DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 11

Madame, Monsieur,

Le cabinet Derriennic Associés est fier de vous annoncer qu'il a remporté le trophée d'or Décideurs Juridiques 2019 dans la catégorie Informatique, Internet & Données personnelles.

En dehors de cet évènement particulier, nous notons un regain d'activité de la CNIL, avec plusieurs décisions de condamnation, dont celle de Google à une amende de 50 millions d'euros.

Au programme de cette lettre RGPD de février, nous vous proposons ainsi les actualités suivantes :

- le prononcé, par la CNIL, d'une amende record de 50 millions d'euros à l'encontre de Google ;
- la condamnation d'UBER, par la CNIL, à une amende de 400 000 euros pour atteinte à la sécurité des données de ses utilisateurs ;
- le second examen du Privacy Shield par la Commission européenne ;
- une décision de la chambre sociale de la Cour de cassation sur la géolocalisation des salariés.

UBER condamné par la CNIL à une amende de 400 000 € pour atteinte à la sécurité de ses utilisateurs

La CNIL a prononcé une sanction de 400 000 € à l'encontre d'UBER FRANCE SAS pour un manquement à son obligation d'assurer la sécurité les données des utilisateurs de son service de VTC.

En 2017, la société UBER TECHNOLOGIES INC. a publié sur son site internet un article faisant état du fait qu'à la fin de l'année 2016, deux individus extérieurs à la société avaient accédé aux données de 57 millions d'utilisateurs des services UBER à travers le monde.

Les attaquants ont obtenu l'accès à un espace de travail privé UBER sur la plateforme de développement de logiciel GitHub, au sein de laquelle ils ont trouvé une clé d'accès inscrite en clair dans un fichier de code source. Les attaquants ont par la suite utilisé cette clé pour accéder aux bases de données de la société UBER, stockées sur les serveurs Amazon Web Services.

Après avoir pris connaissance de cette violation, et après avoir entendu les représentants d'UBER, la CNIl a retenu un manquement à l'obligation d'assurer la sécurité des données à caractère personnel. En effet, la CNIL a considéré que :

- l'accès à la plateforme GitHub, « *outil de travail central dans le développement des activités de la société* », « *aurait dû être encadré par des règles de sécurité adéquates* » ;
- les identifiants permettant d'accéder aux bases de données d'UBER n'auraient pas dû être « *stockés dans un fichier qui ne serait pas protégé* » ;
- compte tenu du nombre très important de personnes dont les données personnelles sont conservées, « *la mise en place d'un système de filtrage des adresses IP, quand bien même cela nécessitait un long développement, constituait un effort nécessaire qui aurait dû être planifié dès le début de l'utilisation des services* ».

La CNIL a prononcé une sanction pécuniaire de 400 000 euros à l'encontre de la société UBER FRANCE SAS pour manquement aux obligations de l'article 34 de la loi du 6 janvier 1978.

Décision :
https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037830841&fastReqId=413824161&fastPos=1

CNIL : Amende record de 50 millions d'euros à l'encontre de Google

Le 21 janvier 2019, la formation restreinte de la CNIL a prononcé une sanction de 50 millions d'euros à l'encontre de la société Google LLC, en application du RGPD, pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité.

La CNIL a été saisie de plaintes formulées par deux associations mandatées par près de 10 000 personnes au titre de l'article 80 du RGPD : None Of Your Business et la Quadrature du net. Ces plaintes concernaient l'information et les bases juridiques des traitements mis en œuvre par Google LLC dans le cadre de la personnalisation de la publicité.

1. **Manquement à l'obligation de transparence et d'information**

A l'issue d'un contrôle, la formation retreinte a constaté que l'architecture générale de l'information choisie par Google LLC s'agissant des traitements liés au compte Google ne permettait pas de respecter les obligations du RGPD, car les informations étaient éparpillées dans plusieurs documents : « Règles de confidentialité et conditions d'utilisations » (affichées au cours de la création de compte), puis « Conditions d'utilisation » et « Règles de confidentialité », (accessibles dans un deuxième temps au moyens de liens cliquables figurant dans le premier document). Ainsi, selon la CNIL :

> « *Ces différents documents comportent des boutons et liens qu'il est nécessaire d'activer pour prendre connaissance d'informations complémentaires. Un tel choix ergonomique entraine une fragmentation des informations obligeant ainsi l'utilisateur à multiplier les clics nécessaires pour accéder aux différents documents.* »

Par ailleurs, selon elle, « *la description des* ***finalités poursuivie*** *ne permettait pas aux utilisateurs de mesurer l'ampleur des traitements et le degré d'intrusion dans leur vie privée qu'ils sont susceptibles d'emporter* ». En effet, les finalités annoncées dans les différents documents (« *proposer des services personnalisés en matière de contenu et d'annonce, assurer la sécurité des produits et services, fournir et développer des services, etc.* ») ont été jugées par la formation restreinte trop génériques au regard de la portée des traitements mis en œuvres et de leurs conséquences.

