragraphe 2, incluront, si nécessaire, des mesures concernant les données déjà partagées.

5. Exemption au titre de la sécurité nationale

20. L'article 3 établit que l'accord s'applique aux «*informations à caractère personnel transférées*» entre les autorités compétentes des parties ou «*autrement transférées conformément à un accord*» entre les États-Unis et l'Union ou ses États membres «*afin de prévenir et de détecter les infractions pénales, dont les actes terroristes, et de procéder aux enquêtes et poursuites en la matière*». Le CEPD se félicite que les accords bilatéraux entre les *États membres* et les États-Unis ont aussi été inclus dans le champ d'application de l'accord. Nous observons également que les «transferts *ou autres formes de coopération entre les autorités des États membres et des États-Unis autres que celles visés à l'article 2, paragraphe 5, responsables de la protection de la sécurité nationale*» ne relèvent pas du champ d'application de l'accord, conformément à l'article 3, paragraphe 2.

21. Toutefois, compte tenu de la définition large d'une «*autorité compétente*» prévue à l'article 2, paragraphe 5, qui, eu égard aux autorités américaines, renvoie à une «*autorité répressive nationale responsable de la prévention et de la détection des infractions pénales, dont les actes terroristes, et des enquêtes et poursuites en la matière*», lue en combinaison avec les dispositions de l'article 6, paragraphe 2, qui garantit que le traitement ultérieur d'informations à caractère personnel partagées «*par d'autres autorités répressives, réglementaires ou administratives nationales respecte les autres dispositions du présent accord*», nous comprenons que les autorités nationales chargées de protéger la sécurité nationale seront soumises aux dispositions de l'accord lors du traitement des données transférées aux fins prévues dans l'accord. Le cas échéant et par souci de clarté, cette conclusion peut être insérée dans une déclaration explicative de l'accord. Enfin, le CEPD observe que la définition large d'«autorité compétente» couvre également les ministères publics et les autorités judiciaires dans la mesure où ils effectuent les tâches susmentionnées dans le domaine pénal.

6. Transferts de données de parties privées vers des autorités compétentes

22. Le CEPD observe que si l'accord s'applique essentiellement aux données transférées entre des autorités compétentes des parties, il peut également s'appliquer aux transferts de données entre des parties privées et des autorités compétentes, pour autant qu'un accord soit conclu entre les États-Unis et l'Union ou ses États membres. À cet égard, l'article 3, paragraphe 1, spécifie que l'accord s'applique aux données à caractère personnel transférées entre des autorités compétentes «*ou autrement transférées conformément à un accord conclu entre les États-Unis et l'Union ou ses États membres*» dans le domaine répressif. Par conséquent, nous comprenons que l'accord puisse aussi couvrir les transferts de données de sociétés privées, comme des transporteurs aériens (p.ex. transferts de données PNR) ou des

prestataires de services qui offrent des services de communications électroniques accessibles au public, vers les autorités compétentes des parties, mais uniquement lorsque ces transferts sont basés sur un accord international.

7. Application des garanties aux personnes

23. L'article 3 («Champ d'application») ne contient aucune référence spécifique au champ d'application *rationae personae* de l'accord. Il établit un champ d'application *rationae personae* large en établissant que l'accord s'applique à (toute) «*information à caractère personnel transférée*» entre les parties dans le domaine répressif. Cette référence générale aux informations à caractère personnel semble impliquer que les informations à caractère personnel de toute personne bénéficient de la même manière des garanties inscrites dans l'accord. Cette interprétation est encouragée par des références spécifiques à un champ d'application personnel large de l'article 16 «Accès», de l'article 17 «Rectification» et de l'article 18 «Recours administratif» (puisqu'ils renvoient à «toute personne»). Elle peut toutefois être contredite par la disposition générale de «non-discrimination» de l'article 4. Conformément à cet article, chaque partie doit satisfaire aux obligations qui lui incombent au titre de l'accord afin de protéger les «*informations à caractère personnel de ses propres ressortissants et des ressortissants de l'autre partie*» sans discrimination arbitraire. En outre, l'article 19 «Recours juridictionnel» ne s'applique qu'aux «citoyens» des parties.

24. S'il est mis en œuvre en excluant toute personne autre que les ressortissants de l'Union du champ d'application personnel de l'accord, l'accord ne serait pas conforme à la protection conférée par les articles 7, 8 et 47 de la Charte, selon lesquels les droits fondamentaux au respect de la vie privée, à la protection des données à caractère personnel et à un recours effectif s'appliquent à «toute personne» dans l'Union, indépendamment de sa nationalité ou de son statut. Par conséquent, le CEPD recommande d'apporter une clarification importante à l'accord, du moins dans ses déclarations explicatives, afin de confirmer que son champ d'application personnel est conforme à la Charte.

IV. Analyse des dispositions fondamentales de l'accord

1. Définitions

25. Le régime juridique de l'Union en matière de protection des données prévoit des définitions bien établies de concepts tels que «données à caractère personnel» et «traitement [de données à caractère personnel]». Bien que la terminologie choisie pour le texte de l'accord diffère en partie du régime juridique pertinent dans l'Union (l'accord faisant référence aux «informations à caractère personnel» et non aux «données à caractère personnel»), le CEPD salue la définition large, à l'article 2, paragraphe 1, des «informations à caractère personnel», qui est conforme à la définition correspondante des «données à caractère personnel» établie dans la directive 95/46/CE et dans le règlement (CE) nº 45/2001. Toutefois, la définition figurant à l'article 2, paragraphe 1, de l'accord ne renvoie pas à «toute information», mais aux «informations». Dès lors, par exemple, des doutes peuvent surgir quant à savoir si des métadonnées faisant référence à une personne identifiée ou identifiable seront considérées comme des informations à caractère personnel dans le cadre de l'accord.

