Le 18 juin dernier, le Comité Européen de la Protection des Données (CEPD) a publié ses recommandations sur les mesures à adopter en cas de transfert de données à caractère personnel vers les Etats-Unis.

La fin du « bouclier de protection des données » américain

Ces recommandations font suite à la décision de la CJUE du 16 juillet 2020 « Shrems II » qui avait invalidé la décision d'adéquation (Privacy Shield) de la Commission européenne entre l'Union Européenne et les Etats-Unis.

La CJUE a considéré que les Etats-Unis n'accordaient pas un niveau de protection suffisant des données personnelles des résidents européens. En effet la Cour s'est exprimée en indiquant que « le droit de ce pays tiers ne prévoit pas les limitations et les garanties nécessaires à l'égard des ingérences autorisées par sa règlementation nationale et n'assure pas non plus une protection juridictionnelle effective contre de telles ingérences ».

Cette décision oblige donc les responsables de traitement à trouver une autre solution pour encadrer leurs transferts de données personnelles vers les Etats-Unis.

Les exigences du RGPD en matière de transfert de données à caractère personnel

Pour assurer la continuité de la protection des données à caractère personnel, leur transfert en dehors de l'Union européenne est soumis à des règles particulières que l'on peut retrouver aux articles 45 et suivants du RGPD. En effet le transfert ne pourra avoir lieu que si la Commission européenne constate, par le biais d'une décision d'adéquation, que le destinataire assure un niveau de protection adéquat.

Néanmoins en l'absence d'une telle décision le destinataire devra prendre les mesures nécessaires pour « compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. » Ces mesures peuvent notamment être :

- des règles d'entreprise contraignantes (« Binding Corporate Rules » - « BCR »), des clauses types de protection des données (« CCT »), un code de conduite ou un mécanisme de certification approuvé par la CNIL (article 46 du RGPD)
- des clauses contractuelles ad hoc préalablement autorisées par la CNIL (article 46 du RGPD)
- l'une des dérogations prévues à l'article 49 du RGPD (consentement explicite de la personne concernée, exécution d'un contrat dans l'intérêt de la personne concernée, motifs importants d'intérêt public, etc).

L'élaboration par le CEPD d'un processus afin de pallier les lacunes de la protection des données lors d'un transfert hors de l'Union européenne

En vertu du principe d'« accountability », l'exportateur des données aura à identifier quelles mesures devront être prises pour combler les éventuelles lacunes dans la protection des données et sera en charge de conserver les preuves des actions effectuées en cas de contrôle.

Un processus en six étapes a été élaboré par le CEPD afin de guider l'exportateur des données dans cette tâche. Il s'agira donc :

- d'identifier les transferts,
- de déterminer les outils utilisés pour permettre le transfert,
- d'évaluer la réglementation du pays destinataire,
- en cas d'insuffisance, d'adopter des mesures complémentaires pour renforcer le niveau de protection

- de respecter les mesures de procédure formelles liées aux mesures retenues,
- de réexaminer à intervalles appropriés le niveau de protection dans le temps.