Transferts de données personnelles vers les USA : tous dans l'illégalité ?

Utilisez-vous comme (presque) tout le monde des solutions Saas d'origine américaine ? Dans ce cas, vous n'ignorez sans doute pas que vous transférez très probablement des données personnelles vers les Etats-Unis.

écrit le 13 octobre 2021, MÀJ le 25 mai 2023

Conformément au RGPD, vous devez prévoir des " garanties appropriées ". La plupart du temps, votre prestataire nord-américain aura pourvu à ce besoin en insérant dans les tréfonds des annexes à ses conditions générales les clauses contractuelles types proposées par la Commission européenne. Ces clauses types ont été récemment mises à jour. Mais, contrairement à sa vocation première, cette nouvelle version inquiète plus qu'elle ne rassure. Et ce, d'autant plus que la violation des obligations du RGPD y afférentes peut être sanctionnée par une amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial, en plus de la mauvaise presse qu'une sanction publique de la CNIL peut occasionner.

Pour bien comprendre le nœud du problème, un bref retour en arrière s'impose.

Petit retour en arrière

Jusqu'à récemment encore, les transferts de données personnelles entre l'Union européenne et les Etats-Unis étaient encadrés par un accord entre le Département du commerce américain et la Commission européenne appelé " Privacy Shield ", successeur du " Safe Harbor ".

Mais, à la suite des révélations fracassantes d'un certain Edward Snowden sur le programme de surveillance américain PRISM, l'activiste autrichien Maximilian Schrems en a obtenu l'invalidation par la Cour de justice de l'Union européenne (CJUE). Et pour cause, l'application de la loi américaine en matière de renseignement rendait le Safe Harbor et le Privacy Shield tout simplement inefficaces.

Les juges luxembourgeois ont néanmoins validé le mécanisme juridique des clauses contractuelles types de la Commission européenne. Cette validation était d'autant plus opportune qu'en l'absence de Privacy Shield, ces clauses devenaient - pour de très nombreux cas - la seule " garantie appropriée " pour les transferts de l'UE vers les Etats-Unis.

Ainsi pour les juges, il incombe au responsable du traitement situé en UE (i) de vérifier au cas par cas que la législation du pays tiers destinataire des données respecte le niveau de

protection requis par le droit européen et (ii) de mettre en place des " mesures supplémentaires " si ce n’est pas le cas.

Vérification de la législation du pays tiers

Les nouvelles clauses types de la Commission européenne parues en juin dernier formalisent cette obligation pour l’exportateur des données de vérifier si la législation, mais également les pratiques, du pays destinataire lui permettent de remplir ses obligations au regard du RGPD.

Pour en revenir à notre hypothèse initiale, lorsque vous utilisez une solution Saas américaine, il vous appartient donc de vérifier par vos propres moyens (en documentant vos recherches) si la législation étatsunienne permet le respect des obligations du RGPD, avant de conclure des clauses contractuelles types avec votre destinataire.

Or, comme vu ci-dessus, la CJUE a constaté que la législation des Etats-Unis en matière de renseignement ne permettait pas de se conformer à la réglementation sur les données personnelles.

Par conséquent, et en l’absence de " mesures supplémentaires ", les entreprises peuvent légitimement se demander si elles ne violent pas le RGPD lorsqu’elles transfèrent des données vers les Etats-Unis.

Mesures supplémentaires

La solution la plus sécurisante semblerait donc d’éviter tout transfert de données vers les Etats-Unis.

Toutefois, certaines " mesures supplémentaires " de natures techniques, contractuelles ou organisationnelles permettant de préserver la confidentialité et la sécurité des données à l’encontre d’accès par les autorités publiques américaines peuvent être mises en place. Il vous revient, en tant qu’exportateur de données personnelles d’y procéder. A cet égard, le Comité européen de la protection des données (CEPD) recommande par exemple l’usage de techniques de chiffrement particulièrement robustes ou encore de pseudonymisation strictes. Et on ne saurait trop vous recommander de contractualiser ces mesures techniques ou de vérifier que cela figure dans la documentation contractuelle afin de leur donner la force juridique et contraignante nécessaire.

Bien entendu, si le tiers situé aux Etats-Unis doit avoir accès aux données en clair pour accomplir une tâche, alors aucune mesure de chiffrement ou de pseudonymisation ne semble véritablement efficace. Dans ce cas, le CEPD considère même qu’il n’y a, pour l’heure, pas de " mesure supplémentaire " suffisante.

Pour conclure, si vous devez avoir recours à une solution Saas transférant des données personnelles vers les Etats-Unis, alors nous vous recommandons :

- d’y réfléchir à deux fois ;

- de vérifier quelle " garantie appropriée " est utilisée par votre prestataire - il s’agira très probablement de clauses contractuelles types de la Commission européenne ;
- de vérifier si la législation et les pratiques américaines demeurent toujours problématique, et de documenter vos recherches ;
- le cas échant, de mettre en place des " mesure supplémentaires " techniques, contractuelles et organisationnelles afin de préserver la sécurité et la confidentialité des données ;
- de réévaluer à intervalles réguliers si la législation et les pratiques aux Etats-Unis demeurent les mêmes et si les " mesures supplémentaires " prises sont toujours appropriées.

Thomas Livenais, avocat associé, Inlo Avocats

Article écrit par Thomas Livenais