26. En ce qui concerne la définition du «traitement des informations à caractère personnel» à l'article 2, paragraphe 2, de l'accord, certaines différences fondamentales sont observées par rapport à la définition du «traitement des données à caractère personnel» inscrite dans la décision-cadre, dans la directive 95/46/CE et dans le règlement (CE) nº 45/2001. Comme

défini dans l'accord, le «traitement des informations à caractère personnel» signifie «*toute opération ou ensemble d'opérations telles que la collecte, la mise à jour, l'utilisation, la modification, l'organisation ou la structuration, la divulgation ou la diffusion ou la mise à disposition*». Contrairement aux instruments pertinents de l'Union, cette définition exclut du champ d'application de l'accord des opérations telles que «*l'enregistrement, la conservation, l'extraction, la consultation, le rapprochement ou l'interconnexion, le verrouillage, l'effacement ou la destruction*». Par ailleurs, l'article 2, paragraphe 1, de l'accord fait référence, contrairement à la définition prévue dans le régime juridique de l'Union, à la «*mise à jour*» et à la «*mise à disposition*». Ces deux notions ne semblent pas couvrir la signification des opérations énumérées dans le droit de l'Union.

27. Une clarification est recommandée afin d'assurer l'application des garanties prévues dans l'accord pour les opérations clés, par exemple lorsqu'une autorité compétente consigne des données ou lorsque l'autorité se contente de stocker les informations qu'elle reçoit, sans faire d'autre usage des informations. Il convient également de préciser que la «consultation», qui est également absente de la définition, est couverte par le terme «utilisation», dans la mesure où une utilisation abusive trouve souvent son origine dans une consultation illégitime de données à caractère personnel.

28. Le CEPD recommande donc que la définition des opérations de traitement soit mise en conformité avec les exigences fondamentales du droit de l'Union afin d'inclure les opérations clés susmentionnées, telles que l'enregistrement et la conservation des informations. Dans le cas où les parties n'alignent pas totalement les définitions d'«informations à caractère personnel» et d'«opération de traitement» sur celles prévues par le droit de l'Union, le CEPD recommande de clarifier dans les documents explicatifs accompagnant l'accord que l'application des deux notions ne différera pas substantiellement de la manière dont elles sont comprises dans le droit de l'Union.

2. Limitation de la finalité et transferts ultérieurs

29. Le CEPD salue la reconnaissance des principes de proportionnalité et de nécessité établis au dernier paragraphe du préambule. À la lumière de cette considération, l'article 6, paragraphe 1, de l'accord limite le transfert des informations à caractère personnel à «*des fins spécifiques autorisées par la base juridique applicable au transfert (...)*» et l'article 6, paragraphe 5 ajoute que ces informations doivent être traitées «*d'une manière qui soit directement pertinente et non excessive ou exagérée au regard de la finalité de ce traitement*». En outre, l'article 6, paragraphe 2, interdit tout traitement ultérieur qui est incompatible avec les finalités pour lesquelles les données ont été transférées.

30. Concernant les transferts ultérieurs vers un État qui n'est pas partie à l'accord, l'article 7, paragraphes 1 et 2, exige le consentement de l'autorité compétente qui a initialement transféré les données à caractère personnel et, à cet effet, il convient de tenir dûment compte de «*tous les facteurs pertinents*» détaillés dans la disposition. Ce niveau de protection est encore renforcé par la possibilité d'interrompre le transfert d'informations à caractère personnel vers des autorités d'entités territoriales constituantes des parties, conformément à l'article 14, paragraphe 2, de l'accord, lorsque les dispositions relatives à la limitation de la finalité et aux transferts ultérieurs ne sont pas satisfaites. Le CEPD se félicite de ces dispositions.

31. L'article 7, paragraphe 3, de l'accord stipule en outre que lorsque les parties concluent un accord concernant des transferts autres que pour des cas spécifiques, elles doivent satisfaire aux «conditions spécifiques» prévues dans l'accord autorisant les transferts. Nous observons que ces transferts peuvent aussi impliquer, dans la pratique, des transferts massifs de données. Les conditions de ces transferts ne sont pas définies à l'article 7, paragraphe 3. Le traitement massif des données constitue une grave atteinte aux droits au respect de la vie privée et à la protection des données à caractère personnel en raison du nombre de personnes et de la quantité de données à caractère personnel impliqués[31]. Nous recommandons l'insertion dans la déclaration explicative d'une liste indicative des «conditions spécifiques» susmentionnées.

