LA LETTRE DU CABINET

DONNÉES PERSONNELLES

EDITO

Les données sont au cœur de l'économie numérique. Ce phénomène se reflète également dans notre activité juridique. Outre les dossiers d'accompagnement à la mise en conformité de nos clients au RGPD, les questions juridiques relatives aux données personnelles sont de plus en plus fréquentes et complexes.
L'actualité des données personnelles prend une telle importance que nous avons décidé de lancer une nouvelle newsletter dédiée à ce domaine. L'objectif est de proposer une veille juridique, pas nécessairement exhaustive, mais en sélectionnant des textes réglementaires et des jurisprudences pertinents, en dégageant des tendances, en France et à l'international afin d'éclairer nos clients et contacts sur l'évolution du droit des données personnelles.

Cette première lettre « Données personnelles » est organisée autour des thématiques suivantes : un point sur la réglementation, la conformité au RGPD, la jurisprudence, la sécurité et une partie internationale, sans oublier un point flash sur la première sanction rendue par la CNIL contre Google, en application du RGPD.

N'hésitez pas à diffuser cette newsletter à vos collègues et contacts !

Si vous le souhaitez, merci de nous faire part de vos impressions, critiques ou suggestions.

Bonne lecture !

* Nous poursuivons par ailleurs la publication régulière de notre newsletter sur les technologies.

SOMMAIRE

ⓘ FLASH – LA CNIL PRONONCE UNE SANCTION RECORD DE 50 MILLIONS D'EUROS À L'ENCONTRE DE GOOGLE

Le 21 janvier 2019, la formation restreinte de la CNIL a prononcé une première sanction en application du RGPD pour un montant de 50 millions d'euros à l'encontre de la société Google LLC.
L'un des objectifs majeurs du RGPD est de donner aux personnes concernées plus de maîtrise sur leurs données personnelles, en renforçant les principes de transparence et de consentement éclairé, grâce à une information préalable claire et compréhensible. En l'espèce, la décision de la CNIL sanctionne un manque de transparence de la part de Google et met en cause le consentement obtenu à partir d'informations qui « *ne sont pas toujours claires et compréhensible* », ni aisément accessibles pour les utilisateurs.

Le RGPD permet les plaintes collectives. Les 25 et 28 mai 2018, quelques jours après l'entrée en application du RGPD, la CNIL a ainsi reçu deux plaintes collectives déposées par les associations None Of Your Business et La Quadrature du Net, au motif que Google traitait les données personnelles des utilisateurs de ses services, notamment à des fins de ciblage publicitaire, sans base juridique valable.
En septembre 2018, la CNIL a procédé à un contrôle en ligne pour vérifier la conformité à la loi Informatique et Libertés et au RGPD des traitements de données personnelles réalisés par Google. Pour ce faire, la Commission a analysé le parcours d'un utilisateur et les documents auxquels il peut avoir accès, en créant un compte Google lors de la configuration de son téléphone mobile sous Android.

Deux séries de manquements au RGPD ont été constatés

1 - Un manquement aux obligations de transparence et d'information

La CNIL relève que d'une part les informations fournies par Google ne sont pas aisément accessibles pour les utilisateurs, d'autre part, ces informations ne sont pas toujours claires et compréhensibles : « *des informations essentielles, telles que les finalités pour lesquelles les données sont traitées, la durée de conservation des données ou les catégories de données utilisées pour la personnalisation de la publicité, sont excessivement disséminées dans plusieurs documents, qui comportent des boutons et liens qu'il est nécessaire d'activer pour prendre connaissance d'informations complémentaires. L'information pertinente n'est accessible qu'après plusieurs étapes, impliquant parfois jusqu'à cinq ou six actions.* ».
Le manque de clarté et la difficulté des utilisateurs à « *comprendre l'ampleur des traitements mis en place par Google* », considérés comme « *particulièrement massifs et intrusifs* » est en partie la conséquence du nombre de services proposés par Google, de la quantité de données collectées ainsi que leur nature. Enfin, la durée de conservation n'est pas toujours précisée.

