



CJUE, 16 JUILLET 2020, DATA PROTECTION COMMISSIONER c. MAXIMILIAN SCHREMS ET FACEBOOK IRELAND

Affaire C-311/18 – « SCHREMS II »

**Conformité au droit de l'Union Européenne des clauses contractuelles types et du
« Privacy Shield »**

Synthèse : Par un arrêt du 16 juillet 2020 ^[1], particulièrement attendu, la Cour de Justice de l'Union Européenne a, en grande Chambre, validé la décision de la Commission Européenne du 5 février 2010 relative aux clauses contractuelles types. La Cour a en effet estimé que les clauses contractuelles types datant de 2010 n'étaient pas en elles-mêmes contraires aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union Européenne, mais que le respect de ces dispositions ne pouvait s'apprécier qu'en procédant à une évaluation de l'effectivité des garanties telles qu'appliquées par l'importateur des données en question, au regard des obligations qui pèsent sur lui dans le pays tiers concerné. **A l'inverse, elle a prononcé l'invalidation du Privacy Shield, mécanisme mis en place par la décision de la Commission en date du 12 juillet 2016.**

Si votre entité effectue des transferts de données à caractère personnel vers les États-Unis, sur la base du Privacy Shield ^[2], il convient dès aujourd'hui de basculer sur un autre mécanisme permettant un tel transfert de données.

Les transferts de données à caractère personnel hors de l'Espace Economique Européen (ci-après « **EEE** ») sont encadrés par le Chapitre V (articles 44 et suivants) du Règlement (UE) 2016/679 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 (ci-après « **RGPD** »). Tout transfert hors de l'EEE nécessite la mise en place de garanties suffisantes afin d'assurer un niveau de protection des données au moins équivalent à celui garanti par le RGPD sur le territoire de l'EEE ^[3].

Au titre de ces garanties encadrant un transfert de données à caractère personnel vers un pays tiers, la Commission Européenne a adopté, le 5 février 2010, la Décision 2010/87/UE relative aux clauses contractuelles types^[4] (ci-après « **CCT** »). Ces clauses sont destinées à pallier l'insuffisance des garanties offertes par des Etats tiers, en posant des exigences contractuelles que l'importateur est tenu de respecter.

Ainsi, pour rappel, les transferts de données à caractère personnel vers des pays tiers (ou organisations internationales) doivent être effectués :

- Vers des pays ayant fait l'objet d'une décision d'adéquation de la Commission Européenne en vertu de l'article 45 du RGPD ^[5] ;
- A l'aide des CCT adoptées par la Commission Européenne en 2010 ;
- En vertu de règles d'entreprise contraignantes (ou « *BCR* »), d'un code de conduite, d'une certification ou de clauses contractuelles approuvées par une autorité de contrôle compétente, conformément à l'article 46 du RGPD ^[6] ;
- Dans le cadre des dérogations prévues à l'article 49 du RGPD^[7] ;
- Et auparavant, dans le cadre du « Bouclier de protection des données UE-Etats-Unis », ou *Privacy Shield*.

Le *Privacy Shield* est un mécanisme encadrant les transferts de données à caractère personnel vers les Etats-Unis, adopté par la Commission Européenne par la décision d'exécution (UE) 2016/1250 du 12 juillet 2016^[8]. Celui-ci fait suite à l'invalidation du *Safe Harbor* par une décision de la Cour de Justice de l'Union Européenne (CJUE) en date du 6 octobre 2015^[9], conséquence de la requête déposée par Maximilian Schrems, activiste autrichien.

I. La validité des clauses contractuelles types

Par le dépôt d'une plainte devant le *Data Protection Commissioner* (DPC – l'autorité de protection des données irlandaise) le 2 décembre 2015, Maximilian Schrems s'attaque cette fois aux CCT établies par la Commission Européenne.

M. Schrems, activiste et avocat, estime que le mécanisme des CCT ne garantit pas une protection suffisante aux données à caractère personnel transférées par Facebook Ireland Ltd à Facebook Inc., société mère basée aux Etats-Unis. En effet une fois le transfert réalisé à l'aide des CCT, les données sont librement accessibles par les autorités américaines et leurs services de renseignement. Partant, Maximilian Schrems a formé une plainte contre Facebook Ireland Ltd concernant le transfert de ses données personnelles par celle-ci vers Facebook Inc.