3. Sécurité des informations

32. Le CEPD se félicite des dispositions de l'article 9 concernant la sécurité des informations. Toutefois, en ce qui concerne la notification des incidents liés à la sécurité des informations, l'article 10, paragraphe 2, point b), de l'accord autorise l'omission de la notification d'une violation des données lorsque celle-ci «*est susceptible de représenter une menace à la sécurité nationale*», la conséquence possible («*susceptible*») sur la sécurité nationale n'étant pas claire. Le CEPD remet également en cause la nécessité d'omettre totalement la notification plutôt que de simplement la retarder ou de limiter, pour des raisons de sécurité, la qualité des destinataires pouvant recevoir les informations. En outre, le texte ne contient aucune condition spécifique concernant le report des notifications à l'autorité compétente effectuant le transfert. Le CEPD recommande de mettre en évidence, dans une déclaration explicative, l'intention des parties d'appliquer ces dispositions en vue de limiter autant que possible l'omission des notifications, d'une part, et d'éviter des retards excessifs de notification, allongeant les périodes durant lesquelles l'autorité compétente n'est pas informée des violations de données qu'elle a transférées, d'autre part.

4. Conservation des données

33. L'article 12, paragraphe 1, de l'accord exige des parties qu'elles «*garantissent que la durée de la conservation des informations à caractère personnel n'excède pas la durée nécessaire et appropriée*». À la lumière du principe de limitation de la finalité invoqué par les parties dans l'accord, la précision suivante doit être ajoutée: «*aux fins spécifiques pour lesquelles elles ont été transférées*».

34. En outre, l'article 12, paragraphe 2, de l'accord, relatif aux règles en matière de conservation des données dans le cas de transferts massifs, devrait également faire référence aux critères à prendre en considération afin de déterminer la durée de la période de conservation telle qu'elle est établie à l'article 12, paragraphe 1, en tenant compte des principes de proportionnalité et de nécessité.

5. Transferts massifs de données sensibles

35. Eu égard au fait que la notion de données sensibles diffère entre les parties[32], les catégories particulières de données énumérées à l'article 13, paragraphe 1, de l'accord doivent être saluées parce que le texte clarifie la signification des données sensibles aux fins de l'accord et l'aligne sur la définition de l'Union[33].

36. Néanmoins, le CEPD s'inquiète que l'article 13, paragraphe 2, de l'accord rend possibles les transferts massifs de données sensibles parce qu'il permet à un accord conclu entre les

États-Unis et l'Union ou un État membre de fournir la possibilité d'un «*transfert d'informations à caractère personnel autre que pour des cas spécifiques, des enquêtes ou des poursuites*». Bien que l'article 13, paragraphe 2, de l'accord exige la prise en considération de la nature des informations, il laisse à chaque accord spécifique la charge de déterminer les catégories de données à échanger. Dans ce contexte, le CEPD rappelle ses avis précédents sur l'usage de données des dossiers passagers (PNR), dans lesquels il a préconisé l'exclusion complète des données sensibles dans le contexte des transferts massifs[34]. Par exemple, le CEPD a spécifiquement remis en question le traitement des données sensibles par le ministère américain de la sécurité intérieure, recommandant que l'accord en cause précise que les transporteurs aériens ne devraient pas transférer les données sensibles au ministère[35].

37. Par conséquent, le CEPD recommande que les transferts massifs de données sensibles soient exclus du champ d'application de l'accord.

6. Droits de la personne concernée

38. Le CEPD se félicite que l'accord prévoie plusieurs droits pour la personne concernée: le droit à être informé (article 20), le droit d'accès (article 16), le droit de rectification, qui renvoie également à l'effacement et au verrouillage (article 17), les droits à un recours administratif et juridictionnel (articles 18 et 19), et le droit de ne pas être soumis à une décision automatisée (article 15). Le CEPD tient à rappeler que les droits de la personne concernée, et en particulier les droits d'accès et de rectification, sont inscrits à l'article 8, paragraphe 2, de la Charte en tant que composantes essentielles du droit à la protection des données à caractère personnel.

39. Les exceptions, prévues dans l'accord, à l'exercice des droits d'accès et d'information sont considérables. Eu égard au droit d'accès, l'article 16, paragraphe 2, prévoit une limitation de l'accès en application de critères supplémentaires, notamment la protection des «*informations sensibles se rapportant à l'action répressive*», les critères consistant à éviter de gêner «*des enquêtes, des recherches ou des procédures officielles ou judiciaires*», à éviter de nuire à la «*prévention, à la détection, à la recherche et à la poursuite d'infractions pénales ou à l'exécution des sanctions pénales*», ainsi que la «*sécurité publique*» et la «*sécurité de l'État*». Une autre exception dispose que des limitations de l'accès peuvent être imposée afin de «*protéger les intérêts prévus dans la législation relative à la liberté de l'information et à l'accès du public aux documents*»[36]. Il est difficile de concevoir une situation dans laquelle des données à caractère personnel transférées aux fins de cet accord ne seront pas considérées comme des «informations sensibles se rapportant à l'action répressive» par l'autorité compétente, en l'absence de critères spécifiques permettant de déterminer[37] en quoi consistent les «informations sensibles se rapportant à l'action répressive».

40. Le CEPD recommande un réexamen de la liste des exceptions afin de garantir que la personne conserve automatiquement la possibilité d'avoir accès à ses propres données, même si l'accès est limité ou exercé par un tiers de confiance dans des situations où l'accès est refusé afin de protéger des informations sensibles se rapportant à l'action répressive. En ce sens, l'article 16, paragraphe 4, de l'accord est salué dans la mesure où il prévoit une forme d'accès indirect, mais son application est limitée uniquement aux cas «autorisés par le droit national applicable».