2 - Un manquement à l'obligation de disposer d'une base légale pour les traitements de personnalisation de la publicité

L'un des principes fondamentaux du droit de la protection des données repose sur la caractère licite du traitement. La CNIL relève que le consentement de l'utilisateurs n'est pas valablement recueilli car non suffisamment éclairé (l'information est disséminée dans plusieurs documents), et qu'il n'est ni « spécifique » (le consentement concerne plusieurs traitements alors que le RGPD implique un consentement distinct pour chaque traitement ou finalité), ni « univoque » (plusieurs cases sont pré-cochées alors qu'elles devraient être décochées).
Le montant de cette sanction a été fixé en application des nouvelles dispositions du RGPD (art. 83) et notamment compte tenu de la gravité des manquements constatés, du nombre d'utilisateurs et du volume de données concernés, et enfin du fait que ces manquements sont continus et non pas délimités dans le temps. Cette amende reste cependant très en deçà du plafond de 20% du chiffre d'affaires mondial de Google, prévu par le RGPD.
La société Google dispose de quatre mois pour former un recours devant le Conseil d'Etat.
(Délibération de la formation restreinte n°SAN-2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC)

RÉGLEMENTATION

Dans cette première rubrique, nous abordons les questions relatives à la réglementation, française (loi Informatique et Libertés) et européenne (RGPD), ainsi que les avis et recommandations publiés par la CNIL

Informatique et Libertés – Entrée en vigueur de la nouvelle loi Informatique et Libertés pour mise en conformité au RGPD

Bien que le RGPD soit d'application directe dans les Etats-membres depuis le 25 mai 2018, il comprend de nombreux renvois aux lois nationales nécessitant, pour chaque Etat-membre l'obligation d'adapter et de compléter sa loi sur la protection des données pour une pleine application du règlement. La loi du 20 juin 2018 relative à la protection des données a ainsi modifié la loi Informatique et Libertés afin de mettre en conformité le droit français avec le RGPD et transposer la directive « police-justice » (fichiers du domaine pénal).

Les principales modifications apportées par la loi du 20 juin 2018 concernent :

- *L'extension des pouvoirs de la CNIL* : la Commission, en qualité d'autorité de contrôle nationale, exercera désormais ses missions dans un périmètre élargi, (art. 11 de la loi). Ce nouveau périmètre d'intervention correspond, d'une part à la reconnaissance de droits accrus aux personnes sur leurs données (consentement explicite, transparence des informations, des communications et des modalités de l'exercice des droits de la personne concernée, droit à l'oubli, droit à la portabilité des données), d'autre part au renforcement de la responsabilité des organismes (notion de responsabilité active, ou "accountability"). Dans ce cadre, la CNIL cumule plusieurs rôles et missions dont certains viennent s'ajouter à ses fonctions existantes ;
- *Le champ d'application territorial de la loi nationale* : (titre II de la loi) en cas de divergences de législations entre les Etats membres de l'UE, la loi nationale s'applique dès lors que la personne concernée réside en France, y compris lorsque le responsable du traitement n'y est pas établi ;
- *Les modalités de traitements des données sensibles* telles que les données relatives aux condamnations pénales et infractions, ou les données de santé ont été aménagés.

A noter que le seuil d'âge du consentement des mineurs aux services en ligne a été fixé à 15 ans. Cela signifie que les services en ligne à destination des enfants sont soumis au consentement parental (ou du titulaire de la responsabilité parentale) dès lors que l'enfant a moins de 15 ans. Le responsable du traitement doit s'efforcer de vérifier le respect de cette obligation "compte tenu des moyens technologiques disponibles".

La loi du 20 juin 2018 transpose par ailleurs en droit français la directive « police-justice ». Cette directive permet de faire exception à l'exercice des droits des personnes (droit d'information, droit d'accès, droit à la portabilité, etc.) pour garantir certains objectifs d'intérêt public tels que la sécurité, la défense nationale, ou l'indépendance de la justice et des procédures judiciaires. Ces dérogations devront être fixées par décret en Conseil d'Etat.

Il conviendra donc de combiner désormais le RGPD et la nouvelle loi Informatique et Libertés pour une approche globale du droit de la protection des données.

Une ordonnance de réécriture complète de la loi Informatique et Libertés, prévue par la loi du 20 juin 2018, est parue au JO du 13 décembre 2018. Cette ordonnance a pour objet d'assurer une plus grande cohérence entre le RGPD et la loi française et de résoudre les difficultés de lisibilité de ce cadre juridique composite.

Enfin, le droit national sera complété par un nouveau décret d'application de la loi Informatique et Libertés pour achever la mise en conformité du droit national au cadre juridique européen. L'ordonnance doit entrer en vigueur en même temps que ce décret, qui doit être publié au plus tard le 1er juin 2019.

