COMMISSION
EUROPÉENNE

Bruxelles, le 18.10.2017
COM(2017) 611 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur le premier examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis

{SWD(2017) 344 final}

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur le premier examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis

1. PREMIER EXAMEN ANNUEL - FINALITÉ, PRÉPARATION ET PROCÉDURE

Dans sa décision du 12 juillet 2016[1] (ci-après la «décision d'adéquation»), la Commission a considéré que le bouclier de protection des données UE-États-Unis (ci-après le «bouclier de protection des données») assure un niveau de protection adéquat des données à caractère personnel transférées depuis l'Union européenne vers des organisations établies aux États-Unis.

Le bouclier de protection des données reflète les principes et exigences établis par la Cour de justice de l'Union européenne dans l'arrêt qu'elle a rendu dans l'affaire *Schrems*[2], par lequel elle a invalidé l'ancien cadre de la sphère de sécurité. Il apporte un certain nombre d'éléments nouveaux par rapport à la sphère de sécurité, qui renforcent la protection des données à caractère personnel qui sont transférées vers les États-Unis. Figurent parmi ces éléments l'imposition d'obligations plus strictes aux entreprises certifiées dans le cadre du bouclier de protection des données, par exemple en ce qui concerne les limitations quant à la période pendant laquelle une entreprise peut conserver des données à caractère personnel (le principe dit de la «conservation des données») ou les conditions dans lesquelles les données peuvent être partagées avec des tiers en dehors du cadre (le principe dit de la «responsabilité quant aux transferts ultérieurs»). Il prévoit également un suivi plus régulier et rigoureux de la part du ministère américain du commerce et renforce considérablement les possibilités de recours des particuliers de l'UE. En outre, le bouclier de protection des données s'appuie sur des observations et garanties écrites précises formulées par le gouvernement américain selon lesquelles l'accès des autorités publiques à des données à caractère personnel transférées dans le cadre du bouclier de protection des données pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois fait l'objet de limitations et de garanties claires. À cet effet, il crée aussi un mécanisme de recours complètement nouveau, à savoir le mécanisme du médiateur.

La Commission s'est engagée à évaluer son constat d'adéquation chaque année et, à cette fin, procède à un examen annuel du fonctionnement du bouclier de protection des données. Le premier examen annuel du fonctionnement du bouclier de protection des données se conclut par le présent rapport. L'examen a porté sur tous les aspects du bouclier de protection des

[1] Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, JO L 207 du 1.8.2016, p. 1.

[2] Arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire C-362/14, *Maximilian Schrems/Data Protection Commissioner* (ci-après l'affaire «*Schrems*»).

données, c'est-à-dire la mise en œuvre, la gestion, la supervision et le respect de l'application du cadre du bouclier de protection des données par les autorités et instances américaines compétentes ainsi que les questions relatives à l'accès des autorités publiques américaines aux données à caractère personnel transférées dans le cadre du bouclier de protection des données à des fins d'intérêt public, relevant en particulier de la sécurité nationale. Il a également comporté un dialogue au sujet du thème spécifique de la prise de décision automatisée, ainsi qu'une évaluation des nouveaux éléments intervenus dans le système juridique américain au cours de l'année écoulée qui pourraient avoir une incidence sur le fonctionnement du bouclier de protection des données.

Le cadre du bouclier de protection des données est entré en vigueur le 1er août 2016. Comme il s'agit de la première année de mise en application, l'examen annuel de la Commission s'attache principalement à vérifier si tous les mécanismes et procédures prévus par le cadre - dont de nombreux ont été nouvellement créés - – ont été pleinement mis en œuvre et fonctionnent de la manière prévue par la décision d'adéquation. En outre, la Commission a mis en particulier l'accent sur la question de savoir si, et comment, les diverses autorités américaines associées à la mise en œuvre du cadre ont bien donné suite à leurs déclarations et ont tenu leurs engagements, en ce qui concerne tant la gestion et la supervision des aspects commerciaux du bouclier de protection des données que l'accès des pouvoirs publics aux données à caractère personnel. Ce point est devenu particulièrement important depuis le changement de l'administration américaine en janvier 2017.