41. En outre, l'article 16, paragraphe 1, de l'accord prévoit l'accès aux données «*conformément au cadre juridique applicable de l'État dans lequel le recours est effectué*».

Si le régime d'accès actuellement en vigueur aux États-Unis s'applique aux données transférées dans le cadre du champ d'application de l'accord, il ne semble pas, à première vue, que les conditions prévues à l'article 8, paragraphe 2, de la Charte seront satisfaites. Bien que l'*US Privacy Act* (loi américaine sur la vie privée) de 1974 accorde aux personnes le droit d'accéder à leurs données à caractère personnel[38], ce droit est considérablement restreint par plusieurs exceptions[39]. Premièrement, une dérogation spéciale stipule que ce droit ne s'applique pas à toute information «*compilée en prévision raisonnable d'une action ou procédure civile*»[40]. Deuxièmement, des dérogations générales suppriment l'obligation d'accorder l'accès aux informations lorsqu'une agence dont l'activité principale a trait à la répression pénale demande la dérogation en promulguant une règle à cet effet[41]. Troisièmement, des dérogations spécifiques prévoient, notamment, qu'une agence puisse publier une règle lui permettant de déroger à l'obligation d'accorder l'accès à un système de dossiers contenant des informations classifiées qui sont des «informations relatives à la défense nationale ou à la politique étrangère ou des informations d'enquête compilées à des fins répressives»[42]. Ces dérogations entravent sensiblement l'exercice du droit d'accès, s'il pouvait effectivement être exercé conformément au droit actuellement en vigueur aux États-Unis.

42. Un droit effectif à être informé est important. À cet égard, la CJUE a établi que «*cette* exigence *d'information des personnes concernées par le traitement de leurs données personnelles est d'autant plus importante qu'elle est une condition nécessaire à l'exercice par ces personnes de leur droit d'accès et de rectification des données traitées*»[43]. La disposition relative à la «Transparence» (article 20) produit un effet très limité en raison du fait que des avis d'information doivent être publiés «*dans un format et au moment prévus par la loi applicable à l'autorité prévoyant les avis*», ce qui peut vouloir dire, dans la pratique, que même des avis d'information généraux pourraient être publiés longtemps après qu'un certain transfert ou une certaine opération de traitement a été effectué. En outre, toutes les limitations applicables au droit d'accès s'appliquent de la même manière aux obligations en matière de transparence.

43. À la suite de cette analyse préliminaire, le CEPD considère que les parties à l'accord doivent redoubler d'efforts pour veiller à ce que les restrictions à l'exercice du droit d'accès soient limitées de façon sélective à celles qui sont indispensables pour défendre les intérêts généraux énumérés et pour renforcer l'obligation de transparence.

44. Le CEPD se félicite du fait que les décisions automatisées «*ne puissent pas uniquement être basées sur le traitement automatisé d'informations à caractère personnel sans intervention humaine*», conformément à l'article 15. C'est particulièrement important dans le domaine répressif, où les conséquences de l'établissement de profils sur les personnes peuvent s'avérer plus graves. Toutefois, le seuil à atteindre avant de déclencher l'applicabilité de l'article 15 est relativement élevé parce qu'il exige que les décisions produisent des «*effets défavorables importants*» pour ne pas être uniquement basées sur un traitement automatique, tandis que le droit de l'Union interdit habituellement les décisions qui produisent des *«effets juridiques défavorables pour la personne concernée ou qui l'affecte de manière significative*»[44].

7. Recours juridictionnels et administratifs

45. Dans le contexte différent d'une décision sur un constat d'adéquation (la sphère de sécurité), la Cour de justice de l'Union européenne a constaté[45] que l'absence de possibilité

d'exercer un recours juridictionnel lors du transfert de données à caractère personnel vers un pays tiers touche à l'essence même de l'article 47 de la Charte, qui prévoit le droit à une protection juridictionnelle effective. Dans ce contexte, la Cour de justice a établi qu'une «*réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte*» et que «*l'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à* ***un recours effectif*** *devant un tribunal dans le respect des conditions prévues à cet article*»[46].

46. L'article 19, paragraphes 1 et 2, de l'accord exige des parties qu'elles prévoient, dans leur cadre juridique applicable, la possibilité pour leurs *citoyens* de demander un contrôle judiciaire concernant le refus d'accès ou la modification de registres ou la divulgation illicite intentionnelle d'informations. Si l'article 19, paragraphes 1 et 2, de l'accord prévoit la possibilité que les citoyens de l'Union demandent à exercer un recours en rapport avec certaines dispositions fondamentales de l'accord, les *personnes autres que les citoyens de l'Union*, qui sont autrement protégés par la Charte (p.ex. demandeurs d'asile, résidents de l'Union) n'ont pas, sur la base de ces deux paragraphes, la possibilité d'exercer des voies de droit afin d'accéder à des données à caractère personnel les concernant ou d'en obtenir la rectification. En outre, ni les citoyens ni les personnes qui ne sont pas des citoyens n'ont la possibilité d'exercer des voies de droit afin d'obtenir l'*effacement* des données. L'article 19, paragraphe 3, de l'accord établit que ces limitations «*sont sans préjudice de tout autre contrôle judiciaire disponible en ce qui concerne le traitement des informations à caractère personnel d'une personne dans le cadre du droit de l'État dans lequel le recours est demandé*». Le CEPD n'est pas en mesure d'évaluer complètement, dans le présent avis préliminaire, l'efficacité d'autres recours juridiques qui peuvent être prévus par la législation sectorielle, particulièrement aux États-Unis et au niveau des États, ni de déterminer dans quelle mesure ils peuvent offrir un recours organique et global à toutes les personnes concernées. Par conséquent, il nourrit de graves préoccupations quant à la conformité de l'article 19 avec la Charte. En ce qui concerne la **nature effective** des recours judiciaires, qui est également une exigence de l'article 47 de la Charte, elle devra être examinée une fois que les dispositions de l'accord seront mises en œuvre dans le droit national des États-Unis[47].