(*Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; Ordonnance n°2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles*)

CONFORMITÉ AU RGPD/GDPR

Sous cette rubrique, nous faisons un point sur les questions relatives à la conformité au RGPD et sur les mises en demeure de la CNIL à différents organismes sur des questions de non-conformité au RGPD

Une écrasante majorité de sites web français ne seraient pas en conformité avec le RGPD
Un article du Monde Informatique de décembre 2018 donne deux informations intéressantes :
D'une part, sur près de 440.000 sites web français contactés par la société Misakey pour savoir si les données personnelles du demandeur sont gérées par le site web en cause, 83% non pas répondu dans le délai imparti d'un mois, et 16% ne disposaient pas d'une adresse de contact valide dans leurs mentions légales. Seul 1% des sites web contactés a répondu ! D'autre part, 60% des consommateurs estiment que la protection des données personnelles n'est pas une priorité pour les entreprises et 65% des internautes boycotteraient les sites ne respectant pas la vie privée.
Comme nous le verrons plus loin, les consommateurs sont apparemment de plus en plus sensibles à la question de la protection des données personnelles. Le nombre de plaintes à la CNIL est en forte hausse, le RGPD permettant par ailleurs de déposer des plaintes collectives.
(« 65% des internautes boycottent les sites ne respectant pas la vie privée », in Le Monde Informatique, 13 Décembre 2018 ; Etude « Les Français et le respect de leur vie privée sur internet », Sondage OpinionWay pour Misakey réalisé en ligne les 21 et 22 novembre 2018 auprès de 1060 personnes représentatives de la population française âgée de 18 ans et plus)

ACTIONS DES AUTORITÉS (CNIL, CEPD)

RGPD – La CNIL publie un premier bilan après 6 mois d'application
Le 23 novembre 2018, la CNIL a publié un premier bilan après l'entrée en application du RGPD le 25 mai. Parmi les points abordés dans ce rapport, nous retiendrons :

- Le nombre de DPO (délégués à la protection des données) atteint 15.000, représentant 32.000 organismes, contre 5.000 CIL (correspondants informatique et libertés) avant le RGPD.
- 1.000 notifications de violations de données ont été reçues à la date de la publication de ce bilan, et plus de 1.200 mi-janvier 2019, soit plus de 5 nouvelles notifications par jour.

Il convient cependant de noter que la nomination d'un DPO ainsi que la notification de la violation de données sont désormais des obligations incombant aux responsables de traitements.

- Par ailleurs, la CNIL a reçu 9.700 plaintes de la part de particuliers, ce qui tendrait à démontrer une plus grande sensibilisation à la protection des données dans le public. Selon la CNIL, l'instruction de ces plaintes, par les organismes mis en cause, entraîne la réorganisation de leurs procédures de traitement des données personnelles. Trois plaintes collectives ont été reçues par la CNIL dont une plainte concernant Google, Amazon, Facebook, Apple et LinkedIn, représentant 45.000 personnes concernées, déposée par la Quadrature du Net.
- Le comité européen à la protection des données (CEPD, ex-groupe de travail Article 29), qui rassemble les autorités des 28 Etats-membres, a notamment pour mission de clarifier la mise en œuvre du RGPD. Ainsi, 19 lignes directrices ont été adoptées et 6 sont en cours d'élaboration (la certification, les codes de conduite, les transferts de données, la vidéosurveillance) ; 20 listes nationales de traitements devant faire l'objet d'une analyse d'impact sur les données personnelles (AIPD) ont également été validées.

(RGPD : quel bilan 6 mois après son entrée en application ? 23 novembre 2018, Site de la CNIL)

Analyse d'impact - La CNIL publie la liste des traitements devant faire l'objet d'une AIPD
Les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques doivent faire l'objet d'une analyse d'impact. Afin d'accompagner les organismes à la mise en œuvre du RGPD, la CNIL a publié la liste des traitements devant faire l'objet d'une analyse d'impact (AIPD), comprenant des lignes directrices permettant aux responsables de traitement de savoir s'ils sont ou non soumis à cette obligation
Cette liste comporte quatorze types d'opérations de traitement pour lesquelles la CNIL estime obligatoire de réaliser une analyse d'impact relative à la protection des données (AIPD). Attention : cette liste n'est pas exhaustive !
(Site de la CNIL : Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise)

Certification de DPO - La CNIL adopte deux référentiels
Parmi les modifications apportées par la loi Informatique et Libertés avec la loi du 20 juin 2018, la Commission dispose désormais de nouvelles compétences en matière de certification. Elle peut ainsi adopter des référentiels de certification et agréer les organismes en charge de leur délivrance.
C'est ce qu'elle a fait, courant octobre 2018 en adoptant deux référentiels pour la certification de DPO. Le premier référentiel, concernant la certification, fixe les conditions à remplir par un candidat DPO et la liste de 17 compétences et savoir-faire requis ; Le second référentiel, concernant l'agrément, fixe

les critères applicables aux organismes souhaitant être habilités par la CNIL pour certifier les compétences d'un DPO, la certification n'étant par délivrée directement par la CNIL.
Parmi les compétences requises, le candidat DPO doit notamment organiser et participer à des audits de protection des données, identifier des mesures de protection des données dès la conception et par défaut adaptées aux risques et à la nature des opérations de traitement ou gérer les relations avec les autorités de contrôle (dont l'instruction des plaintes et les contrôles).
L'agrément de la CNIL n'est toutefois pas obligatoire, tout organisme certificateur pouvant continuer de certifier les DPO sur la base de son propre référentiel.
(Communiqué de la CNIL du11 octobre 2018 « Certification des compétences du DPO : la CNIL adopte deux référentiels »)

