Privacy Shield et donnés personnelles : un décret de Trump inquiète

Un décret adopté par Donald Trump menace potentiellement le Privacy Shield, l'accord censé veiller à la protection des données personnelles des citoyens européens exportées aux États-Unis par des entreprises comme Google et Facebook. La Commission européenne se veut rassurante mais affirme sa vigilance.

Privacy Shield et donnés personnelles : un décret de Trump inquiète

Un décret adopté par Donald Trump menace potentiellement le Privacy Shield, l'accord censé veiller à la protection des données personnelles des citoyens européens exportées aux États-Unis par des entreprises comme Google et Facebook. La Commission européenne se veut rassurante mais affirme sa vigilance.

L'accord Privacy Shield, qui présume que les données personnelles des Européens exportées aux États-Unis par des entreprises bénéficient du même degré de protection qu'en droit européen, aura nécessité de longs mois de négociation entre les États-Unis et l'Union européenne avant d'être adopté en juillet dernier.
Si de grands noms du milieu, comme Microsoft, Google et Facebook n'ont pas tardé à s'engager à le respecter – alors que de nombreuses critiques perdurent à son sujet – son application est désormais directement menacée par Donald Trump.

EXCLUSION DES « NON-CITOYENS AMÉRICAINS »

La quatorzième clause du décret « *d'amélioration de la sécurité publique au sein des États-Unis* » – le fameux texte anti-immigration de Trump – signé cette semaine par le 45ème président affirme en effet : « *Les agences* [comme la NSA et le FBI] *devront, dans la mesure permise par la loi en vigueur, s'assurer que leurs politiques de protection des données personnelles excluent les non-citoyens américains et les non-résidents permanents autorisés, des protections offertes par le Privacy Act au regard des informations personnelles identifiables.* »
Le rapporteur du Parlement européen en matière de protection de données, Jan Philipp Albrecht, n'a pas caché son inquiétude sur Twitter : « *Si cela est confirmé, la Commission européenne doit immédiatement suspendre le Privacy Shield et sanctionner les États-Unis d'avoir violé l'accord* ».
Suivre

Jan Philipp Albrecht
✔@JanAlbrecht
If this is true @EU_Commission has to immediately suspend #PrivacyShield & sanction the US for breaking EU-US umbrella agreement. #CPDP2017 https://twitter.com/cobun/status/824398742275104768 …
10:45 – 26 Janv 2017

LA COMMISSION EUROPÉENNE SE VEUT RASSURANTE

La Commission européenne, elle, a tenu à se montrer rassurante en indiquant que le Privacy Shield ne dépendait pas du Privacy Act, le texte de 1974 qui encadre l'usage des données personnelles de citoyens américains par les agences fédérales : « *Nous sommes au courant du décret qui a été adopté. Le Privacy Act américain n'a jamais garanti la protection des données personnelles des Européens.* » Cette affirmation contredit pourtant une déclaration antérieure de l'Union européenne à propos du Privacy Act.

Dans une explication de septembre 2015 sur le contenu du Privacy Shield, elle le présentait en effet comme une « *extension du cœur des garanties juridiques* » fournies par le Privacy Act. L'adoption du Privacy Shield a été permise par le Judicial Redress Act adopté par Barack Obama en 2014, une extension directe des garanties du Privacy Act aux citoyens non-Américains.
L'Union européenne affirme tout de même sa vigilance : « *Nous continuerons à suivre de près […] le moindre changement aux États-Unis qui pourrait avoir un impact sur les droits des Européens en matière de protection de leurs données personnelles* »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Demande dannulation du

Privacy Shield par UFC-Que Choisir

Demande d'annulation du Privacy Shield par UFC Que Choisir

Alors que la protection des données personnelles est une préoccupation majeure des consommateurs, l'UFC-Que Choisir, compte tenu des risques que fait peser l'accord transatlantique sur la protection des données personnelles (Privacy Shield), intervient en soutien de deux recours en annulation contre cet accord.