Dans le cadre de la préparation de l'examen annuel, la Commission a collecté des informations et retours d'information au sujet de la mise en œuvre et du fonctionnement du cadre du bouclier de protection des données auprès de différents acteurs, plus particulièrement auprès d'entreprises certifiées dans le cadre du bouclier de protection des données par l'intermédiaire de leurs associations professionnelles respectives, et auprès d'organisations non gouvernementales (ONG) actives dans le domaine des droits fondamentaux et, en particulier, des droits numériques et du respect de la vie privée. Elle a également sollicité auprès des autorités américaines associées à la mise en œuvre du cadre, et obtenu de leur part, des informations écrites, notamment des documents et du matériel utiles.

Le premier examen annuel conjoint s'est tenu les 18 et 19 septembre 2017 à Washington, DC. Inauguré par Mme Věra Jourová, commissaire européenne pour la justice, les consommateurs et l'égalité des genres, et Wilbur Ross, secrétaire d'État américain au commerce, cet examen annuel a été mené, pour le compte de l'UE, par des représentants de la direction générale de la justice et des consommateurs de la Commission européenne. La délégation de l'UE comprenait également huit représentants désignés par le groupe de travail «article 29», l'organe consultatif qui réunit les autorités nationales chargées de la protection des données (APD) ainsi que le Contrôleur européen de la protection des données.

Du côté américain, des représentants du ministère du commerce, de la Commission fédérale du commerce, du ministère du transport, du département d'État, du bureau du directeur du renseignement national et du ministère de la justice ont participé à cet examen, ainsi que le médiateur faisant fonction, un membre du conseil de surveillance de la vie privée et des libertés civiles (PCLOB) et du bureau de l'inspecteur général des services de renseignement. De plus, des représentants d'organisations qui proposent des services indépendants de règlement des litiges dans le cadre du bouclier de protection des données, l'Association américaine d'arbitrage en sa qualité d'administratrice du panel d'arbitrage du bouclier de protection des données et quelques entreprises certifiées dans le cadre dudit bouclier ont apporté leurs contributions au cours de l'examen annuel.

La réflexion relative à l'examen annuel a en outre été alimentée par des données accessibles au public, telles que des décisions de justice, des règles et procédures de mise en œuvre édictées par les autorités américaines compétentes, des rapports et études d'ONG, des rapports concernant la transparence publiés par des entreprises certifiées dans le cadre du bouclier de protection des données, des articles de presse et autres informations parues dans les médias.

2. CONSTATATIONS, CONCLUSIONS ET RECOMMANDATIONS GENERALES

L'examen annuel a démontré que les autorités américaines ont mis en place les structures et procédures nécessaires au bon fonctionnement du bouclier de protection des données. La procédure de certification a été gérée d'une manière globalement satisfaisante, plus de 2 400 entreprises ayant été certifiées à ce jour. Les autorités américaines ont mis en place les mécanismes et procédures de traitement des réclamations et de surveillance de l'application afin de préserver les droits individuels. En font également partie les nouvelles voies de recours supplémentaires à la disposition des particuliers de l'Union, tels que le panel d'arbitrage et le mécanisme du médiateur. En ce qui concerne ce dernier, un médiateur faisant fonction a été désigné après le changement d'administration en janvier 2017, tandis que la nomination d'un médiateur permanent est toujours en suspens. La coopération avec les autorités européennes chargées de la protection des données a été renforcée. Pour ce qui est de l'accès des autorités publiques aux données à caractère personnel à des fins de sécurité nationale, les garanties américaines pertinentes restent en place, notamment celles basées sur la directive présidentielle n° 28 émise en 2014, qui expose les limitations et garanties en ce qui concerne l'utilisation de données à caractère personnel par les autorités nationales de sécurité, indépendamment de la nationalité de la personne concernée. Dans ce contexte, il convient également de faire remarquer que l'article 702 de la loi américaine sur la surveillance et le renseignement étranger (FISA) expirera le 31 décembre 2017 et que des propositions de réforme sont en cours de discussion au Congrès américain.

Les constatations factuelles détaillées relatives au fonctionnement de tous les aspects du cadre du bouclier de protection des données un an après son entrée en service sont présentées dans

le document de travail des services de la Commission sur l'examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis [SWD(2017) 344 final], qui accompagne le présent rapport.