Aide à la mise en conformité – La CNIL et Bpifrance publient un guide pratique destiné aux TPE et PME
Pour les petites et moyennes entreprises qui ne seraient pas encore en conformité avec le RGPD, le guide pratique publié par la CNIL et Bpifrance peut être un premier outil d'accompagnement. Ce guide comprend :

- Des fiches thématiques rappelant les grands principes du RGPD ;
- Un plan d'action en quatre étapes : 1. Constituez un registre de vos traitements de données ; 2. Faites le tri dans vos données ; 3. Respectez les droits des personnes ; 4. Sécurisez vos données ;
- Des fiches pratiques relatives aux principaux fichiers mis en œuvre dans les TPE et PME (communication et vente en ligne, relation client, données des salariés) ; et
- Les 6 bons réflexes de la protection des données personnelles.

(Site de la CNIL : La CNIL et Bpifrance s'associent pour accompagner les TPE et PME dans leur appropriation du Règlement européen sur la protection des données (RGPD))

MISES EN DEMEURE POUR NON-CONFORMITÉ

Détournement de finalité du traitement - Cinq sociétés d'assurance mises en demeure
Le 18 octobre 2018, la Présidente de la CNIL a mis en demeure des sociétés des groupes Humanis et Malakoff-Médéric de cesser d'utiliser des données personnelles collectées exclusivement afin de payer les allocations retraite, pour de la prospection commerciale. Les deux groupes gèrent les comptes de plus de 16 millions de personnes.
Les sociétés des groupes Humanis et Malakoff-Médéric ont notamment accès à des données personnelles mises à disposition par les fédérations AGIRC-ARRCO aux fins de recouvrer les cotisations et payer les allocations retraite.
Lors de contrôles réalisés dans les locaux de ces groupes en février et mars 2018, la CNIL a constaté que ces sociétés utilisaient les données personnelles détenues dans le cadre de leur mission d'intérêt général (gestion des régimes de retraite complémentaire) afin de faire de la prospection commerciale pour des produits et services de ces groupes (détournement de finalité).
Les sociétés concernées ont été mises en demeure de cesser ce détournement de finalité dans un délai d'un mois.
La CNIL précise que la mise en demeure n'est pas une sanction. Aucune suite ne sera donnée si les sociétés se conforment à la loi dans le délai imparti, auquel cas la clôture de la procédure sera rendue publique.
(Décisions MED-2018-034 à 038 du 25 septembre 2018 concernant les sociétés Malakoff Médéric Mutuelle, Grand Est Mutuelle, Auxia, Humanis Assurance et Mutuelle Humanis Nationale, et Délibérations de la CNIL du 11 octobre 2018 de rendre publiques ces mises en demeure)

Applications mobiles - Trois sociétés mises en demeure pour absence de consentement au traitement de données de géolocalisation
Entre juin et novembre 2018, la CNIL a mis en demeure trois sociétés de marketing mobile spécialisées dans le traitement de données de géolocalisation à des fins de ciblage publicitaire. Ces sociétés utilisent des SDK (Software Development Kit), intégrés dans le code de l'application mobile des partenaires commerciaux. Le SDK permet ensuite de collecter notamment les données de géolocalisation des utilisateurs puis d'afficher de la publicité ciblée sur leur smartphone, à partir des lieux visités.
Lors d'un contrôle de la CNIL, la Commission a constaté un manquement concernant le consentement des personnes, les utilisateurs n'étant pas toujours informés lors du téléchargement des applications mobiles, qu'un SDK collectait leurs données de localisation. Or, le consentement nécessite une information préalable de l'utilisateur.
Par ailleurs, la société Singlespot, mise en demeure, n'avait pas défini de durée de conservation, ni