Après l'invalidation en 2015 par la Cour de justice de l'Union européenne de l'accord encadrant le transfert de données entre les Etats-Unis et l'Europe, le « Safe Harbour », compte tenu du niveau de protection insuffisant des consommateurs européens, l'Union européenne a négocié un nouvel accord avec les Etats-Unis, le Privacy Shield. Cet accord a été adopté le 8 juillet 2016, malgré les inquiétudes formulées par le Parlement européen, plusieurs gouvernements, les CNIL et les associations de consommateurs européennes.

Loin de renforcer significativement le cadre juridique du transfert des données personnelles aux Etats-Unis et d'offrir un niveau de protection « adéquate », comme exigé par les textes communautaires, le nouvel accord n'offre qu'une protection lacunaire aux ressortissants européens :

L'admission d'une collecte massive et indifférenciée des données personnelles par les services de renseignements américains

Les lois américaines autorisent encore aujourd'hui, malgré les critiques formulées dans le cadre de l'invalidation du Safe Harbour, la collecte massive d'information par la NSA et les services de renseignement américains auprès des entreprises détentrices de données personnelles, incluant des données de consommateurs français qui ont été transférées aux Etats unis.

Bien que le gouvernement américain se soit moralement engagé à réduire cette collecte autant que possible, aucune mesure concrète n'a encore été mise en place pour limiter ces traitements de données personnelles.

Cette situation est d'autant plus inquiétante que les autorités américaines sont aussi autorisées, sur la seule base de vos données personnelles, à rendre des décisions susceptibles de produire des effets juridiques préjudiciables à votre égard. Ainsi, suite à l'envoi d'un message privé sur Facebook, exprimant une opinion politique ou critiquant la collecte à tous crins des données par les multinationales américaines, vous pourriez vous voir interdire l'entrée aux Etats Unis par les autorités américaines !

Un ersatz de droit au recours pour les consommateurs européens

Alors que le droit européen exige un droit au recours effectif et un accès à un tribunal impartial, le dispositif de réclamation prévu par le Privacy Shield est stratifié et complexe… Le principal recours en cas de décision préjudiciable rendue par les autorités américaines à l'encontre d'un ressortissant européen, est un médiateur… nommé par le Secrétaire d'état américain.

Enfin, le droit de s'opposer à un traitement est prévu uniquement en cas de «modification substantielle de la finalité du traitement », alors même que le droit européen offre le droit de s'opposer à un traitement de ses données personnelles à tout moment, aussi bien lors de la collecte, qu'en cours de traitement de données personnelles.

Dans le contexte de mondialisation des échanges et de transfert des données vers des Etats avec des niveaux moindres de protection que le niveau européen, ces risques sont loin d'être théoriques comme l'a souligné récemment l'association s'agissant de la collecte de données via des jouets connectés ou des applications mobiles et leur transfert vers les Etats-Unis.

Au vu de ces éléments inquiétants, deux recours en annulation ont été déposés en septembre 2016 devant le Tribunal de l'Union européenne : l'un par le 'Digital Right Ireland', groupe lobbyiste Irlandais de défense de la vie privée sur Internet, l'autre par les 'Exégètes amateurs', groupe de travail regroupant trois associations françaises…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Protection des données personnelles : demande dannulation du Privacy Shield — UFC-Que Choisir

Le FBI a désormais le droit de pirater n’importe quel ordinateur dans le monde !

Le FBI a désormais le droit de pirater n’importe quel ordinateur dans le monde !

Le FBI est désormais doté de nouveaux pouvoirs, à savoir l'extension de ses capacités actuelles en matière de piratage informatique. Sur la base d'un mandat spécial, les agents du bureau pourront s'introduire sur n'importe quel ordinateur, situé aux États Unis mais également dans le monde.