En 2016, l'autorité de protection des données irlandaise saisit la *High Court* (la Haute Cour irlandaise) pour transmission d'une question préjudicielle^[10] à la CJUE. En effet, l'autorité estime que le traitement de la demande de M. Schrems dépend de la validité des CCT.

En 2017, la Haute Cour étudie la demande de renvoi, formée par l'autorité, fondée sur les conditions dans lesquelles sont traitées les données à caractère personnel sur le territoire des Etats-Unis. La Cour conclut au traitement de masse de données personnelles d'internautes européens par les autorités américaines. Cette conclusion soulève la question de l'effectivité de la protection des données à caractère personnel sur le territoire des Etats-Unis et justifie, selon elle, la saisine de la CJUE.

En 2018, la High Court saisit la CJUE de 11 questions préjudicielles. Les dix premières questions portent sur les modalités de mise en œuvre de la décision CCT 2010/87/UE du 5 février 2010 et sur les garanties effectivement offertes par ce mécanisme.

La onzième et dernière question porte sur la conformité des CCT avec les articles 7^[11] (droit au respect de la vie privée), 8^[12] (protection des données à caractère personnel) et 47^[13] (droit à un recours effectif) de la Charte des droits fondamentaux de l'Union Européenne.

Dans sa décision du 16 juillet 2020, la CJUE a estimé que « *l'évaluation de ce niveau de protection [fourni dans l'Etat tiers] doit prendre en compte tant les stipulations contractuelles convenues entre l'exportateur des données établi dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données ainsi transférées, les éléments pertinents du système juridique de celui-ci* ».

Dès lors, les CCT ne sont pas en elles-mêmes contraires au droit de l'Union Européenne tant qu'elles garantissent « *des mécanismes effectifs permettant, en pratique, d'assurer que le niveau de protection requis par le droit de l'Union soit respecté et que les transferts de données à caractère personnel, fondés sur de telles clauses, soient suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer* ».

Par conséquent, la décision de la Commission Européenne du 5 février 2010 est validée par la Cour, et les CCT sont maintenues.

II. Les conséquences attendues concernant le Privacy Shield

Nombre d'auteurs ont rapproché la question relative à la validité des CCT au problème épineux de la validité du « *Privacy Shield* ». Ce mécanisme, issu de la refonte du « *Safe Harbor* » après l'arrêt « *Schrems I* », a un fonctionnement distinct de celui des CCT : il s'agit d'un dispositif d'auto-certification pour les entreprises établies aux États-Unis, reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données transférées par une entité se trouvant dans l'EEE vers cette entreprise auto-certifiée aux États-Unis. Seuls sont en mesure de s'auto-certifier les organismes soumis au contrôle de la Commission Fédérale du Commerce (la « **FTC** ») ou du Département des Transports américain (le « **DoT** »).

Toutefois, le transfert de données personnelles vers les États-Unis peut sembler problématique et ce, qu'il repose sur l'un ou l'autre des mécanismes encadrant les transferts. La législation américaine permet en effet à terme aux autorités et agences de renseignement d'accéder aux données transférées dès lors qu'un intérêt national est en jeu. Autrement dit, les transferts effectués entre l'EEE et les États-Unis comportent le risque d'être appréhendés par les autorités et par les agences de renseignement afférentes indépendamment du mécanisme utilisé pour ce transfert, ce qui est susceptible de vider le mécanisme utilisé de protection des données de son sens.

La CJUE a donc procédé à ladite évaluation de la protection des données en ce qui concerne le Privacy Shield, lequel est désormais invalidé par la Cour : « *les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers ce pays tiers, et que la Commission a évaluées dans la décision 2016/1250, ne sont pas encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, par le principe de proportionnalité, en ce que les programmes de surveillance fondés sur cette réglementation ne sont pas limités au strict nécessaire* ».