47. En ce qui concerne le recours administratif, le CEPD observe que l'article 18 renvoie au recours administratif prévu par l'autorité compétente, telle qu'elle est définie à l'article 2 de l'accord, et non par une autorité de surveillance. L'article 18, paragraphe 1, établit que ce type de recours administratif sera disponible pour les atteintes alléguées aux droits d'accès, de rectification et d'effacement. La CJUE a souligné qu'il est essentiel que les personnes puissent introduire des plaintes auprès d'autorités de contrôle indépendantes[48] et demander à exercer, par conséquent, un recours administratif. Le CEPD lit la disposition relative à un contrôle effectif (article 21) et la disposition relative au recours administratif (article 18) comme ne restreignant pas la possibilité d'un particulier d'introduire une plainte auprès de l'autorité de contrôle à la suite de violations des articles 16 et 17 de l'accord (droits d'accès, de rectification et d'effacement).

8. Contrôle effectif

48. Le CEPD salue les dispositions relatives à la responsabilité de l'article 14, telles qu'elles sont mentionnées au paragraphe 19 du présent avis. Toutefois, ces dispositions devraient être complétées par un contrôle externe indépendant.

49. À cet égard, le CEPD rappelle que l'article 8, paragraphe 3, de la Charte prévoit que le respect des règles relatives à la protection des données est soumis au contrôle d'une autorité indépendante[49], à savoir, d'après la CJUE, une autorité en mesure de décider indépendamment de toute influence extérieure directe ou indirecte. Cette autorité ne doit pas seulement être indépendante des parties qu'elle contrôle, elle doit aussi être indépendante du gouvernement étant donné que ce dernier peut lui-même être partie intéressée[50].

50. Le CEPD se félicite de l'exigence prévue à l'article 21, paragraphe 1, point a), de l'accord selon laquelle les autorités de contrôle doivent «*exercer des fonctions et pouvoirs de contrôle indépendants*». Toutefois, notamment à la lumière du débat actuel concernant les pouvoirs effectifs pour **mettre en œuvre** la loi relative à la protection des données et au respect de la vie privée de certaines autorités de contrôle américaines[51], énumérées à l'article 21, paragraphe 3, de l'accord, nous estimons qu'il est essentiel qu'une déclaration explicative bilatérale accompagnant l'accord soit signée par les parties afin d'énumérer spécifiquement:

- les autorités de contrôle qui sont compétentes en la matière et le mécanisme permettant aux parties de s'informer mutuellement sur les changements futurs;
- les pouvoirs effectifs qu'elles peuvent exercer;
- l'identité et les coordonnées du point de contact qui aidera à l'identification de l'organe de contrôle compétent (voir l'article 22, paragraphe 2). [52]

9. Examen conjoint et suspension

51. Le CEPD salue l'article 23 sur l'examen conjoint de l'accord. L'article 23, paragraphe 3, de l'accord empêche la «duplication» des examens conjoints, qui pourrait avoir une incidence sur les examens conjoints déjà prévus dans les accords existants. Le CEPD recommande toutefois à la Commission européenne de clarifier de quelle manière cela pourrait avoir une incidence sur la mise en œuvre d'accords spécifiques tels que ceux ayant trait à l'échange des données des dossiers passagers[53] ou de dossiers financiers[54].

52. Le CEPD se félicite également du fait que l'article 26 autorise la suspension de l'accord dans le cas d'une violation flagrante de ses dispositions. À cet effet, le CEPD souligne le rôle primordial du contrôle indépendant de l'application de l'accord afin de détecter les violations.

V. Conclusions

53. Le CEPD salue l'intention de prévoir un instrument juridiquement contraignant ayant pour objectif de garantir un niveau élevé de protection des données à caractère personnel transférées entre l'Union et les États-Unis afin de prévenir et de détecter les infractions pénales, dont les actes terroristes, et de procéder aux enquêtes et poursuites en la matière.

54. La plupart des dispositions fondamentales de l'accord visent à se conformer pleinement ou en partie aux garanties essentielles du droit à la protection des données à caractère personnel dans l'Union (comme les droits de la personne concernée, le contrôle indépendant et le droit à un contrôle judiciaire).

55. Bien que l'accord ne constitue techniquement pas une décision d'adéquation, il crée une présomption générale de conformité pour les transferts fondés sur une base juridique spécifique, dans le cadre de l'accord. Par conséquent, il est indispensable de garantir que cette «présomption» est renforcée par toutes les garanties nécessaires dans le texte de l'accord, afin d'éviter toute violation de la Charte, en particulier des articles 7, 8 et 47.