Applicable dès aujourd'hui, la réforme est à nuancer. En effet, l'application de la **règle 41** du *Federal Rules of Criminal Procedure* (équivalent de notre code de procédure pénale) est strictement encadrée par un **juge fédéral**, qui instruit au préalable le dossier. Il s'agira d'une procédure **exceptionnelle**, la spécificité de l'affaire devant justifier de l'**opportunité** d'une telle mesure.
L'intervention reste, en effet, une **intrusion dans la vie privée des gens** *–qui ne sont pas forcément coupables de ce qui pourrait leur être reproché*. Cela n'empêche pas les politiques américains de s'inquiéter sur des atteintes aux libertés personnelles, des abus possibles ou d'éventuelles finalités politiques.
Précisons que ce pouvoir n'est pas unique en son genre, il existe déjà en France où il est actuellement renforcé du fait du plan *vigipirate* au même titre que certains pouvoirs de surveillance.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur 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 réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) 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, arnaques 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 : Les nouveaux pouvoirs de piratage informatique du FBI

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 reconnaitre 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-Etats-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

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques 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

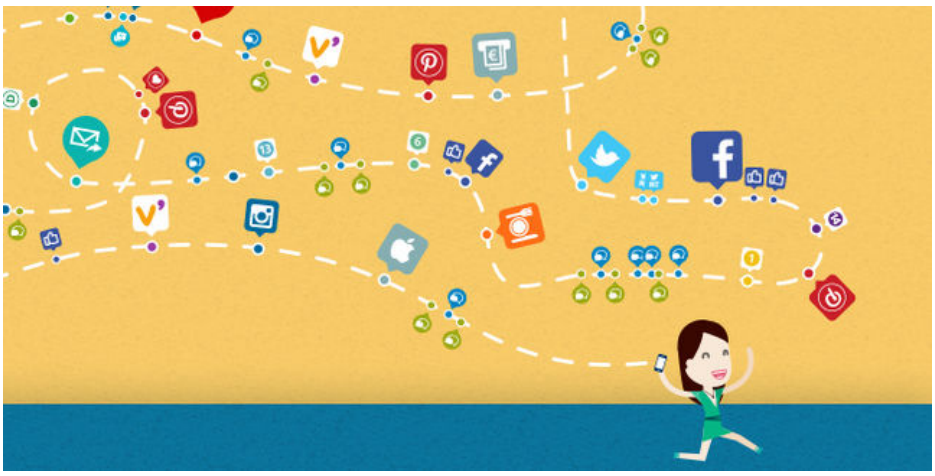
Contactez-nous

Réagissez à cet article

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

---

Ma vie disséquée à travers mes données personnelles



Ma vie disséquée à travers mes données personnelles

Original de l’article mis en page : Ma vie disséquée à travers mes données personnelles

---

Privacy Shield : 1 an de sursis donné par les CNIL européennes

Privacy Shield : 1 an de sursis donné par les CNIL européennes

---

Les CNIL européennes ne sont pas satisfaites du Privacy Shield, mais prennent date en 2017 pour s'inviter dans la révision de l'accord.

Le verdict était attendu. Les CNIL européennes du groupe de l'article 29 (G29) ont rendu leur décision définitive sur le Privacy Shield. Cet accord encadre le transfert des données entre les Etats-Unis et l'Union européenne Il est le successeur du Safe Harbor, invalidé par la Cour de Justice de l'Union européenne. Dans un communiqué de presse, le G29 souligne ses réserves sur le Privacy Shield. Il considère néanmoins que l'accord a été voté et il donne rendez-vous au 1 an de l'accord lors de sa révision pour un examen plus approfondi de certaines dispositions.

En avril dernier, le groupe avait émis différentes critiques sur le Privacy Shield. Il avait souligné *« un manque de clarté général »*, une *« complexité »*, et parfois une *« incohérence »*, des documents et annexes qui composent le Privacy Shield. C'est notamment le cas pour les voies de recours que pourront emprunter les citoyens européens contestant l'exploitation de leurs données outre-Atlantique, indique le groupe dans son avis consultatif.

