

Privacy Shield adopté, nouveau fondement pour les transferts de données outre- atlantique

Privacy Shield adopté,
nouveau fondement pour les
transferts de données
outre-atlantique

La Commission européenne a adopté mardi 12 juillet dernier le Privacy Shield. Ce nouvel accord remplace le Safe Harbor, et aura pour effet d'autoriser les transferts de données à caractère personnel depuis l'Union européenne vers les entreprises établies aux Etats-Unis adhérant à ce dispositif.

L'adoption de ce nouveau « bouclier de protection des données personnelles » est l'aboutissement d'un long processus, commencé dès 2014, avec la révélation par l'ancien agent de la CIA Edward Snowden de la surveillance de masse effectuée par les services de renseignements américains puis par le refus, sur ce motif, d'un citoyen autrichien de transférer ses données vers les Etats-Unis. La Cour de Justice de l'Union Européenne a ainsi dans une décision du 6 octobre 2015 déclaré invalide la décision de la Commission du 26 juillet 2000 constatant que les Etats-Unis assurent un niveau de protection adéquat aux données caractère personnel transférées. En effet la Cour a considéré que les Etats-Unis n'apportaient pas les garanties suffisantes pour protéger les données des citoyens Européens au motif que les pouvoirs des services de renseignements américains s'étendaient à toutes données exportées depuis l'Europe dès lors que l'intérêt de sécurité publique était en cause. La CJUE a considéré que ces intrusions étaient disproportionnées et heurtaient les principes de la Charte des droits fondamentaux de l'Union Européenne.

A la suite de cette décision, l'ensemble des transferts de données personnelles vers des entités situés aux Etats-Unis sur le fondement du Safe Harbor ont dû être suspendus et des solutions alternatives mises en place. Le Groupe de travail de l'article 29, qui est constitué des différents autorités de protection des données à caractère personnel au sein de l'UE (le G29), a assuré les organisations souhaitant poursuivre le transfert de données de l'UE vers les Etats-Unis qu'elles pouvaient se fonder sur les mécanismes alternatifs prévus par la directive de 1995 relative à la protection des données, telles que les clauses contractuelles types et les règles d'entreprise contraignantes (BCR).

En parallèle la Commission européenne et le gouvernement américain engageaient des discussions afin de trouver un nouvel accord sur le transfert des données personnelles des citoyens européens vers les Etats-Unis.

Le 2 février 2016, la Commission européenne et le gouvernement des États-Unis sont parvenus à un premier accord politique. La Commission a présenté le projet d'accord le 29 février 2016. Le groupe de travail « Article 29 » a ensuite rendu un premier avis le 13 avril 2016 assez critique en particulier sur l'insuffisance des gardes fous accordés aux citoyens européens pour contrôler l'usage de leurs données.

Une résolution a été adoptée le 26 mai par le Parlement européen, et la Commission a clôturé la procédure d'adoption du nouvel accord le 12 juillet 2016 en adoptant une décision d'adéquation visant à reconnaître au mécanisme « EU-U.S. Privacy Shield » un niveau de protection « essentiellement équivalent » aux exigences européennes. .

Le nouveau dispositif : Comment ça marche ?

Le Privacy Shield vise à permettre aux entreprises de transférer plus facilement vers les Etats Unis des données personnelles collectées dans l'Union européenne, tout en protégeant les droits des personnes concernées.

Le Privacy Shield est fondé sur les principes suivants :