56. Le CEPD recommande d'apporter trois améliorations essentielles au texte afin d'en garantir la conformité avec la Charte et avec l'article 16 TFUE:

1) clarification selon laquelle toutes les garanties s'appliquent à tous, pas seulement aux ressortissants de l'Union;

2) garantie que les dispositions en matière de recours juridictionnel soient efficaces au sens de la Charte;

3) clarification selon laquelle les transferts massifs de données sensibles ne sont pas autorisés.

57. Par ailleurs, par souci de sécurité juridique, le CEPD recommande que les améliorations ou clarifications suivantes soient apportées au texte de l'accord ou dans les déclarations explicatives à joindre à l'accord, ou lors de la phase de mise en œuvre de l'accord, comme détaillé dans le présent avis:

1) il conviendrait d'interpréter l'article 5, paragraphe 3, comme respectant le rôle des autorités de contrôle afin qu'il soit conforme à l'article 8, paragraphe 3, de la Charte;
2) les bases juridiques spécifiques des transferts (article 5, paragraphe 1) doivent satisfaire pleinement aux garanties prévues dans l'accord et, dans le cas de dispositions contradictoires entre une base juridique spécifique et l'accord, ce dernier prévaudra;
3) dans le cas d'une protection insuffisante des données transférées à des autorités au niveau de l'État, les mesures pertinentes prévues à l'article 14, paragraphe 2, doivent inclure, le cas échéant, des mesures relatives aux données déjà partagées;
4) les définitions des opérations de traitement et des informations à caractère personnel (article 2) doivent être alignées afin d'être conformes à leur compréhension bien établie au titre du droit de l'Union; si les parties ne s'alignent pas pleinement sur ces définitions, il doit être clarifié, dans les documents explicatifs accompagnant l'accord, que l'application des deux notions ne différera fondamentalement pas de leur compréhension dans le droit de l'Union;
5) une liste indicative des «conditions spécifiques» dans lesquelles les données sont transférées massivement (article 7, paragraphe 3) pourrait être intégrée dans la déclaration explicative;
6) les parties entendent appliquer les dispositions relatives aux notifications des violations d'informations (article 10) en vue de limiter autant que possible l'omission des notifications, d'une part, et d'éviter les retards de notification excessifs, d'autre part;

7) la disposition relative à la conservation des données, prévue à l'article 12, paragraphe 1, est complétée par la précision «*aux fins spécifiques pour lesquelles elles ont été transférées*» à la lumière du principe de limitation de la finalité invoqué par les parties à l'accord;
8) les parties à l'accord devraient envisager de redoubler d'efforts afin de garantir que les restrictions à l'exercice du droit d'accès sont limitées à celles qui sont indispensables pour défendre les intérêts généraux énumérés et renforcer l'obligation de transparence;
9) il conviendrait qu'une déclaration explicative détaillée à l'accord détaille spécifiquement (article 21):
   - les autorités de contrôle qui sont compétentes en la matière et le mécanisme permettant aux parties de s'informer mutuellement sur les changements futurs;
   - les pouvoirs effectifs qu'elles peuvent exercer;
   - l'identité et les coordonnées du point de contact qui aidera à l'identification de l'organe de contrôle compétent (voir l'article 22, paragraphe 2).

58. Enfin, le CEPD tient à rappeler que toute interprétation, toute application et toute mesure de mise en œuvre de l'accord doit être, dans le cas d'un manque de clarté et de conflit manifeste entre des dispositions, conforme aux principes constitutionnels de l'Union, en particulier à l'article 16 TFUE et aux articles 7 et 8 de la Charte, indépendamment des améliorations qu'il serait bienvenu d'apporter en application des recommandations formulées dans le présent avis.