Quant à l'accès des agences de renseignement aux données transférées dans le cadre du Privacy Shield (volet sécurité nationale), il soulève de *« fortes préoccupations »*. Le risque d'une collecte *« massive et indiscriminée »* des données par un État n'est pas écarté. Le groupe s'inquiète aussi du statut et de l'indépendance du médiateur (*« ombudsman »*) vers lequel les citoyens européens pourront se tourner.

Un an de sursis et une mise en garde

Certaines réserves ont été prises en compte, note le G29, mais « cependant un certain nombre de préoccupations demeurent ». Au premier rang desquels, le risque toujours bien réel d'une surveillance de masse par le gouvernement américain. Il évoque le rôle du médiateur et la révision annuelle de l'accord.

Les CNIL européennes comptent beaucoup sur cette révision annuelle prévue en juillet 2017. Elles profiteront de cette occasion « *pour non seulement évaluer si les questions en suspens ont été résolues, mais aussi si les garanties prévues par le Privacy Shield entre les Etats-Unis et l'UE sont réalisées et efficaces* ». Et de prévenir, que « *tous les membres de l'équipe en charge de cette révision doivent avoir accès à toutes les informations nécessaires à l'accomplissement de leur examen y compris des éléments favorisant leur propre évaluation sur la proportionnalité et la nécessité de la collecte et l'accès aux données par les pouvoirs publics* ». Une mise en garde contre les risques d'être éconduits dans un an.

Pendant ce temps-là, le Privacy Shield pourrait être contesté par des citoyens européens, comme cela a été le cas avec Max Schrems pour le Safe Harbor. Lors d'une récente discussion dans le cadre de Cloud Confidence, le jeune avocat avais émis l'hypothèse d'une nouvelle action en justice contre le Privacy Shield.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Privacy Shield : les CNIL européennes accordent 1 an de sursis

---

La Cnil épingle Windows 10 sur la collecte des données personnelles

	**La Cnil épingle Windows 10 sur la collecte des données personnelles**

Constatant plusieurs manquements dont la collecte de données excessives et non pertinentes par Windows 10, la Cnil a mis en demeure Microsoft de se conformer à la loi dans un délai de 3 mois.

A quelques jours de la fin de la gratuité pour migrer sur Windows 10, la Cnil s'invite dans le débat sur le dernier OS de Microsoft. Et le moins que l'on puisse dire est que le régulateur n'est pas content des méthodes de l'éditeur américain. Elle vient de mettre en demeure Microsoft de se conformer dans un délai de 3 mois à la Loi Informatique et Libertés.

Alertée sur la collecte de données de Windows 10 (dont nous nous étions fait l'écho à plusieurs reprises : « pourquoi Windows 10 est une porte ouverte sur vos données personnelles » ou « Windows 10 même muet il parle encore »), la Cnil a effectué une série de contrôles entre avril et juin 2016 pour vérifier la conformité de Windows 10 à la loi.

De ces contrôles, il ressort plusieurs manquements. Le premier concerne une collecte des données excessives et non pertinentes. Elle reproche par exemple à Microsoft de connaître quelles sont les applications téléchargées et installées par un utilisateur et le temps passé par l'utilisateur sur chacune d'elles. Microsoft s'est toujours défendu de collecter des données personnelles en mettant en avant des relevés de « télémétrie » pour améliorer son produit.

Défaut de sécurité, absence de consentements et référence au Safe Harbor

Autre point soulevé par le régulateur, un défaut de sécurité a été trouvé dans le code PIN à 4 chiffres. Ce dernier est utilisé pour s'authentifier sur l'ensemble des services en ligne. Or le nombre de tentatives de saisie du code PIN n'est pas limité.

De plus, la Cnil constate une absence de consentement des personnes notamment sur le ciblage publicitaire lors de l'installation de Windows 10. Idem pour le dépôt de cookies déposés sur les terminaux des utilisateurs.

