_swissprivacy.law

Schrems II ou la quadrature du cercle

Philipp Fischer, le 18 octobre 2020

Le 16 juillet 2020, la Cour de justice de l'Union européenne (la « CJUE ») a rendu sa décision (n° C-311/18) dans le cadre de l'affaire dite *Schrems II*, du nom de Maximilian Schrems, un juriste autrichien qui, pour la deuxième fois après 2015 (arrêt de la CJUE du 6 octobre 2015 dans la cause n° C-362/14), obtient l'invalidation judiciaire d'un mécanisme de transmission de données personnelles vers les États-Unis.

Rappel du dispositif de l'arrêt *Schrems II*

Le *EU-US Privacy Shield* est un programme d'auto-certification par lequel une entreprise américaine peut s'engager à respecter certains standards en matière de protection des données, permettant ainsi une libre circulation de données personnelles entre cette entreprise et des acteurs situés au sein de l'Union européenne (moyennant bien sûr le respect des principes généraux en matière de protection des données). Dans le cadre de l'arrêt *Schrems II*, la CJUE a invalidé le *EU-US Privacy Shield*, au motif que cet instrument n'offre pas un niveau suffisant de protection des données personnelles à la lumière du droit de l'Union, notamment compte tenu des mesures de surveillance à disposition des autorités américaines. Cette décision a pour conséquence que les transferts de données personnelles entre les entreprises américaines participant au *EU-US Privacy Shield* et les entreprises européennes ne bénéficient plus d'une présomption de conformité au Règlement européen sur la protection des données (« **RGPD** »).

Au-delà du *EU-US Privacy Shield*, un transfert de données personnelles dans un pays qui n'offre pas un niveau de protection adéquat (tel que les États-Unis) peut toutefois être autorisé si les parties mettent en place des garanties contractuelles appropriées (art. 46 par. 2 let. c RGPD), appelées *Standard Contractual Clauses* (SCC). La Cour a confirmé que les SCC publiées par la Commission européenne constituaient une telle garantie, pour autant que l'exportateur des données (i) effectue une analyse de risques et (ii) s'assure que les SCC permettent effectivement une protection adéquate des données transférées. Dès lors, si une telle analyse révèle que les SCC ne sont pas suffisantes à assurer un niveau de protection adéquat dans le pays de destination, l'exportateur devra (iii) prendre des mesures de protection supplémentaires.

Et en Suisse ?

Même si l'arrêt *Schrems II* ne déploie pas d'effet direct en Suisse, le Préposé fédéral à la protection des données et à la transparence (le « Préposé ») a retenu que le *Swiss-US Privacy Shield* (l'équivalent du *EU-US Privacy Shield*) n'offre pas un niveau de protection suffisant et ne constitue donc plus un instrument permettant le transfert des données vers les État-Unis (communiqué du Préposé du 8 septembre 2020). Les États-Unis ne répondent donc pas aux exigences d'une protection des données adéquate au sens de l'art. 6 al. 1 LPD. Le Préposé impose alors une analyse des risques en cas de recours aux SCC.

Et maintenant ?

En priorité, les entreprises concernées doivent vérifier si des transferts de données personnelles vers un récipiendaire localisé aux États-Unis sont fondés sur le *Privacy Shield* (version UE ou suisse) et, dans l'affirmative, mettre en œuvre immédiatement une solution alternative.

S'agissant des transferts fondés sur les SCC, les entreprises doivent procéder à une évaluation des risques au vu du cadre légal de l'État de destination des données. Certes, les SCC sont soumises aux mêmes limitations que le *EU-US Privacy Shield*, vu qu'un mécanisme contractuel ne peut pas faire échec à des droits d'accès des autorités nationales. Cela étant dit, l'existence d'un tel droit d'accès ne constitue pas à nos yeux un obstacle insurmontable si le standard de la note de bas de page 2 de la Clause 5 des SCC « Responsables à Sous-Traitants » est respecté (dans l'arrêt *Schrems II*, la CJUE a du reste fait expressément référence à cette note de bas de page (§ 141)):