De ces constatations, la Commission tire la conclusion que les États-Unis continuent d'assurer un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis dans le cadre du bouclier de protection des données.

La Commission considère dans le même temps que la mise en œuvre concrète du cadre du bouclier de protection des données peut faire l'objet d'améliorations afin de veiller à ce que les garanties et garde-fous qu'il prévoit continuent de fonctionner conformément à l'intention première.

À cet effet, la Commission formule les recommandations suivantes.

2.1. Les entreprises ne devraient pas pouvoir se prévaloir publiquement de leur certification dans le cadre du bouclier de protection des données avant que ladite certification n'ait été finalisée par le ministère du commerce

Il est apparu clairement, au cours de l'examen annuel, que les entreprises qui ont introduit une demande de certification dans le cadre du bouclier de protection des données, mais dont la certification n'a pas encore été finalisée par le ministère du commerce, peuvent malgré tout déjà l'invoquer publiquement. Il peut en résulter une divergence entre des informations accessibles au public et la liste du bouclier de protection des données du ministère du commerce, dans laquelle ne figurent pas les entreprises dont la certification n'a pas encore été finalisée. Pareille divergence génère de l'incertitude pour les particuliers et les entreprises de l'UE qui souhaitent transférer leurs données vers les États-Unis, accroît le risque de fausses déclarations de participation au bouclier et entame la crédibilité du cadre dans son ensemble.

Aussi la Commission recommande-t-elle qu'il ne soit pas permis aux entreprises de faire des déclarations publiques au sujet de leur certification au titre du bouclier de protection des données tant que le ministère du commerce n'a pas finalisé ladite certification et inclus l'entreprise dans la liste du bouclier de protection des données. Les informations fournies aux entreprises par le ministère du commerce au sujet de la procédure de certification, notamment sur le site web du bouclier de protection des données, devraient être modifiées de manière à préciser clairement que les entreprises ne peuvent pas publiquement invoquer leur adhésion au cadre tant qu'elles ne figurent pas sur la liste du bouclier de protection des données.

2.2. Recherche proactive et régulière de fausses déclarations par le ministère du commerce

La Commission recommande que le ministère du commerce procède, de manière proactive et régulière, à des recherches visant à détecter d'éventuelles fausses déclarations de participation au bouclier de protection des données, non seulement dans le contexte de la procédure de

certification, c'est-à-dire à l'égard des entreprises qui ont entamé, mais pas achevé, le processus de certification et qui font malgré tout déjà valoir qu'elles participent au cadre, mais également, et de manière plus générale, à l'égard des entreprises qui n'ont jamais sollicité une telle certification mais font des déclarations suggérant au public qu'elles respectent les exigences du cadre. À cette fin, le ministère du commerce devrait prendre des mesures supplémentaires, comprenant des recherches sur l'internet. Comme le montrent les enseignements tirés du prédécesseur du bouclier de protection des données, à savoir le programme relatif à la sphère de sécurité, les pratiques trompeuses ne sont pas rares et peuvent entamer la crédibilité et la solidité de l'ensemble du système.

2.3. Suivi permanent par le ministère du commerce du respect des principes du bouclier de protection des données

La Commission recommande que le ministère du commerce effectue régulièrement des contrôles de la conformité. De tels contrôles pourraient par exemple prendre la forme de questionnaires de contrôle de la conformité envoyés à un échantillon représentatif d'entreprises certifiées sur une question «thématique» bien précise (par exemple transferts ultérieurs, conservation de données), ou le ministère du commerce pourrait systématiquement demander à recevoir les rapports annuels de contrôle de la conformité (qui peuvent consister soit en des auto-évaluations soit en des examens externes de la conformité) d'entreprises certifiées cherchant à obtenir la reconduction de leur certification. Le ministère du commerce pourrait ensuite utiliser les rapports annuels de contrôle de la conformité pour recenser les éventuels problèmes qui se posent en la matière et qui pourraient justifier d'autres actions de suivi avant qu'une entreprise ne puisse être recertifiée, ou des lacunes plus systémiques au niveau du fonctionnement du cadre et nécessitant des mesures correctives.

2.4. Meilleure sensibilisation

La Commission encourage tant le ministère du commerce que les APD à poursuivre et à renforcer davantage les efforts de sensibilisation qu'ils ont déjà entrepris au cours de l'année écoulée.