Enfin, cerise sur le gâteau, Microsoft est enjoint par la Cnil d'arrêter de se baser sur le Safe Harbor pour transférer les données personnelles aux Etats-Unis. Cet accord a été invalidé par la Cour de Justice de l'Union européenne en octobre 2015. Il a été remplacé par le Privacy Shield qui doit bientôt rentrer en vigueur.

La balle est maintenant dans le camps de Microsoft.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : La Cnil épingle Windows 10 sur la collecte des données

Sanction de la CNIL pour BrandAlley.fr

	Sanction de la CNIL pour BrandAlley.fr

La CNIL vient d'infliger une sanction administrative de 30 000 euros à l'encontre de BrandAlley.fr. La société éponyme, derrière ce site de ventes en ligne, est épinglée pour plusieurs indélicatesses à l'égard de la loi de 1978.

Le 13 janvier 2015, une délégation de la CNIL effectuait un premier contrôle sur place pour relever déjà différents manquements de cette société française. Cela aurait pu en rester là si tout avait été rectifié à temps, mais en mars de la même année, une cliente a saisi la CNIL pour se plaindre de difficultés dans l'exercice de son droit d'accès aux données personnelles. Cette internaute adressait d'ailleurs au site de e-commerce une nouvelle lettre en mai 2015, sans plus d'effet.
Le 3 juillet 2015, BrandAlley était du coup mise en demeure par la CNIL de corriger plusieurs points de son système dans les trois mois. Bon prince, la Commission lui accordait un peu plus tard une rallonge de trois nouveaux mois. Les points litigieux visent à :
• Encadrer le traitement relatif à la prévention des fraudes,
• Mettre en place d'une durée de conservation des données clients,
• Recueillir le consentement préalable des clients pour la conservation des données bancaires,
• Prendre en compte de la demande de la plaignante,
• Obtenir l'accord des internautes s'agissant des cookies,
• Cesser de transmettre les données à caractère personnel vers des pays hors UE qui n'assurent pas un niveau suffisant de protection de la vie privée et des libertés et droits fondamentaux.

Dans un courrier de janvier 2016, BrandAllay affirmait à la CNIL qu'elle s'était désormais mise en conformité. Peu satisfaite des réponses « lacunaires », la Commission organisait un nouveau contrôle sur place en février 2016. Contrôle qui a montré la persistance de plusieurs problèmes déjà relevés. En outre, un mois plus tard, elle a effectué un contrôle à distance du site Internet, une possibilité accordée par la loi sur la consommation.
La procédure gagnait alors un tour de vis supplémentaire. La CNIL a désigné un rapporteur, en l'occurrence François Pellegrini, une étape préalable à toute sanction où la société peut encore donner ses explications. Dans ce document désormais public , le rapporteur a constaté plusieurs défauts.

Des réactions trop tardives

Premièrement, BrandAllay.fr n'avait pas déposé dans le délai imparti, de demande d'autorisation pour la mise en œuvre d'un traitement antifraude. Selon les éléments du dossier, c'est « la réception du rapport de sanction qui a conduit la société à effectuer une demande d'autorisation ». Mais beaucoup trop tardivement pour ne pas abuser de la patience de l'autorité administrative…
S'agissant de la durée de conservation des données personnelles, on se retrouve un peu dans même situation. À l'échéance du délai imparti, la société avait indiqué s'être conformé à la norme simplifie 48, celle relative à la gestion de clients et de prospects. Dans le même temps, elle ajoutait que les données clients seraient conservées 5 années durant, à compter de la fin de la relation commerciale. Or ce délai non prévu par la norme en question. Pire, lors du deuxième contrôle sur place, la CNIL a constaté qu' « aucune purge des données n'avait été réalisée ». Les explications fournies par le site de e-commerce – liées à la complexité de mise en œuvre – n'ont pas eu de poids, même si elle a depuis corrigé le tir pour revenir à un délai de conservation de 3 ans.