assuré la sécurité et la confidentialité des données collectées.
Quant à la société Vectaury, le manquement à l'obligation de recueil du consentement de l'utilisateur concernait également l'utilisation des données pour des enchères en temps réel.
La CNIL considère que ces traitements « *présentent un risque particulier au regard de la vie privée. Ils sont en effet révélateurs des déplacements des personnes et de leurs habitudes de vie* ». Les sociétés concernées ont été mises en demeure de se conformer à la loi dans un délai de trois mois.
Les sociétés Fidzup et Singlespot se sont mises en conformité dans les délais. Les procédures de mise en demeure à leur encontre ont donc été clôturées.
(Décision n°MED 2018-023 du 25 juin 2018 mettant en demeure la société Fidzup et Décision n°MED 2018-023 du 29 novembre 2018 Clôture de la décision n°MED 2018-023 du 25 juin 2018 mettant en demeure la société Fidzup ; Décision n°MED 2018-043 du 8 octobre 2018 mettant en demeure la société Singlespot et Décision n°MED 2018-043 du 29 novembre 2018 Clôture de la décision n°MED 2018-043 du 8 octobre 2018 mettant en demeure la société Singlespot ; Décision n°MED 2018-042 du 30 octobre 2018 mettant en demeure la société Vectaury)

SÉCURITÉ

Assurer la sécurité des données est l'une des principales obligations incombant aux responsables de traitements. Bien que cette obligation de sécurité ne soit pas nouvelle, elle existait déjà à l'article 34 de la loi Informatique et Libertés avant l'entrée en application du RGPD, tous les responsables de traitement, victimes d'une faille de sécurité, sont désormais soumis à une obligation de notification à l'autorité de contrôle compétente (en France, la CNIL) dans les meilleurs délais, et si possible, 72 heures au plus tard après en avoir eu connaissance.
Plusieurs sociétés ont déjà été condamnées pour des atteintes à la sécurité des données et les sanctions continuent de tomber. Dans cette rubrique, nous traitons les questions liées à la sécurité des données, notamment à travers les dernières décisions publiées.

Manquement à l'obligation de sécurité des données personnelles – Uber sanctionnée par les autorités française, néerlandaise et britannique de protection des données pour près d'1,4 million d'euros
La société Uber a révélé en novembre 2017 une faille de sécurité datant d'octobre 2016 et ayant atteint 57 millions d'utilisateurs du service, dont 1,4 millions en France.
L'enquête a permis d'identifier les failles. Après avoir accédé à des identifiants stockés en clair sur la plateforme de développement Github, les deux auteurs de l'attaque ont pu accéder au serveur sur lequel sont stockées les données et ont téléchargé les données de 57 millions d'utilisateurs.
Selon la CNIL, les mesures de sécurité suivantes auraient dû être mises en œuvre : connexion à Github par une mesure d'authentification forte (identifiant, mot de passe et code envoyé sur un téléphone), les identifiants d'accès au serveur n'auraient pas dû être stockés en clair dans le code source de Github, et Uber aurait dû mettre en place un système de filtrage des adresses IP pour accéder à ses serveurs.
La CNIL et les autorités néerlandaise et britannique de protection des données ont ainsi estimé que Uber avait manqué à son obligation de sécurité des données personnelles.
Les sociétés Uber France SAS, Uber Technologies Inc. et Uber B.V. ont été condamnées à des amendes s'élevant à 400.000€ en France, 600.000€ aux Pays Bas et 385.000£ au Royaume-Uni. On notera que compte tenu de la date des faits, le RGPD n'était pas encore applicable. Le montant des sanctions aurait pu être beaucoup plus élevé en vertu du RGPD.
(Délibération de la formation restreinte n°SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société Uber France SAS)

Manquement à l'obligation de sécurité des données personnelles – Amende de 250.000€ à l'encontre de Bouygues Telecom
En mars 2018, la CNIL a réalisé un contrôle sur place chez Bouygues Telecom, suite à un signalement relatif à un problème de sécurité des données personnelles des clients B&You. Lors de ce contrôle, la CNIL a pu confirmer l'existence d'une vulnérabilité permettant d'accéder à des contrats et factures de clients B&You en modifiant une adresse URL sur le site de l'opérateur. Plus de deux millions de clients étaient concernés par cette faille pendant plus de deux ans. Bouygues Telecom a rapidement corrigé la vulnérabilité après en avoir eu connaissance. L'opérateur aurait omis de réactiver la fonction d'authentification à l'espace client après une phase de tests sur son site.

