# Hughes Hubbard & Reed

# L'impact de l'arrêt Schrems II sur les programmes de conformité anticorruption

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000



Le 16 juillet 2020, la Cour de justice de l'Union européenne (la « CJUE ») a rendu son arrêt tant attendu dans l'affaire C-311/18 (« Schrems II »), en invalidant avec effet immédiat le Privacy Shield UE-États-Unis et validant sous certaines conditions les clauses contractuelles types (« CCT »). Nous avons précédemment publié une alerte sur Schrems II.

**La situation actuelle**

Les réactions des autorités nationales chargées de protection des données (les « APD ») à l'arrêt Schrems II ont été disparates.
Le Commissaire irlandais à la protection des données a noté que « l'*application du mécanisme de transfert CCT aux transferts de données à caractère personnel vers les États-Unis est désormais contestable. Il s'agit d'une question qui devra être examinée de manière plus approfondie, notamment parce que les évaluations devront être faites au cas par cas* ». Au Royaume-Uni, l'APD a indiqué que « *la Commission européenne et l'CEPD [Comité européen de la protection des données] poursuivent leurs travaux afin d'apporter des orientations plus complètes sur les mesures supplémentaires que vous pourriez devoir adopter. En attendant, vous devriez faire le point sur les transferts internationaux que vous effectuez et réagir rapidement dès que des orientations et des conseils seront disponibles* ». En Allemagne, l'APD fédérale a annoncé qu'elle « *encouragera une mise en œuvre rapide [de Schrems II] dans les cas particulièrement pertinents* » et que les transferts vers les États-Unis sont toujours possibles avec des garanties supplémentaires. L'APD de Berlin a déclaré que les transferts vers les États-Unis ne sont pas possibles actuellement et a encouragé les responsables de traitement à faire appel à des prestataires de services qui se trouvent au sein de l'UE, et l'APD de Hambourg a noté que les raisons invoquées par la CJUE pour invalider le Privacy Shield s'appliquent également aux CCT. En Norvège, l'APD a noté qu'il appartient toujours à l'exportateur de données de l'UE et à l'importateur de données hors l'UE d'évaluer si le niveau de protection dans les CCT sera également respecté dans le pays importateur. En Serbie, l'APD a souligné que la loi nationale fait toujours référence aux États-

Unis comme étant un pays tiers adéquat lorsque les données sont transférées en utilisant le Privacy Shield et qu'elle a envoyé une lettre au gouvernement Serbe afin d'adapter la loi nationale à l'arrêt Schrems II.

À la suite de son évaluation annuelle du Régime suisse-américain de protection des données et de l'arrêt Schrems II, l'APD fédérale suisse a conclu que le cadre suisse-américain de protection des données n'apporte pas un niveau de protection adéquat pour les données personnelles transférées de la Suisse vers les États-Unis en vertu de la Loi fédérale sur la protection des données et que l'utilisation de CCT ou de règles d'entreprise contraignantes (les « BCR ») exige des entreprises qu'elles procèdent à une évaluation des risques et mettent éventuellement en place des garanties supplémentaires.

Le Ministère américain au commerce a déclaré qu'il continuera à gérer le programme du Privacy Shield UE-États-Unis, sans doute pour les données qui ont déjà été transférées aux États-Unis. La Commission européenne a entamé des discussions avec le Ministère américain au commerce afin d'évaluer la possibilité d'un Privacy Shield UE-États-Unis amélioré qui serait conforme à Schrems II. Le Commissaire européen à la justice, Didier Reynders, a annoncé que l'UE achèverait la mise à niveau des CCT post-Schrems II d'ici la fin de 2020. Entre-temps, Schrems et son organisation à but non lucratif ont déjà déposé 101 plaintes auprès de plusieurs autorités nationales de protection des données dans l'UE.