> « *Les exigences impératives de la législation nationale applicable* [à l'importateur de données] *et qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique* pour l'un des intérêts énoncés à l'article 13 paragraphe 1 de la Directive 95/46/EC [maintenant : art. 23 par. 1 RGPD], c'est-à-dire si elles constituent une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie des professions réglementées ; un intérêt économique ou financier important d'un État ou la protection de la personne concernée ou des droits et libertés d'autrui, *ne vont pas à l'encontre des clauses contractuelles types*. Parmi les exemples de ces exigences impératives qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique figurent, *notamment*, les sanctions reconnues sur

> le plan international, les obligations de déclaration fiscale et les obligations de déclaration de lutte contre le blanchiment des capitaux. » (nous mettons en évidence)

Si le responsable de traitement conclut que ce standard est respecté, il nous semble néanmoins recommandé de procéder à un renforcement (contractuel) des SCC, même si la CJUE a reconnu la validité des SCC dans leur principe. S'agissant de ce renforcement des SCC, une autorité de contrôle allemande a publié des propositions intéressantes (*Landesbeauftragter für Datenschutz und Informationssicherheit Baden-Württemberg, Orientierungshilfe : Was jetzt in Sachen internationaler Datentransfer ?*). Par ailleurs, les points évoqués dans le Guide « Cloud » de l'Association suisse des banquiers (pages 40–41) constituent des pistes envisageables au-delà de l'industrie bancaire.

En revanche, si les modalités d'accès des autorités de l'État du récipiendaire excèdent le standard évoqué ci-dessus – ce qui est le cas, par exemple, s'agissant des entreprises américaines soumises au *Foreign Intelligence Surveillance Act (FISA)* et à l'*Executive Order 12333* –, la conclusion implicite de l'arrêt *Schrems II* est que les SCC, même renforcées, sont insuffisantes. Le responsable de traitement doit alors explorer d'autres alternatives :

1. *Autres fondements juridiques* : Le transfert vers un État qui n'est pas au bénéfice d'une reconnaissance d'adéquation est notamment licite (i) en présence d'un consentement explicite de la personne concernée (art. 49 par. 1 let. a RGPD / art. 6 al. 1 let. b LPD / art. 17 al. 1 let. a nLPD) ou (ii) si le transfert est nécessaire à l'exécution d'un contrat conclu (a) entre la personne concernée et le responsable du traitement (art. 49 par. 1 let. b RGPD / art. 6 par. 2 al. c LPD / art. 17 al. 1 (b) (1) nLPD) ou (b) dans l'intérêt de la personne concernée (art. 49 par. 1 let. c RGPD / art. 17 al. 1 let. b ch. 2 nLPD). Il convient de noter que ces autres fondements juridiques sont considérés comme résiduels par le Comité Européen de la Protection des Données et constituent donc des exceptions qui sont soumises à des exigences spécifiques.
2. *Mesures techniques* : Une autre alternative est de recourir à des mesures techniques de protection (cryptage ou anonymisation des données). Cette option n'est pas disponible si le récipiendaire doit traiter les données personnelles afin de pouvoir rendre le service attendu (ainsi, les *cloud service providers* offrent aujourd'hui des services de traitement de données qui vont au-delà d'un simple stockage de données).

Ainsi, les SCC ne constituent plus un « standard » permettant *ipso facto* un transfert de données personnelles vers un État dépourvu d'une reconnaissance d'adéquation. Le recours aux SCC doit être précédé d'une analyse de risques documentée, ce d'autant plus que, sous

l'empire de la LPD actuelle, l'utilisation des SCC doit être notifiée au Préposé (art. 6 al. 3 LPD, une exigence à laquelle la nouvelle LPD renonce).

Proposition de citation : Philipp FISCHER, Schrems II ou la quadrature du cercle, 18 octobre 2020 *in* www.swissprivacy.law/17