Considérant que la société Bouygues Telecom avait manqué à son obligation d'assurer la sécurité des données personnelles des utilisateurs de son site (art. 34 de la loi Informatique et Libertés), la formation restreinte de la CNIL a prononcé une sanction pécuniaire d'un montant de 250.000 euros.
La formation restreinte a cependant tenu compte de la réactivité de l'opérateur dans la résolution de l'incident de sécurité et des mesures mises en place pour limiter ses conséquences. Comme pour la sanction prononcée contre Uber, le RGPD n'était pas encore applicable dans l'affaire Bouygues Telecom. Le montant des sanctions aurait pu être beaucoup plus élevé.
(Délibération de la formation restreinte n°SAN-2018-012 du 26 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société Bouygues Telecom)

Atteinte à la sécurité des données – Le groupe Marriott révèle un piratage sur 500 millions de clients
Le 19 novembre 2018, le Groupe Marriott a annoncé que sa base de données de réservation au réseau des hôtels Starwood (Sheraton, Le Méridien, etc.) avait été piratée, Marriott en ayant eu connaissance depuis le 8 septembre. La faille de sécurité concernerait près de 500 millions de clients du groupe. Les données en cause comprendraient les noms, adresses postales et emails, n° de téléphone, n° de passeport et dates de naissance, ainsi que des données de carte bancaire.
Cet accès non autorisé au réseau Starwood durait depuis 2014.
En vertu de l'article 33 du RGPD, les responsables de traitement, victimes d'une violation de données à caractère personnel, sont soumis à une obligation de notification à l'autorité de contrôle compétente dans les meilleurs délais, et si possible, 72 heures au plus tard après en avoir eu connaissance. En l'espèce, le groupe Marriott aurait divulgué la faille plus de deux mois après en avoir eu connaissance, posant ainsi un problème de conformité au RGPD, et l'imposition d'une amende de la part des autorités de contrôle des pays concernés.
(« 500 millions de clients des hôtels Marriott piratés », in Le Monde Informatique, 30 novembre 2018)

UNION EUROPÉENNE

Royaume-Uni – Quelles conséquences sur les transferts de données personnelles en cas de « hard Brexit » ?
Le rejet du plan de sortie de l'UE par les parlementaires britanniques le 15 janvier dernier pose notamment des problèmes pour les transferts de données personnelles entre le Royaume-Uni et l'Union européenne, les sociétés de services numériques, les établissements financiers et les multinationales étant particulièrement concernés.
Les sociétés britanniques et leurs co-contractants européens doivent donc être préparés en cas de sortie de l'UE sans accord (« hard Brexit »), afin de minimiser les conséquences d'une telle situation sur leurs activités.
Concernant les transferts de données personnelles entre l'UE et le Royaume-Uni, et bien que ce dernier soit pour l'instant soumis au RGPD depuis mai 2018, un hard Brexit signifie que le Royaume-Uni sera alors considéré comme un pays tiers, sans pouvoir bénéficier du statut de pays offrant un niveau de protection adéquate, au moins jusqu'à ce que la Commission régularise en prenant une décision d'adéquation pour le Royaume-Uni. Les sociétés concernées, à savoir, les responsables de traitement, les cotraitants et les sous-traitants, devront mettre en place des accords de même type que les entreprises à l'international, à savoir les clauses contractuelles types (CCT), un contrat ad hoc, ou pour les multinationales, des BCR. Toutefois, la mise en œuvre de ces accords demande du temps. Des décisions devront être prises très rapidement par les entreprises concernées pour minimiser les blocages de transferts de données entre le Royaume-Uni et le continent européen.
Par ailleurs, en vertu des articles 3(2) et 27 du RGPD, les sociétés britanniques qui traitent d'importants volumes de données de résidents européens devront désigner un représentant situé dans l'un des Etats-membres, comme toute société non-européenne dans la même situation. Quant aux sociétés non-européennes qui auraient désigné un représentant britannique, elles devront désigner un nouveau représentant situé dans l'un des Etats-membres pour se mettre en conformité.
Enfin, les sociétés non-européennes qui auraient désigné l'autorité de contrôle britannique (ICO) comme autorité de contrôle chef de file devront rapidement désigner une nouvelle autorité de contrôle, conformément à l'article 56 du RGPD.

Portugal – Première sanction de 400.000 euros à l'encontre d'un centre hospitalier
Les premières sanctions des autorités de contrôle européennes pour violation du RGPD commencent à tomber… Ainsi, en décembre 2018, l'autorité de contrôle portugaise (CNPD) a imposé une sanction de 400.000 euros à l'encontre du Centre hospitalier Barreiro Montijo (région de Coimbra). La décision du CNPD (non publiée) repose sur trois chefs de violations :

- un accès aux données de patients à un nombre excessif d'utilisateurs, dont des médecins sans lien avec les patients en cause, ou des utilisateurs n'appartenant pas ou plus aux personnels de l'hôpital ;
- l'absence d'application de mesures techniques et organisationnelles pour éviter l'accès non autorisé aux données personnelles ;
- l'incapacité du centre hospitalier d'assurer la confidentialité, la disponibilité et la résilience des traitements, ainsi que l'absence de mesures de sécurité pour assurer une protection adéquate des données.