Cookies, chiffrement, Maroc et Tunisie

S'agissant des cookies, la société mise en demeure avait informé l'autorité de la mise en place un bandeau afin de recueillir le consentement des internautes, avant dépôt de cookies. Le contrôle en ligne effectué en mars 2016 a révélé la solidité de cette affirmation. D'un, le fameux bandeau « était rédigé de telle sorte qu'il n'informait pas les utilisateurs de leur possibilité de paramétrer le dépôt de cookies ». Soit un joli manquement à l'article 32-II de la loi de 1978.
De deux, des cookies à finalités publicitaires étaient déposés dès l'arrivée sur le site, sans l'ombre d'un consentement préalable. Pour ce dernier point, la CNIL n'a finalement pas retenu de grief, s'estimant « insuffisamment éclairée (…) sur la répartition exacte des responsabilités entre l'éditeur du site, les annonceurs et les régies publicitaires concernés ». Par constat d'huissier, BrandAlley a par ailleurs démontré s'être mise depuis d'aplomb.
Ce n'est pas tout. La CNIL a pareillement dénoncé l'absence de chiffrement du canal de communication et d'authentification lors de l'accès à BrandAlley.fr (usage du HTTP, plutôt que HTTPS). Le 29 mars 2016, la société a produit un nouveau constat d'huissier pour montrer à la CNIL que ce défaut se conjuguait désormais au passé. Un peu tard là encore pour la Commission qui a relevé un nouveau manquement.
Enfin, la société transférait vers le Maroc et la Tunisie les données personnelles de ses clients, via l'un de ses sous-traitants. Malgré des affirmations en sens contraire en janvier 2016, la CNIL a relevé en février la persistance de ces transferts. Or, en principe, de telles opérations ne sont possibles que si le pays de destination offre un niveau de protection comparable à celui en vigueur en Europe, ce qui n'était pas le cas ici (pas plus qu'aux Etats-Unis depuis l'invalidation du Safe Harbor par la justice européenne).
Après délibération, la CNIL a décidé de sanctionner la société de 30 000 euros d'amende, outre de rendre public la délibération. Une sanction loin d'être négligeable, le critère de la confiance sur Internet étant cruciale pour un site de e-commerce. La société peut maintenant attaquer, si elle le souhaite, la décision devant le Conseil d'État.

Article original de Marc Rees

Réagissez à cet article

Original de l’article mis en page : Données personnelles : BrandAlley.fr sanctionné par la CNIL

Discorde entre l’Union européenne et les Etats-Unis sur la protection des données personnelles

Discorde entre l’Union européenne et les Etats-Unis sur la protection des données personnelles

En cette période de pause estivale propice aux voyages, nombreux sont ceux qui ont réservé une chambre d'hôtel sur un site internet ou s'apprêtent à poster sur Facebook leurs photos souvenirs. Parmi ces personnes, combien s'interrogeront sur l'utilisation qui peut être faite des données quils auront ainsi (bien involontairement) transmises?

Cette question est au cœur de la problématique de la protection des données personnelles, qui intéresse l'Union européenne, notamment lorsque le transfert se fait d'un pays européen vers un pays tiers. Le principe veut que ce type de transfert de données à caractère personnel vers un pays tiers soit interdit, sauf si le pays en question assure un niveau de protection suffisant pour ces informations.

En juin 2013, les révélations d'Edward Snowden sur la récupération par l'agence de renseignements américaine, la NSA (National Security Agency), des données personnelles des citoyens européens, et donc leur surveillance par les autorités américaines, ont conduit l'UE à revoir les accords existants sur le sujet.

Alors que les négociations étaient en cours, une décision de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2015, a précipité le processus. La Cour avait à se prononcer sur une question posée par la Haute Cour de justice irlandaise relative à la validité des principes dits Safe Harbor (sphère de sécurité). Ceux-ci étaient énoncés dans la décision de la Commission européenne du 26 juillet 2000 dans laquelle elle considérait que les Etats-Unis assuraient un niveau suffisant de protection des données personnelles pour permettre le transfert des données.