Fait à Bruxelles, le 12 février 2016

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

Notes

[1] Voir MEMO 10/1661 de la Commission européenne, publié le 3 décembre 2010, disponible à l'adresse http://europa.eu/rapid/press-release_IP-10-1661_fr.htm.
[2] Voir MEMO 11/203 de la Commission européenne, publié le 29 mars 2011, disponible à l'adresse http://europa.eu/rapid/press-release_MEMO-11-203_en.htm.
[3] Voir le communiqué de presse 14-668 du bureau du procureur général, publié le 25 juin 2014, disponible à l'adresse http://www.justice.gov/opa/pr/attorney-general-holder-pledges-support-legislation-provide-eu-citizens-judicial-redress.
[4] Voir MEMO 15/5612 de la Commission européenne, publié le 8 septembre 2015, disponible à l'adresse http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.
[5] Texte disponible à l'adresse http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.
[6] Voir l'affaire C-181/73, R. & V. Haegeman/État belge, ECLI:EU:C:1974:41, point 5 (dans la section «Motifs»).
[7] Affaire C-308/06, Intertanko et autres, ECLI:EU:C:2008:312, point 42.
[8] Affaires jointes C-402/5 P et C-415/05 P, Kadi/Conseil, ECLI:EU:C:2008:461, point 285.
[9] Voir à cet effet les dispositions pertinentes:
- dans le domaine du marché unique: articles 25 et 26 de la directive 95/46/CE;
- dans le domaine répressif, concernant uniquement les données traitées dans le cadre d'un transfert transfrontalier: article 13 de la décision-cadre 2008/977/JAI du Conseil 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, p. 60;
- pour les transferts de données d'Europol vers des pays tiers: article 23, paragraphe 6, point b), de la décision 2009/371/JAI du 6 avril 2009 portant création de l'Office européen de police (Europol), JO L 121, p. 37;
- pour les transferts de données par des institutions et organes de l'Union: article 9 du règlement (CE) nº 45/2001.
Aucun aperçu des lois nationales relatives à la protection des données n'est disponible dans le domaine répressif. Voir par ailleurs l'étude de la commission LIBE, «*A Comparison between US and EU Data Protection Legislation for Law Enforcement*» (auteur: F. Boehm), PE 536.459, publiée en septembre 2015, (ci-après, l'«étude Boehm»), p. 30 à 35.
[10] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012)11 [première lecture] (ci-après, la «proposition de règlement général sur la protection des données»).
[11] Affaire C-362/14, Schrems, ECLI:EU:C:2015:650 (ci-après l'«affaire Schrems»).
[12] Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012)10 [première lecture] (ci-après, la «proposition de directive sur la protection des données en matière pénale»).
[13] Voir l'affaire Schrems, points 38, 40, 47, 53, 54, 58, 64, 66, 72, 91, 94 et 95.
[14] Plus précisément, la Cour de justice a récemment affirmé que les exigences visant à garantir des transferts internationaux légaux de données à caractère personnel, inscrites dans le droit dérivé de l'Union, en particulier la possibilité dont dispose la Commission d'adopter des décisions d'adéquation en vue de «*la protection de la vie privée et des libertés et droits fondamentaux des personnes*» (article 25, paragraphe 6, de la directive 95/46/CE), découlent de l'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union (ci-après, la «Charte») et de l'obligation explicite de «protection des données à caractère personnel» qu'il contient. Voir à cet égard l'arrêt Schrems, point 72: «*Ainsi, l'article 25, paragraphe 6, de la directive 95/46/CE* (n. - conditions pour que la Commission européenne constate qu'un pays tiers assure un niveau de protection adéquat) *met en œuvre l'obligation explicite de protection des données à caractère personnel, prévue à l'article 8, paragraphe 1, de la Charte, et vise à assurer, comme l'a relevé M. l'avocat général au point 139 de ses conclusions, la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers*». En outre, la Cour dispose que l'expression «niveau de protection adéquat» doit être comprise comme «*exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte*» [affaire Schrems, point 73]. La condition de l'existence d'un niveau de protection substantiellement équivalent est prévue tant dans le futur règlement

général sur la protection des données [considérant 81 du préambule] que dans la directive sur la protection des données en matière pénale [considérant 47 du préambule].

[15] Décision-cadre 2008/977/JAI du Conseil 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, p. 60.

[16] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

[17] Article 54 de la décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), JO L 205, p. 63.

[18] Article 31 du règlement (CE) nº 767/2008 du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour, JO L 218, p. 60.

[19] Article 23, paragraphe 6, point b), de la décision 2009/371/JAI du Conseil.

[20] Voir, par exemple, l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, JO L 215, p. 5. Décision 2009/820/PESC du Conseil du 23 octobre 2009 concernant la conclusion, au nom de l'Union européenne, de l'accord d'extradition entre l'Union européenne et les États-Unis d'Amérique et de l'accord d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique, JO L 291, p. 40. Voir également les différents traités d'entraide judiciaire entre des États membres et des pays tiers.

[21] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, STCE nº 108.

[22] Le considérant 10 de la directive 95/46/CE et le considérant 10 de la décision-cadre 2008/977/JAI du Conseil prévoient expressément que, en règle générale, le système juridique de protection des données créé dans le cadre de chacun de deux actes juridiques «*doit avoir pour objectif de garantir un niveau élevé de protection*».

[23] Voir, par exemple, les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland (C-293/12) et Seitlinger (C-594/12), ECLI:EU:C:2014:238, (ci-après, l'«affaire DRI»), point 67, et l'affaire Schrems, points 39 et 72.

[24] «*Aux fins du présent accord et de sa mise en œuvre, le DHS est réputé garantir, au sens de la législation de l'Union européenne applicable en matière de protection des données, un niveau adéquat de protection lors du traitement et de l'utilisation des dossiers passagers. À cet égard, les transporteurs qui ont fourni des données de dossiers passagers au DHS conformément au présent accord sont réputés avoir respecté les exigences légales en vigueur dans l'Union concernant le transfert de telles données de l'UE vers les États-Unis.*»

[25] Le CEPD rappelle que la Cour de justice de l'Union a souligné dans sa jurisprudence appliquant l'article 8, paragraphe 1, de la Charte que l'expression «niveau de protection adéquat» «*doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union*» (arrêt Schrems, point 73). La Cour a établi en outre que «*lors de l'examen du niveau de protection offert par un pays tiers*», l'appréciation doit porter sur «*le contenu des règles applicables dans ce pays résultant de la législation interne ou des engagements internationaux de celui-ci ainsi que la pratique visant à assurer le respect de ces règles*» (arrêt Schrems, point 75) et doit également «*prendre en compte toutes les circonstances relatives à un transfert de données à caractère personnel vers un pays tiers*» (arrêt Schrems, point 75). En outre, l'une des principales raisons pour lesquelles la CJUE a invalidé la décision relative à la sphère de sécurité de 2000 était que celle-ci ne contenait pas de constatation motivée que le système juridique en question «assure» un niveau de protection adéquat (arrêt Schrems, points 96 à 98).