- Des obligations strictes pour les entreprises qui traitent des données : dans le cadre du nouveau dispositif, le ministère américain du commerce procédera régulièrement à des mises à jour et à des réexamens concernant les entreprises participantes, afin de veiller à ce qu'elles observent les règles auxquelles elles ont souscrit. Les entreprises dont la pratique ne sera pas conforme aux nouvelles règles s'exposeront à des sanctions et à une radiation de la liste des entreprises adhérant au dispositif.
- Un accès des pouvoirs publics américains soumis à des conditions claires et à des obligations de transparence : les États-Unis ont donné à l'Union européenne l'assurance que l'accès des pouvoirs publics aux données à des fins d'ordre public et de sécurité nationale serait soumis à des limitations, à des conditions et à des mécanismes de surveillance bien définis. De même, tous les citoyens de l'Union bénéficieront pour la première fois de mécanismes de recours dans ce domaine. Les États-Unis ont exclu toute surveillance de masse systématique des données à caractère personnel transférées vers leur territoire dans le cadre du bouclier de protection des données UE-États-Unis. Le secrétaire d'État américain a instauré une possibilité de recours pour les Européens dans le domaine du renseignement national en créant un mécanisme de médiation au sein du département d'État ;
- Une protection effective des droits individuels : tout citoyen estimant que les données le concernant ont fait l'objet d'une utilisation abusive dans le cadre du Privacy Shield bénéficiera de plusieurs mécanismes accessibles et abordables de règlement des litiges. Lorsqu'un litige n'aura pas été réglé par l'un de ces moyens, un mécanisme d'arbitrage sera disponible, en dernier ressort. La possibilité d'un recours dans le domaine de la sécurité nationale ouvert aux citoyens de l'UE passera par un médiateur indépendant des services de renseignement des États-Unis ;
- Un mécanisme de réexamen annuel conjoint : ce mécanisme permettra de contrôler le fonctionnement du Privacy Shield, et notamment le respect des engagements et des assurances concernant l'accès aux données à des fins d'ordre public et de sécurité nationale. Le réexamen sera mené par la Commission européenne et le ministère américain du commerce, lesquels y associeront des experts nationaux du renseignement travaillant au sein des autorités américaines et européennes de protection des données. La Commission s'appuiera sur toutes les autres sources d'information disponibles et adressera un rapport public au Parlement européen et au Conseil.

Le Privacy Shield reste donc un mécanisme souple, à l'instar du Safe Harbor sous-tendu par une nécessité d'auto-certification des entreprises américaines. Pour bénéficier de l'accord et faciliter les transferts de données personnelles entre l'Europe et les Etats Unis, les entreprises américaines adhérant au dispositif devront s'engager à respecter les obligations de protection des données du Privacy Shield.

La décision « Privacy Shield » entrera en vigueur à compter de sa notification à chacun des Etats membres de l'Union européenne et sera contraignante pour ceux-ci. L'applicabilité de ce cadre juridique aux entreprises concernées sera ensuite subordonnée à l'enregistrement de celles-ci auprès des autorités américaines en charge de la mise en œuvre du dispositif. Les entreprises américaines pourront obtenir la certification Privacy Shield à partir du 1er août 2016.

Si un des objectifs poursuivi par le Privacy Shield est d'exclure tout traitement massif des données européennes transatlantique la collecte massive de données pourra cependant être effectuée si elle est limitée à des objectifs de sécurité nationale prédéfinis : espionnage, terrorisme, armes de destruction massive, menaces sur la cyber-sécurité, sur les armées, ou menaces criminelles transnationales.

Un accord déjà critiqué

En dépit de son objectif d'amélioration de la protection des données personnelles, le nouveau cadre fait pourtant l'objet de nombreuses critiques.

Le G29 dans son avis d'avril 2016 avait notamment fait part de ses préoccupations sur un certain nombre de points manquants, incomplets ou peu clairs. Le G29 avait en particulier regretté l'absence de plusieurs principes tels que la limitation de la durée de conservation et l'interdiction des décisions automatisées. En ce qui concerne l'accès par les autorités publiques aux données, le G29 avait déploré que les autorités américaines n'aient pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens. Enfin, le G29 avait émis des doutes sur l'indépendance du médiateur (Ombudsperson) et sur le fait qu'il dispose de pouvoirs suffisants pour exercer son rôle efficacement et permettre d'obtenir un recours satisfaisant en cas de désaccord avec l'administration.

Il n'est pas certain que la nouvelle rédaction satisfasse pleinement le G29.

De même le 30 mai 2016, le contrôleur européen de la protection des données (EDPS en anglais), Giovanni Buttarelli, dans un Avis sur le Privacy Shield, demandait des améliorations « significatives » avant son adoption par la Commission européenne (CE). Selon l'Avis de l'EDPS: « La proposition de Privacy Shield est un pas dans la bonne direction, mais dans sa rédaction actuelle elle ne prend pas suffisamment en compte, de notre point de vue, toutes les garanties appropriées pour protéger les droits européens des individus à la vie privée et à la protection des données notamment en ce qui concerne le recours juridictionnel. Des améliorations significatives sont nécessaires dans l'hypothèse où la Commission européenne souhaiterait adopter une décision d'adéquation ».

Le G29 mène actuellement une analyse de la décision de la Commission et se réunira le 25 juillet 2016 afin de finaliser sa position.

Article original de DLA PIPER



Réagissez à cet article

Original de l'article mis en page : Adoption du Privacy Shield par la Commission européenne : un nouveau fondement pour les transferts de données outre-atlantique, Partenaire – Les Echos Business