L’accord Privacy Shield entre en vigueur

	L’accord Privacy Shield entre en vigueur

---

[par le Général d'armée (2S) Marc Watin-Augouard, Fondateur du FIC et Directeur du CREOGN]
Il y a quelques semaines, le Privacy Shield vient d'être adopté en remplacement du Safe Harbor. Cet accord, relatif à la protection des données à caractère personnel des Européens, est un progrès, même s'il suscite des réserves de la part du G29. Sa révision en 2017 sera l'occasion de faire un premier bilan.

Les principes du Safe Harbor ont été établis pour protéger les données à caractère personnel, conformément aux dispositions de l'ancienne directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, encore en vigueur jusqu'au 25 mai 2018. Celle-ci impose un niveau élevé de protection des droits et libertés des personnes, équivalent dans tous les États membres, en particulier pour permettre la libre circulation de leurs données à l'intérieur de l'Espace économique européen (EEE). Elle interdit le transfert de données à caractère personnel vers un pays tiers, lorsque celui-ci n'offre pas un « niveau de protection adéquat ».
La décision d'adéquation du 26 juillet 2000 de la Commission 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » reconnaissait que les transferts entre l'Union et les États-Unis répondaient aux conditions. La décision ne visait pas le secteur financier ou bancaire concerné par l'accord SWIFT[1]. Elle ne s'appliquait pas non plus lorsque sont établies des règles internes de transfert de données (*Binding Corporate Rules* ou BCR) validées par les 28 régulateurs nationaux (à vrai dire un seul en vertu du principe de reconnaissance mutuelle), des « clauses contractuelles types » élaborées par la Commission européenne, ou lorsque le transfert répond aux conditions définies par l'article 69 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[2].
La décision de la Commission a été annulée par l'arrêt CJUE C-362/14 *Maximillian Schrems/ Data Protection Commissionner* du 6 octobre 2015. L'arrêt concernait plus de 4000 entreprises américaines implantées en Europe directement affectées par ses conséquences. Tout en étant salué par les défenseurs des droits de l'internaute, il inquiétait les milieux économiques, notamment les PME. Celles-ci ne disposent pas, en effet, de services juridiques suffisamment étoffés pour établir des clauses contractuelles type, des règles internes d'entreprises, ou d'obtenir des autorisations de la CNIL (art.69 de la loi du 6 janvier 1978) prévoyant le transfert de données hors du Safe harbor.
Le 26 octobre, la commissaire européenne à la justice, Vera Jourová, annonce un « Safe Harbor II », preuve que l'urgence est prise en compte. La Commission, sommée de présenter un nouvel accord avant le 31 janvier 2016, accélère les négociations (déjà engagées auparavant) en vue d'aboutir à un texte pouvant être jugé satisfaisant, notamment par le G29. Elle présente ainsi, le 29 février 2016, son projet de «décision sur le caractère adéquat du niveau de protection», ainsi que les textes (*Privacy Shield Principles*) qui composeront le «bouclier de protection des données UE-États-Unis».

Les grandes lignes du Privacy Shield peuvent être ainsi résumées :
1/ Les entreprises seront soumises à des obligations assorties de mécanismes de surveillance permettant de les sanctionner ou de les exclure. Les nouvelles règles comprennent également des conditions plus strictes pour les transferts à d'autres partenaires par les entreprises adhérant au dispositif.
2/ L'accès par les autorités américaines sera étroitement encadré et transparent: le gouvernement américain, par la voix du directeur du renseignement national, a donné par écrit des garanties à l'UE. Tout accès des pouvoirs publics aux données à des fins de sécurité nationale sera subordonné à des limitations, des conditions et des mécanismes de supervision bien définis, qui empêcheront un accès généralisé aux données personnelles. Un mécanisme de médiation, indépendant des services de sécurité nationaux, sera mis en place.
3/ La protection des citoyens de l'UE sera mieux assurée par un mécanisme de règlement extrajudiciaire des litiges, accessible sans frais. Les entreprises visées devront apporter une réponse aux plaintes dans les 45 jours. Les citoyens de l'UE pourront également s'adresser à leur autorité nationale chargée de la protection des données, qui collaborera avec la Federal Trade Commission (Commission fédérale du commerce), un mécanisme d'arbitrage étant disponible, en dernier ressort, pour trouver une solution.
4/ Un réexamen annuel conjoint sera opéré par la Commission européenne et le ministère américain du commerce, associant des experts travaillant au sein des autorités américaines et européennes de protection des données. La Commission organisera une rencontre annuelle avec des ONG et des parties prenantes dans le domaine du respect de la vie privée, pour débattre de l'évolution plus générale de la législation américaine sur la vie privée et de ses répercussions pour les citoyens européens. Elle adressera un rapport annuel public au Parlement européen et au Conseil.
Après la promulgation par Barack Obama, le 24 février, de la loi sur le recours juridictionnel (*Judicial Redress Act[3]*),la Commission ouvre la procédure de signature de l'accord-cadre. Le dispositif doit être adopté par le Collège des commissaires européens, après consultation d'un comité composé de représentants des États membres et après avis des autorités européennes chargées de la protection des données (G29). Entre-temps, les États-Unis doivent mettre en place le nouveau cadre et les mécanismes de contrôle et de médiation. Le 13 Avril 2016, le G29 a fait savoir, par la voix de sa présidente Isabelle Falque-Pierrotin, que le texte constitue une avancée encore perfectible.
La décision sur la conclusion de l'accord est adoptée par le Conseil, le 12 juillet 2016, après approbation du Parlement européen. Elle entrera en vigueur dès sa notification aux États membres. Le 25 juillet 2016, le G29 se réunit et maintient sa position. Parmi les points suscitant les critiques, l'absence de garanties sur l'abandon de la surveillance massive des données des Européens par les services américains, les doutes sur l'impartialité du médiateur et les difficultés que peuvent rencontrer les plaignants. Tout citoyen européen peut en effet se tourner vers la justice américaine, mais, comme le souligne le G29, ce mécanisme pourrait s'avérer trop complexe, notamment lorsqu'ils ne sont pas anglophones. L'accord doit être révisé chaque année. Lors de sa participation à sa réévaluation, le G29 « cherchera à savoir si les problèmes soulevés à l'égard du texte ont été résolus, mais aussi à déterminer si les garde-fous mis en place par le texte sont fonctionnels et effectifs ».
Quoi qu'il en soit, on notera que la démarche isolée d'un homme de 27 ans, s'engageant dans la brèche ouverte par les révélations d'Edward Snowden, remet en cause tout un dispositif engageant 29 Etats. Une démonstration supplémentaire de l'extraordinaire pouvoir asymétrique qu'ont les particuliers dans l'espace numérique.

[1] Accord passé le 28 juin 2010 entre l'UE et les Etats-Unis permettant à ces derniers d'accéder aux données bancaires des européens stockées sur le réseau de la Society for Worldwide Interbank Financial Telecommunication.
[2] Le transfert est expressément accepté par la personne concernée ou réponde à des conditions énumérées par l'article 69 (sauvegarde de la vie de la personne, d'un intérêt public, exercice ou défense d'un droit en justice, etc.)
[3] Cette loi permet aux européens d'engager des actions civiles aux Etats-Unis en cas de violation des règles relatives à leurs données à caractère personnel.

Merci mon Général pour votre clarté ! [Denis JACOPINI]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, attaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : L'accord Privacy Shield entre en vigueur [par le Général d'armée (2S) Marc Watin-Augouard, Fondateur du FIC et Directeur du CREOGN] | Observatoire FIC