Afin de garantir des mesures de protection plus efficaces pour les particuliers de l'UE, les APD, en collaboration avec la Commission, pourraient intensifier leurs efforts visant à informer les particuliers de l'UE sur les modalités à suivre pour exercer leurs droits dans le cadre du bouclier de protection des données, notamment pour introduire des réclamations.

2.5. Amélioration de la coopération entre autorités chargées de l'application du cadre

La Commission recommande que le ministère du commerce et les APD coopèrent, également avec la Commission fédérale du commerce, le cas échéant, afin d'élaborer des lignes directrices au sujet de l'interprétation de certains concepts du bouclier de protection des données qui nécessitent davantage de précisions. Cela contribuerait à améliorer la coopération entre les autorités qui mettent en œuvre le cadre et en contrôlent le respect des deux côtés de

l'Atlantique, à faciliter le rapprochement des interprétations des dispositions relatives au bouclier de protection des données et à accroître la sécurité juridique pour les entreprises.

Il ressort du premier examen annuel que le principe de responsabilité en cas de transfert ultérieur et la définition des données relatives aux ressources humaines sont des exemples de concepts qui gagneraient à être éclaircis davantage.

2.6. Étude sur la prise de décision automatisée

Afin de tirer des conclusions plus précises sur la question de la prise de décision automatisée, notamment dans la perspective du prochain examen annuel, la Commission commandera une étude visant à collecter des données factuelles et à évaluer de façon plus approfondie la pertinence de la prise de décision automatisée pour les transferts réalisés sur la base du bouclier de protection des données.

2.7. Incorporation des protections prévues par la directive présidentielle n° 28 dans la loi sur la surveillance et le renseignement étranger

Le débat à venir sur le renouvellement de l'autorisation de l'article 702 de la loi sur la surveillance et le renseignement étranger (FISA) donne à l'administration et au Congrès américains l'occasion unique de renforcer les mesures de protection de la vie privée contenues dans la FISA. Dans ce contexte, la Commission espère que le Congrès sera favorable à l'incorporation, dans la FISA, des mécanismes de protection offerts par la directive présidentielle n° 28 pour les personnes non américaines, dans le but de garantir la stabilité et la continuité de ces protections. Toute autre réforme supplémentaire, en ce qui concerne tant les limitations de fond que les garanties procédurales, devrait être mise en œuvre dans l'esprit de la directive présidentielle n° 28 et, partant, garantir la protection quel que soit la nationalité ou le pays de résidence.

2.8. Nomination rapide du médiateur du bouclier de protection des données

La Commission invite l'administration américaine à confirmer son engagement politique en faveur du mécanisme du médiateur, en tant que composante essentielle de l'ensemble du cadre du bouclier de protection des données, en désignant dès que possible un médiateur permanent au poste de médiateur du bouclier de protection des données.

2.9. Nomination rapide des membres du PCLOB et publication du rapport du PCLOB sur la directive présidentielle n° 28

En tant qu'agence indépendante au sein de l'exécutif, le PCLOB exerce une fonction importante en ce qui concerne la protection de la vie privée et des libertés civiles dans le domaine des politiques de lutte contre le terrorisme et de leur mise en œuvre. La Commission recommande que l'administration américaine désigne rapidement les membres manquants du PCLOB, de sorte que celui-ci puisse remplir sa fonction sous tous ses aspects.

En outre, compte tenu de l'importance de la directive présidentielle n° 28 pour les limitations et garanties s'appliquant à l'accès du gouvernement au renseignement d'origine électromagnétique et, par conséquent, aux fins du réexamen périodique, par la Commission, de son évaluation de l'adéquation, la Commission appelle l'administration américaine à publier le rapport du PCLOB sur la mise en œuvre de la directive présidentielle n° 28.

2.10. Établissement plus rapide de rapports plus complets par les autorités américaines au sujet des nouveaux éléments pertinents

La Commission recommande que les autorités américaines exécutent de manière proactive leur engagement consistant à fournir à la Commission des informations complètes en temps utile sur tout nouveau développement qui pourrait être pertinent pour le bouclier de protection des données, notamment sur les éléments qui risquent de soulever des questions sur les mesures de protection mises en place par le cadre.