Le respect des législations anticorruption peuvent nécessiter des transferts internationaux de données personnelles sensibles ou criminelles. Les entreprises qui effectuent de tels transferts doivent s'assurer que les données personnelles des résidents de l'UE transférées vers un pays tiers bénéficient d'un niveau de protection essentiellement équivalent à celui garanti par le droit européen, compte tenu des risques liés au transfert. Le 29 juillet 2020, l'APD britannique a ainsi indiqué que « *La CJUE a confirmé que les normes de protection des données de l'UE doivent accompagner les données lorsqu'elles vont à l'étranger, ce qui signifie que cet arrêt a des implications plus larges que la simple invalidation du Privacy Shield UE-États-Unis* ».

Adopter une approche expectative en matière de transferts de données dans le cadre de la conformité à la législation anti-corruption suite à l'arrêt Schrems peut présenter un risque compte tenu (i) de la nature des données personnelles, et (ii) d'une déclaration du CEPD du 17 juillet 2020 indiquant que, suite à l'arrêt Schrems II, l'évaluation de la question de savoir si les pays vers lesquels les données personnelles sont envoyées offrent une protection adéquate est principalement du ressort de l'exportateur et de l'importateur de données personnelles (et non des APD).

**Comment l'arrêt Schrems II affecte les programmes de conformité anticorruption**

Depuis l'arrêt Schrems II, les entreprises qui appliquent des programmes de conformité anticorruption ont peu d'options. Si possible, elles peuvent décider de cesser le transfert des données personnelles en dehors de l'UE. Sinon, elles pourraient utiliser ou continuer à utiliser l'un des mécanismes qui permettent le transfert de données à caractère personnel en dehors de l'UE et adapter leurs programmes de conformité anticorruption suite à l'arrêt Schrems II.

Ce faisant, les entreprises devraient évaluer leurs garanties de conformité en matière de protection des données qui sont pertinentes pour leur programme de conformité anticorruption, et devraient en particulier :

- examiner la liste des sous-traitants participant au programme anticorruption, y compris ceux basés dans des pays tiers, ainsi que la base légale du transfert de données personnelles et les dispositions des clauses de protection des données avec les sous-traitants ;
- effectuer une cartographie des flux de données et, si nécessaire, adapter les processus internes entre les filiales et/ou la société mère afin de limiter les transferts de données à caractère personnel vers des importateurs de données non communautaires sans compromettre l'efficacité du programme anticorruption ;

- évaluer les niveaux de garantie offerts par les importateurs de données basés hors de l'UE et participant à des programmes anticorruption en termes de protection des données à caractère personnel qui leur sont transférées en vertu des lois du pays où ils sont basés et de leurs règles de conduite professionnelles ; et
- effectuer des transferts de données à caractère personnel à des importateurs de données non communautaires sur la base des CCT et des BCR, compte tenu de l'arrêt Schrems II.

Nous présentons ci-dessous quelques recommandations pratiques destinées à aider les entreprises à atteindre ces objectifs.

**Six recommandations de haut niveau sur la manière de gérer l'impact des exigences de l'arrêt Schrems II**

**1. Continuer à suivre les principes de protection des données du Privacy Shield entre l'UE et les États-Unis**. Toutefois, les importateurs de données américains participant au programme du Privacy Shield UE-États-Unis doivent (i) continuer à suivre les principes du Privacy Shield UE-États-Unis, et (ii) chercher une autre base légale pour transférer des données personnelles aux États-Unis.

**2. Examen du registre des activités de traitement**. Les dérogations sous l'article 49 du RGPD couvrent les transferts effectués avec un consentement explicite ou les transferts qui sont nécessaires à l'exécution de contrats ou à l'établissement, l'exercice ou la défense d'un droit en justice. Ces dérogations ne sont pas affectées par l'arrêt Schrems II, et les entreprises peuvent donc continuer à s'en prévaloir comme avant Schrems II.