[26] Voir l'arrêt de la Cour suprême des États-Unis dans l'affaire Medellin/Texas, 552 US (2008), points 505 et 505 nº 2: «*Il faut entendre par "d'application directe" que le traité produit dès sa ratification des effets internes automatiques en tant que loi fédérale*»; «*En résumé, **si les traités peuvent contenir des engagements internationaux... ils ne sont pas pour autant des lois nationales sauf si le Congrès a promulgué des dispositions d'application ou si le traité lui-même véhicule une intention d'être d'application directe et est ratifié à ces conditions***». Voir «*International Law and Agreements*: *Their Effect upon U.S. law*», publié par le *Congressional Research Service*, 18 février 2015, disponible sur www.crs.gov.

[27] Affaire DRI, point 68.

[28] Le considérant 33 de la décision-cadre rappelle qu'il s'agit d'«*une composante essentielle de la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire entre les États membres*». Voir également l'affaire C-518/07, Commission/Allemagne, EU:C:2010:125, point 25. Affaire C-288/12, Commission/Hongrie, EU:C:2014:237, point 48, et l'arrêt Schrems, point 41.

[29] Arrêt Schrems, point 47, qui renvoie spécifiquement à l'article 8, paragraphe 3, de la Charte lors de l'établissement du pouvoir des autorités de contrôle afin de vérifier la légalité des transferts.

[30] Pour d'éventuelles informations sur l'incidence de ces transferts, voir l'étude de la commission LIBE, «*The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*» (auteur: F. Bignami), PE 519.215, publiée en mai 2015 (ci-après, l'«étude Bignami»), p. 6 et 7.

[31] Arrêt Schrems, points 93 et 94; voir également l'étude Bignami, p. 6.
[32] Voir à cet effet l'étude Bignami, p. 12.
[33] L'article 8, paragraphe 1 de la directive 95/46/CE inscrit les «*données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle*» dans les «*catégories particulières de données*».
[34] Voir, par exemple, l'avis du CEPD sur l'accord UE-Canada sur les données PNR, 30 septembre 2013, point 47; avis du CEPD sur la communication de la Commission relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, 19 octobre 2010, point 26; avis du CEPD sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, 25 mars 2011, point 6; avis du CEPD sur l'accord UE-Australie sur les données PNR, 15 juillet 2011, point 26; voir également l'avis nº 4/2003 du groupe de travail «article 29» sur la protection des données concernant le niveau de protection assuré aux États-Unis pour la transmission des données passagers, adopté le 23 juin 2003, p. 7.
[35] Avis du CEPD sur la proposition de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieure, 9 décembre 2011, points 15 et 16.
[36] À des fins de comparaison, l'article 9 de la Convention nº 108 du Conseil de l'Europe prévoit des dérogations au droit d'accès, y compris dans le domaine répressif, lorsque celles-ci sont prévues par la loi et sont nécessaires dans une société démocratique «*a) 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; et (b) à la protection de la personne concernée et des droits et libertés d'autrui*».
[37] Comme requis, par analogie, dans l'arrêt DRI, aux points 60 à 62.
[38] 5 U.S.C. §552a(d)(1).
[39] Voir l'étude Bignami en général, et l'étude Boehm, p. 53 et 54.
[40] 5 U.S.C. §552a(d)(5); Voir l'étude Bignami, p. 12.
[41] 5 U.S.C. §552a(j).
[42] 5 U.S.C. §552a(k).
[43] Affaire C-201/14, Bara/CNAS, ECLI:EU:C:2015:638, point 33.
[44] Article 7 de la décision 2008/977/JAI du Conseil et article 19 de la proposition de directive sur la protection des données en matière pénale.
[45] Arrêt Schrems, point 95.
[46] Arrêt Schrems, point 95.
[47] Le projet de loi a été approuvé par le Congrès le 10 février 2016, mais d'autres procédures sont nécessaires avant qu'il soit considéré comme adopté. Le projet de loi a fait l'objet de critiques de la part des observateurs américains, qui considèrent qu'il prévoit une protection juridique insuffisante pour les citoyens des États-Unis et, en tout état de cause, une protection sensiblement moindre que celle offerte aux ressortissants américains dans le cadre de la *Privacy Act* de 1974. Voir à cet égard l'étude Bignami, p. 13, et le courrier envoyé par l'EPIC au *Committee on the Judiciary* de la Chambre des représentants des États-Unis, 16 septembre 2015, disponible à l'adresse https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.
[48] Arrêt Schrems, points 56 à 58.
[49] Affaire C-614/10, Commission, Autriche, ECLI:EU:C:2012:631, point 36; affaire C-288/12, Commission/Hongrie, point 47; arrêt Schrems, point 40.
[50] Affaire C-518/07, Commission/Allemagne, points 18, 19, 25 et 30.
[51] Voir l'étude Bignami, p. 34, et l'étude Boehm, p. 54 et 72.
[52] Affaire Commission/Autriche, point 36; affaire Commission/Hongrie; affaire Commission/Allemagne et affaire Schrems.
[53] Décision 2012/472/UE du Conseil du 26 avril 2012 relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, JO L 215.
[54] Décision 2010/412/UE du Conseil du 13 juillet 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO L 195.