Elle a également relevé que la **description des données collectées** était « *particulièrement imprécise et incomplète, tant à l'analyse du premier niveau d'information que de celle des autres documents fournis* ».

Le constat du défaut de « clarté » et de caractère « compréhensible » devait être également fait, selon la formation restreinte, s'agissant de la mention de la **base juridique** des traitements de personnalisation de la publicité, les Règles de Confidentialité n'étant pas claires sur le point de savoir si la publicité ciblée avait pour base juridique le consentement ou l'intérêt légitime.

La formation restreinte a également relevé que certaines indications sur la **durée de**

conservation des données sont également « *très générales* », sans que ne soient indiqués « *aucune durée précise ni les critères utilisés pour déterminer cette durée* ».

2. Absence de consentement valable

La formation restreinte a déduit du manquement aux obligations de transparence et d'information évoqué ci-dessus que le consentement demandé par Google LLC n'était pas suffisamment **éclairé**.

Par ailleurs, en étant autorisés et masqués par défaut, les traitements de personnalisation de la publicité ne sauraient, selon la formation restreinte, être considérés comme ayant été acceptés par l'utilisateur par un acte positif **spécifique** et **univoque**.

Elle en a conclu que le consentement sur lequel se fonde Google LLC pour les traitements de personnalisation de la publicité n'était pas valablement recueilli.

La CNIL a prononcé une sanction pécuniaire de 50 millions d'euros.

C'est la première fois que la CNIL fait application des nouveaux plafonds des sanctions prévus par le RGPD.

Lien vers la décision :
https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1

Géolocaliser ses salariés, c'est possible. Mais sous certaines conditions…

Par un arrêt du 19 décembre 2018 (17-14.631), la chambre sociale de la Cour de cassation a de nouveau rappelé que la géolocalisation du salarié afin de contrôler son temps de travail n'est licite que lorsque ce contrôle ne peut avoir lieu par un autre moyen.

En l'espèce, la société Médiapost utilisait le système de géolocalisation Distrio, pour contrôler la durée de travail de ses salariés, distributeurs publicitaires.

Contestant la licéité de ce dispositif, l'organisation syndicale Sud PTT (la « Fédération Sud des activités postales et des télécommunications »), a saisi les juridictions compétentes.

Déboutée par la Cour d'appel, Sud PTT, qui a considéré qu'il existait des moyens alternatifs à ce système de géolocalisation adaptés au but recherché, a formé un pourvoi en cassation.

Après avoir rappelé que « *L'utilisation d'un système de géolocalisation pour assurer le contrôle de la durée du travail, laquelle n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, fût-il moins efficace que la géolocalisation, n'est pas justifiée lorsque le salarié dispose d'une liberté dans l'organisation de son travail* », la Chambre sociale de la Cour de cassation a cassé l'arrêt de la Cour d'appel au motif que celle-ci n'avait pas caractérisé que le système de géolocalisation mis en œuvre par l'employeur était le seul moyen permettant d'assurer le contrôle de la durée du travail de ses salariés.

Privacy Shield : le deuxième examen de la Commission conclut à des améliorations

La Commission européenne a publié, le 19 décembre dernier, son rapport sur le deuxième examen annuel du fonctionnement du bouclier de protection des données (Privacy Shield) Union européenne-Etats Unis.

Pour rappel, la Commission s'est engagée à procéder à un examen annuel du dispositif du Privacy Shield, adopté le 12 juillet 2016, afin de s'assurer qu'il continue de garantir un niveau de protection adéquat des données à caractère personnel.

Pour rappel également, le Parlement européen a, le 5 juillet 2018, demandé à la Commission européenne de suspendre le Privacy Shield à moins que les Etats Unis ne se mettent en conformité avec les règles européennes avant le 1er septembre 2018.

Le rapport de la Commission européenne, rendu public le 19 décembre dernier, fait quant à lui état, 6 mois après la requête du Parlement européen, de la mise en place, par le ministre du commerce américain, d'un système de contrôles sur place afin de renforcer la surveillance du respect des principes du Privacy Shield. Cent sociétés ont ainsi été contrôlées.

Le ministère du commerce a également mis en place un système visant à mettre en évidence les fausses déclarations, afin d'empêcher que des sociétés non certifiées ne se prévalent faussement d'une telle certification.

La Commission fédérale du commerce a, pour sa part, dans l'optique de contrôler le respect des principes du Privacy Shield, adressé des injonctions à des sociétés participant au Privacy Shield, afin d'obtenir des informations de leur part.

La Commission européenne a par ailleurs pris note du fait que la Commission fédérale avait confirmé mener une enquête sur l'affaire Facebook/Cambridge Analytica.

Enfin, la Commission européenne attend du gouvernement américain qu'il propose, au plus tard le 28 février 2019, un candidat à titre permanant pour le poste de médiateur, dont la fonction est, pour rappel, de traiter les plaintes des personnes concernées. A défaut d'une telle proposition, la Commission envisagera de prendre des « *mesures appropriées* », conformément au RGPD.

Trophée d’or 2019 Informatique, Internet & Données personnelles