**3. Procéder à un examen approfondi des CCT en utilisant une méthode par étapes** :

- **Mettre à jour l'analyse d'impact sur la vie privée (« l'AIP »)**. Dans ses FAQ publiées le 23 juillet 2020, le CEPD a recommandé aux entreprises de réaliser une AIP afin de déterminer si les CCT offrent une protection adéquate dans le cadre juridique local de l'exportateur de données. Dans certaines circonstances, le respect des lois anti-corruption exige que les transferts internationaux de données sensibles et pénales qui doivent être inclues dans l'AIP soient effectués avant de commencer le traitement et les transferts internationaux de données personnelles. Suite à l'arrêt Schrems II, les entreprises doivent mettre à jour leur AIP avec l'aide des importateurs de données non européens qu'elles utilisent pour évaluer si la base juridique du transfert de données personnelles en dehors de l'UE offre une protection suffisante dans le cadre du système juridique national de l'exportateur de données.
- **Suivre l'avis de l'Avocat général**. Les conclusions de l'Avocat général dans l'affaire Schrems II indiquent que la protection complémentaire vise à établir des recours efficaces contre l'importateur de données et devrait prendre en considération toutes les circonstances caractérisant les transferts de données à caractère personnel, y compris les transferts de toute donnée à caractère personnel sensible, les mesures de sécurité employées ainsi que la nature et la finalité du traitement. L'Avocat général a ajouté que les garanties minimales pourraient prendre la forme d'une « *indication claire de la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles de voir leurs communications interceptées, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les c quelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements* ».
- **Ajouter des clauses contractuelles aux CCT**. La CJUE a estimé que les CCT sont valables en principe mais peuvent nécessiter des « *garanties supplémentaires* » pour assurer un niveau de protection « *essentiellement équivalent* » mais non identique à celui de l'UE. Il se peut qu'un importateur de données non européen ne puisse pas faire grand-chose, voire rien, pour protéger les données transférées des programmes de surveillance gouvernementaux, mais toute protection contractuelle qui peut être ajoutée peut aider l'exportateur et l'importateur de données à documenter leurs efforts pour se conformer dans un environnement juridique incertain, au cas où une autorité réglementaire de l'UE mettrait en cause un transfert

particulier et/ou en cas de litige. La CJUE a expressément indiqué que, dans des cas appropriés, un importateur de données américain pourrait être en mesure de :
- déclarer qu'il n'a aucune raison de croire que les personnes concernées par le transfert de données de l'UE sont soumises à des programmes de surveillance du gouvernement américain ;
- déclarer qu'il n'a aucune raison de croire que sa législation nationale l'empêcherait de remplir ses obligations au titre des CCT telles que modifiées ;
- s'engager à mettre en œuvre des mesures techniques et organisationnelles supplémentaires pour assurer la sécurité des données (telles que l'utilisation du cryptage ou de la transmission VPN) ;
- s'engager à vérifier et à informer l'exportateur de données de l'UE de l'existence de lois locales susceptibles de compromettre la sécurité des données ;
- s'engager à informer immédiatement l'exportateur de données de l'UE s'il a connaissance de toute modification de la législation ou de la réglementation susceptible d'avoir des conséquences négatives sur les garanties et les obligations offertes par les CCT, telles que modifiées ; et/ou
- s'il est contraint de divulguer des données à caractère personnel à des autorités gouvernementales, s'engager à informer l'exportateur de données de l'UE de son incapacité à se conformer aux CCT telles que modifiées.

**4. Prévoir la révision des BCR**. La validité des BCR n'a pas été abordée dans l'affaire Schrems II, mais le CEPD, dans sa FAQ, a indiqué que « le seuil fixé par la Cour s'applique également à toutes les garanties appropriées (...) utilisées pour transférer des données depuis l'EEE vers un pays tiers ». En conséquence, il serait prudent de procéder à une évaluation des risques pour savoir si les BCR déjà en place offrent une protection suffisante dans le cadre juridique national.

