

La Commission européenne annonce un accord avec le gouvernement américain afin de remplacer le Safe Harbor

[DONNEES PERSONNELLES]

Communiqués de presse de la Commission européenne du 2 & du 29 février 2016

Le 2 février 2016, la Commission européenne a annoncé dans un communiqué de presse être parvenue à un accord avec les Etats-Unis, dans le cadre des discussions engagées en vue de remplacer le *Safe Harbor*. Quelques jours après, le 29 février, ledit accord a été publié par la Commission avec un projet de décision d'adéquation rédigée par le Collège des commissaires européens.

Pour rappel, la décision *Safe Harbor* qui permettait aux entreprises européennes de transférer des données personnelles à destination d'entreprises américaines a été invalidée par la Cour de justice de l'Union Européenne dans son arrêt *Schrems* du 6 octobre 2015. A la suite de cette décision, le groupe de travail G29 – qui rassemble les différentes autorités de protection européennes –, avait enjoint l'U.E. et le gouvernement américain de mettre en place une solution de remplacement avant le 31 janvier 2016. Parallèlement, les responsables de traitement ont été invités à fonder leurs transferts transatlantiques sur des mécanismes alternatifs (les clauses contractuelles standards *SCC* ou les règles interne d'entreprise *BCR*).

Avec quelques jours de retard sur le planning imposé par le G29, la Commission européenne et les Etats-Unis sont donc parvenus à un accord sur un nouveau mécanisme désormais communément appelé le « *Privacy Shield* » (ou le « bouclier vie privée »). Ce mécanisme reposera, tout comme le *Safe Harbor*, sur un système d'auto-certification des entreprises américaines qui s'engageront notamment à respecter les principes généraux suivants :

- *Information* : les entreprises seront tenues de délivrer obligatoirement certaines informations aux personnes dont les données personnelles sont collectées et traitées. En outre, d'autres obligations seront imposées, notamment celle de rendre publiques les politiques de protection des données ;
- *Choix* : les personnes concernées auront la possibilité de s'opposer à la divulgation de leurs données à des tiers et à leur utilisation pour des finalités matériellement différentes ;
- *Sécurité* : les entreprises devront prendre des mesures de sécurité raisonnables et appropriées selon le niveau de risque et la nature des données et devront garantir le même niveau de sécurité au sein de contrats avec d'éventuels sous-traitants ;
- *Intégrité des données et principe de limitation aux finalités* : les traitements devront être limités à ce qui est nécessaire pour atteindre leurs finalités, à l'usage prévu des données et devront être précis, complets et actuels ;
- *Accès* : les personnes concernées pourront demander aux entreprises, si ces dernières traitent leurs données personnelles, la communication de ces données et le cas échéant leur correction, modification ou suppression ;
- *Responsabilité au titre des transferts ultérieurs* : tout transfert ultérieur des données ne pourra se faire que pour certaines finalités et devra être formalisé au sein d'un contrat garantissant le même niveau de protection que celui garanti par le *Privacy Shield* ;



société d'avocats

- *Recours, exécution et responsabilité* : les entreprises auto-certifiées devront mettre en place des mécanismes permettant de s'assurer de leur conformité avec les principes du *Privacy Shield* et devront proposer des voies recours effectives aux citoyens européens. L'auto-certification devra être renouvelée chaque année et l'entreprise devra s'assurer que sa politique de protection des données, conforme au *Privacy Shield*, est effectivement respectée.

Au-delà de ces principes généraux, le *Privacy Shield* prévoit également le respect de principes additionnels plus spécifiques et détaillés (ex : sur les données sensibles, sur la procédure d'accès aux données, sur l'auto-certification etc.).

Plusieurs mécanismes sont prévus afin d'assurer le respect des principes du *Privacy Shield* par les entreprises auto-certifiées. Le *Department of Commerce* et la *Federal Trade Commission* du gouvernement des Etats-Unis seront notamment chargés de contrôler et faire appliquer ces principes. En outre, les citoyens européens auront la possibilité de déposer des plaintes qui devront être efficacement traitées. Enfin, l'accès aux données personnelles des citoyens européens par les autorités publiques américaines sera strictement limité et contrôlé, avec la mise en place de certaines mesures de protection et d'un mécanisme de recours offert aux citoyens européens qui souhaiteraient contester un tel accès.

La liste des entreprises auto-certifiées sera rendue publique et gérée par le *Department of Commerce* du gouvernement américain. Il sera également rendu public une liste des entreprises dont la certification a été retirée.

La décision d'adéquation finale devrait être adoptée par le Collège des commissaires européens après avis du G29 et consultation d'un comité de représentants des Etats-membres. Il convient cependant de noter que ni l'avis du G29 ni celui du comité de représentants ne conditionnent l'adoption de la décision par le Collège des commissaires européens.

Sylvain NAILLAT