(« First GDPR fine in Portugal issued against hospital for three violations », in The Privacy Advisor, 3 janvier 2018)

Non-conformité au RGPD – Google poursuivi dans plusieurs pays d'Europe

Parallèlement à la procédure ayant abouti à l'amende de 50 millions d'euros en France, plusieurs plaintes ont été déposées auprès des autorités de contrôle de la protection des données dans sept pays européens (Norvège, Suède, Pays-Bas, Pologne, République Tchèque, Slovénie et Grèce) courant novembre 2018 contre la société Google pour violation du RGPD, et notamment pour non-respect des obligations d'information et de consentement des utilisateurs. Google collecterait les données de localisation des utilisateurs sans leur consentement. Selon le Bureau européen de l'Union des consommateurs (BEUC), Google collecterait les informations de localisation grâce aux applications intégrées dans leurs comptes Google. Selon la société Google, l'historique de la localisation des utilisateurs est désactivé par défaut. Lorsqu'il est activé, l'utilisateur peut le désactiver à tout moment. Cependant, suivant les paramètres choisis, Google peut continuer à collecter ces données.

(« Google attaqué en Europe pour violation du RGPD », in Le Monde Informatique, 28 novembre 2018)

INTERNATIONAL

ETATS-UNIS

Etats-Unis – Qu'est-ce que le Cloud Act ?

Le « Cloud Act » a beaucoup fait parler de lui depuis plusieurs mois. Nous résumons ci-après ses principales finalités afin de mieux comprendre les enjeux de cette législation.

Intégré dans la loi américaine sur les dépenses 2018 (Consolidated Appropriations Act, 2018), le Cloud Act (pour Clarifying lawful overseas use of data act), adopté le 23 mars 2018, donne un cadre légal à la saisie d'emails, documents et communications électroniques localisés dans les serveurs de sociétés américaines et de leurs filiales à l'étranger.

Alors que les sociétés internet et technologiques américaines se félicitent de l'adoption de cette loi qui clarifie le cadre de leur obligation de communication de données aux autorités, les associations de défense des libertés et de la vie privée, dont l'union des libertés civiles américaines (ACLU) et l'Electronic Frontier Fondation (EFF), y sont vivement opposées.

Le Cloud Act devient une alternative au processus actuel de partage d'informations d'utilisateurs entre pays, le MLAT (Mutual legal assistance treaty). Sa mise en oeuvre est en principe plus rapide et simple à exécuter.

Le Cloud Act contient deux grandes séries de dispositions :

1) toute société dont le siège est aux Etats-Unis, ainsi que les sociétés contrôlées par elle, doit communiquer aux autorités américaines, sur leur demande, les données de communication placées sous son contrôle, sans considération du lieu de stockage de ces données ;

2) le gouvernement américain pourra signer des accords internationaux (« executive agreements ») avec des gouvernements étrangers, permettant aux autorités de chaque pays de demander directement aux fournisseurs de services de communication, de traitement et de stockage électroniques de données relevant de la juridiction de l'autre pays, la divulgation des données de communication les intéressant, sans avoir à passer par les procédures plus lourdes des MLAT ou des commissions rogatoires internationales.

Les demandes de communication de données concernées par ces accords ne peuvent viser que les infractions les plus graves (« *serious crime* »). L'objectif est d'accélérer la procédure d'investigation par les forces de l'ordre.

Des questions se posent cependant sur la compatibilité entre le Cloud Act et le RGPD. Le Privacy Shield, applicable aux transferts entre sociétés européennes et sociétés américaines adhérant au programme, ne couvre pas les entités gouvernementales. Le transfert de données personnelles aux autorités américaines par une société américaine ou sa filiale, en application d'une demande fondée

sur le Cloud Act ne serait pas conforme au RGPD. Il conviendra de suivre comment le Cloud Act sera mis en œuvre dans les prochains mois.
(Consolidated Appropriations Act, 2018 et Clarifying lawful overseas use of data act (Cloud Act), adopté le 23 mars 2018)