**5. Efforts de mise en conformité des documents**. Documenter toutes les analyses, actions et efforts visant à garantir que les CCT et/ou les BCR offrent aux personnes concernées de l'UE des protections essentiellement équivalentes à celles garanties par le droit communautaire. Cela devrait être fait pour les transferts internationaux de données à caractère personnel et pour les autres obligations et principes de la GDPR. Suite à l'arrêt Schrems II, nous nous dirigeons vers une période de contrôle réglementaire accru et d'activisme des ONG, et des efforts de conformité bien documentés peuvent s'avérer inestimables en cas d'action en justice par les ADP dans l'UE et/ou par les parties intéressées telles que les ONG ou les particuliers.

**6. Suivre les orientations du CEPD et de l'APD concernée**. Le CEPD et les ADP devraient publier des orientations supplémentaires concernant l'impact de l'arrêt Schrems II. Les exportateurs de données de l'UE et les importateurs de données hors UE doivent suivre les évolutions futures et adapter leurs programmes de conformité en conséquence. Les orientations de l'autorité de contrôle principale qui a la responsabilité principale en matière de litiges concernant les transferts transfrontaliers sont particulièrement pertinentes.

*  *  *

La présente alerte aux clients n'est pas destinée à servir de conseil juridique. Nos recommandations reflètent ce que nous estimons être les meilleures pratiques, sur la base des orientations actuelles des autorités de l'UE, et peuvent contribuer à défendre le fait de transférer des transferts de données en dehors de l'UE ou à atténuer les sanctions potentielles en cas d'action en justice intentée par les autorités de protection des données dans l'UE et/ou par les ONG. Les entreprises effectuant des transferts internationaux de données à caractère personnel à des fins d'anticorruption devraient donc examiner leur situation à la lumière de leur situation spécifique et des orientations de la ou des autorités de protection des données concernées.

Pour obtenir des conseils et une assistance concernant vos transferts de données en dehors de l'UE, veuillez contacter l'un des avocats de Hughes Hubbard dont la liste figure ci-dessous.

Stefan Naumann | Partner
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +33 (0) 1 44 05 80 60 | Cell +33 (0) 6 64 10 33 06
stefan.naumann@hugheshubbard.com | bio

Seth D. Rothman | Partner
Hughes Hubbard & Reed LLP
One Battery Park Plaza | New York, NY 10004-1482
Office +1 (212) 837-6872 | Cell +1 (917) 697-8093
seth.rothman@hugheshubbard.com | bio

Kevin Abikoff | Partner
Hughes Hubbard & Reed LLP
1775 I Street, N.W., Suite 600 | Washington, DC 20006-2401
Office +1 (202) 721-4770 | Cell +1 (917) 513-6029
kevin.abikoff@hugheshubbard.com | bio

Bryan Sillaman | Partner
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +33 (0) 1 44 05 80 03 | Cell + 1 (202) 412-6868
bryan.sillaman@hugheshubbard.com | bio

Nicolas Tollet | Partner
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +33 (0) 1 44 05 76 06 | Cell +1 (347) 268-0872
nicolas.tollet@hugheshubbard.com | bio

Michael H. Huneke | Partner
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +1 (202) 721-4714 | Cell +1 (571) 271-2738
michael.huneke@hugheshubbard.com | bio

Anne Gaustad | Partner
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +33 (0) 1 44 05 80 57 | Cell + 1 (202) 734-8605
anne.gaustad@hugheshubbard.com | bio

Elsa Malaty | Associate
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +33 (0) 1 44 05 80 18 | Cell +1 (929) 253-5120
elsa.malaty@hugheshubbard.com | bio

## Related People

**Stefan Naumann**

**Seth D. Rothman**

**Kevin T. Abikoff**

**Bryan J. Sillaman**

**Nicolas Tollet**

**Michael H. Huneke**

**Elsa Malaty**

En anglais