Mais la Cour de justice de l'Union européenne a invalidé cette décision. Marquée par les révélations de l'affaire Snowden, elle a constaté que le régime américain de protection des données personnelles « rend possible des ingérences (…) dans les droits fondamentaux des personnes » par les autorités publiques américaines.

La négociation d'un nouvel accord devenait urgente pour les quelques 4.000 entreprises soumises au Safe Harbor devenu caduc et laissant donc place à un vide juridique. Or, le sujet de l'utilisation des données personnelles est particulièrement brûlant quand on connait la valeur de celles-ci pour les entreprises: l'exploitation des données personnelles de ses utilisateurs aurait rapporté 12 milliards de dollars à Facebook en 2014, selon Les Echos.

Le nouveau dispositif, baptisé Privacy Shield (bouclier de protection de la vie privée), a été négocié entre la Commission européenne et les Etats-Unis, qui sont parvenus à un accord le 2 février 2016. Le 13 avril, les autorités européennes de protection des données (la CNIL pour la France) ont émis un avis sur cet accord, où elles expriment de sérieuses préoccupations. Puis le Parlement européen a fait de même dans une résolution votée le 26 mai: les députés européens réclamait de rouvrir les négociations pour apporter plus de garanties. Le 8 juillet, les Etats membres, réunis au sein d'un groupe de travail, ont quant à eux validé le texte, malgré l'abstention de quatre pays, l'Autriche, la Hongrie, la Slovénie et la Bulgarie.

Finalement, le 12 juillet 2016, la Commission européenne adopte sa décision relative au bouclier de protection des données UE-Etats-Unis. La commissaire européenne chargée de la Justice, des Consommateurs et de l'Egalité des genres, Věra Jourová, a déclaré que le Privacy Shield est « un nouveau système solide destiné à protéger les données à caractère personnel des Européens et à procurer une sécurité juridique aux entreprises. Il prévoit des normes renforcées en matière de protection des données, assorties de contrôles plus rigoureux visant à en assurer le respect, ainsi que des garanties en ce qui concerne l'accès des pouvoirs publics aux données et des possibilités simplifiées de recours pour les particuliers en cas de plainte. Le nouveau cadre rétablira la confiance des consommateurs dans le contexte du transfert transatlantique de données les concernant ».

Ainsi, le nouveau système se veut plus protecteur que la précédente « sphère de sécurité »: la collecte des données par les sociétés américaines ne peut notamment pas être utilisée pour des usages non prévus initialement. Egalement, un médiateur aux Etats-Unis sera chargé de recevoir les plaintes des Européens. Tous les ans, la Commission examinera le respect du dispositif par les Etats-Unis.

Toutefois, le bouclier peine à convaincre. Les services de renseignements américains peuvent continuer à intercepter les données personnelles des Européens. Les associations fustigent un accord jugé largement insuffisant, qualifié de bouclier troué par la Quadrature du net. Du côté des députés européens, si la droite (les groupes PPE et CRE) est satisfaite, ce n'est pas le cas des Socialistes, des Verts et des Libéraux. Eux estiment que le nouveau système ne respecte pas les exigences posées par la CJUE: « la CJUE a dit que le problème, c'était les lois américaines. Or rien, dans les textes américains, n'a changé », pointe Jan Philipp Albrecht (Verts).

Le nouvel accord est par conséquent susceptible d'être à nouveau invalidé par les juges européens. Pour finir, il a été élaboré dans le cadre de la directive européenne de 1995 sur la protection des données. Or, cette directive va être remplacée en mai 2018 par un règlement adopté en 2015. L'insécurité juridique, ennemi des entreprises, plane donc toujours. Quant aux citoyens, ils ne peuvent que déplorer que la protection de leur vie personnelle soit mise en balance avec des enjeux économiques et de sécurité.

Avec la contribution de la Maison de l'Europe de Paris

Réagissez à cet article

Original de l’article mis en page : Protection des données personnelles: lautre pomme de discorde entre lUnion européenne et les Etats-Unis | www.francesoir.fr