Relations EU-US – Le Privacy Shield renouvelé pour un an
Pour rappel, le Privacy Shield (« Bouclier de protection des données »), qui a remplacé le système du Safe Harbor en 2016, permet le transfert de données à caractère personnel entre des sociétés européennes et des sociétés américaines adhérentes au programme.
Le 5 juillet 2018, le Parlement européen a voté la suspension du Privacy Shield. Cette résolution non contraignante demandait à la Commission de suspendre le programme sous réserve d'une mise en conformité par les Etats-Unis d'ici le 1er septembre.
Dans un rapport publié le 19 décembre 2018, la Commission européenne déclare que le niveau de protection des données personnelles transférées depuis l'Europe vers les Etats-Unis en application du Privacy Shield reste adéquate. Le Privacy Shield est donc renouvelé pour un an.
Cette deuxième revue annuelle de l'accord s'est tenue les 18 et 19 octobre 2018 à Bruxelles. Le rapport relève les mesures prises par les Etats-Unis sur la base des recommandations de la Commission, notamment :

- le renforcement de la procédure de certification des sociétés. Celles-ci ne peuvent désormais annoncer leur adhésion au Privacy Shield qu'après la finalisation de la procédure de certification par le Ministère du Commerce (DoC) ;
- l'amélioration du suivi de la conformité des sociétés au Privacy Shield.

La Commission a cependant identifié plusieurs points devant être pris en compte, dont la nomination d'un médiateur dans le cadre de cet accord et l'évaluation de son rôle dans le traitement et la résolution des plaintes.
(« European Commission publishes second annual report on EU-U.S. Privacy Shield », in Technology Law Dispatch, 20 décembre 2018)

ASIE

Données personnelles - Le Japon et la Corée du Sud sur la voie d'une décision d'adéquation par la Commission européenne
La Commission européenne est actuellement en train d'étudier la possibilité d'intégrer le Japon et la Corée du Sud dans la liste des pays tiers bénéficiant d'une décision d'adéquation, permettant ainsi de libéraliser les transferts de données personnelles entre l'Union européenne et ces deux pays d'Asie.
Les discussions d'adéquation avec le Japon ont débuté il y a deux ans, en janvier 2017 et un accord de principe a été conclu en juillet de la même année, en parallèle avec la conclusion de l'accord de partenariat économique entre l'Union européenne et le Japon. Un projet de décision d'adéquation a ensuite été publié par la Commission en septembre 2018. La décision définitive est cependant toujours en suspens.
La première loi de protection des données japonaise date de 2005. Une nouvelle loi de protection des données est entrée en vigueur le 30 mai 2017. La loi de 2017 a intégré de nouveaux concepts dans le droit japonais, tels que les notions de données sensibles et d'anonymisation des données, et prend notamment en compte le RGPD. Une autorité de contrôle indépendante (la Commission de protection des données personnelles - PPC) a également été créée.
Les transferts de données personnelles du Japon vers des pays tiers sont limités aux pays figurant sur une liste blanche spécifique. Les Etats-membres de l'Union européenne seraient les premiers pays à figurer sur cette liste.
Le projet de décision d'adéquation identifie les principales différences entre les réglementations japonaise et européenne et comprend, en annexe, des règles supplémentaires que les sociétés japonaises destinataires de données personnelles en provenance de l'UE s'engageraient à respecter. Ce projet est cependant en cours d'examen par le Parlement européen et le CEPD, et aucune date n'a été arrêtée pour son adoption.
Les sociétés japonaises destinataires de données personnelles de sociétés françaises peuvent toutefois continuer à fonctionner avec les clauses contractuelles types, contrat ad hoc ou règles contraignantes d'entreprise (BCR)

Concernant la Corée du Sud, des discussions d'adéquation sont également en cours depuis deux ans. Des députés européens se sont ainsi rendus à Séoul fin octobre 2018 et ont rencontré les autorités coréennes, y compris la Commission des communications coréenne et l'Agence de l'internet et de la sécurité coréenne (KISA) afin d'avancer dans les discussions.

Nous vous tiendrons informés des suites données à ces procédures.
(« Japan's long road for adequacy under the GDPR", in The Privacy Advisor, 18 décembre 2018 ; « MEPs to look into data protection measures in South Korea », Communiqué de presse du Parlement européen, 29 octobre 2018)

AUTRES

Changement de présidente à la CNIL
Marie-Laure Denis vient d'être nommée Présidente de la CNIL, en remplacement d'Isabelle Falque-Pierrotin, dont le mandat arrive à échéance fin janvier. Isabelle Falque-Pierrotin était à la tête de la CNIL depuis 2011. Son mandat avait été reconduit en 2014. Marie-Laure Denis est ancien membre du CSA et de l'Arcep. Sous réserve de la validation de sa nomination par le Parlement, elle prendra ses fonctions le 1er février prochain.

PUBLICATIONS

Retrouvez sur le Blog du Cabinet toutes nos dernières publications

Directeur de la publication : Bénédicte DELEPORTE
Editeur : DELEPORTE WENTZ AVOCAT - 5, rue Tronchet – 75008 Paris - Tel 01.40.17.95.86