En conclusion, la décision tant attendue de la Cour a suivi la position de l'Avocat Général en validant les CCT et a tiré les conséquences de son raisonnement en invalidant le *Privacy Shield*. De fait, la Cour de justice exige une réflexion, au cas par cas, sur les garanties proposées par un importateur implanté dans un pays tiers (le pays recevant les données transférées).

Il convient donc, pour les responsables de traitement comme pour les autorités de contrôle, de procéder à l'évaluation de l'effectivité des garanties telles qu'appliquées par l'importateur en question, au regard des obligations qui pèsent sur ce dernier dans le pays tiers concerné.

La Cour précise, au considérant 202 de son arrêt, les effets qu'elle entend donner à l'invalidation de la décision 2016/1250 : « *S'agissant du point de savoir s'il convient de maintenir les effets de cette décision aux fins d'éviter la création d'un vide juridique [...], il y a lieu de noter que, en tout état de cause, compte tenu de l'article 49 du RGPD, l'annulation d'une décision d'adéquation telle que la décision BPD n'est pas susceptible de créer un tel vide juridique. En effet, cet article établit, de manière précise, les conditions dans lesquelles des transferts de données à caractère personnel vers des pays tiers peuvent avoir lieu en l'absence d'une décision d'adéquation en vertu de l'article 45, paragraphe 3, dudit règlement ou de garanties appropriées au titre de l'article 46 du même règlement.* ».

Pour la Cour, l'article 49 du RGPD prévoyant une liste de dérogations applicables aux transferts de données vers des pays tiers en l'absence d'une décision d'adéquation de la Commission (en vertu de l'article 45 du RGPD) ou de garanties appropriées (telles que celles prévues à l'article 46 du RGPD), l'invalidation du *Privacy Shield* n'est pas susceptible de créer un vide juridique.

De fait, les transferts vers des entités basées sur le territoire des États-Unis sont toujours possibles, tant qu'ils reposent sur des garanties appropriées, telles que listées au Chapitre V du RGPD, et effectives, c'est-à-dire choisies après évaluation par le responsable de traitement des conditions réelles de protection des données une fois celles-ci transférées.

Partant, le *Privacy Shield* est invalidé au jour de la décision et il convient pour les entités de basculer dès aujourd'hui sur un autre mécanisme de transfert des données.

[1] [CJUE, 16 juillet 2020, C-311/18, Data Protection Commissioner c. Maximilian Schrems et Facebook Ireland](#)

[2] La liste des 5378 organismes auto-certifiés est accessible ici : <https://www.privacyshield.gov/list>

[3] [Article 44 du RGPD](#) : « Principe général applicable aux transferts »

[4] [Décision 2010/87/UE de la Commission Européenne du 5 février 2010, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers](#)

[5] [Article 45 du RGPD](#) : « Transferts fondés sur une décision d'adéquation »

[6] [Article 46 du RGPD](#) : « Transferts moyennant des garanties appropriées »

[7] [Article 49 du RGPD](#) : « Dérogations pour des situations particulières »

[8] [Décision d'exécution \(UE\) 2016/1250 de la Commission Européenne 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](#)

[9] [CJUE, Gde Ch., 6 octobre 2015, Maximilian Schrems / Data Protection Commissioner, C-362/14, « Schrems I »](#)

[10] Procédure permettant à une juridiction nationale d'interroger la CJUE sur l'interprétation ou la validité du droit de l'Union européenne dans le cadre d'un litige dont elle est saisie

[11] « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

[12] « Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

[13] « Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter. Une aide juridictionnelle est accordée à ceux qui ne disposent pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l'effectivité de l'accès à la justice. »



Accès direct :

[Les avocats du cabinet](#)

[Les expertises du cabinet](#)

[Nos distinctions](#)

Nous contacter

Coordonnées téléphoniques :

+33 (0)1 55 27 93 93

Adresse email :

vigo@vigo-avocats.com

Adresse du cabinet :

Vigo, cabinet d'avocats 9, rue Boissy d'Anglas Paris 75008 France

Vous recevez cette lettre d'information car vous
vous êtes inscrit à cet effet depuis notre site web.

[Préférences d'envoi](#) | [Se désinscrire](#)

Vous pouvez vous désinscrire à tout moment
d'un simple clic.