

Bilan 2015 de la CNIL

Le bilan 2015 constate une augmentation et une diversification des demandes auprès de la CNIL et en particulier des plaintes. 7908 plaintes ont été enregistrées, soit 2000 de plus qu'en 2014. Ce nombre s'explique en partie par la mise en place, en mars 2015, d'un service de dépôt en ligne, qui a recueilli 65 % des demandes. La CNIL a également procédé à 501 contrôles et a constaté une augmentation de ses mises en demeure : 93 en 2015, contre 62 en 2014.

LINC, un nouveau média dédié aux innovations numériques

Pour contribuer aux débats sur le numérique, la CNIL a lancé, le 21 avril, LINC, « Laboratoire d'innovation numérique de la CNIL ». Avec ce nouvel espace accessible à l'adresse linc.cnil.fr, la CNIL entend partager et diffuser plus largement ses travaux et réflexions en direction de l'ensemble des acteurs de l'innovation et de l'écosystème numérique (chercheurs, start-up, labs, etc.).

Big data dans la santé

La loi de modernisation du système de santé du 26 janvier 2016 facilite l'exploitation et le partage des données de santé des particuliers, en prévoyant notamment la création d'un système national des données de santé. Alors que la Cour des Comptes estime que ces données doivent être plus largement accessibles et ouvertes, la CNIL, dans son rôle, semble s'y opposer. Dans ce cadre, le ministère de la Santé vient de lancer une consultation citoyenne ouverte jusqu'au 20 juin 2016, accessible via le site faire-simple.gouv.fr.

Contours de la réforme de la protection des données personnelles au sein de l'UE

LES FAITS

Initié en 2012 par la Commission européenne, le Parlement européen vient d'adopter ce 14 avril 2016, après 4 ans de travaux et débats, le Règlement général sur la protection des données personnelles (RGPD) visant à redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises.



PRINCIPAUX AXES DE LA RÉFORME

Le Règlement remplacera l'actuelle « vieille » directive 95/46 sur la protection des données qui, datant de 1995, alors qu'Internet n'était encore qu'à ses débuts, est aujourd'hui devenue obsolète. Particulièrement complet, avec plus de 250 pages, ce texte marque une étape capitale dans la construction du droit effectif à la protection des données personnelles au sein de l'Union européenne. Le Règlement atténue considérablement le poids des formalités préalables, caractéristiques du régime actuel, et propose un nouvel équilibre de droits, d'obligations et de sanctions reposant principalement sur les principes d'*accountability* et de *privacy by design*. Ainsi, les entreprises devront s'adapter à un principe de responsabilité accrue qui se traduira, tout d'abord, par l'obligation pour le responsable de traitements, mais également pour les sous-traitants de rendre des comptes (*accountability*). Un registre détaillé des traitements de données personnelles devra être conservé et mis à la disposition des autorités de contrôle. Ensuite, les entreprises devront prendre en compte les obligations du Règlement dès la conception de projets impliquant le traitement des données personnelles et par défaut selon la démarche *privacy by design* en intégrant les outils de protection directement dans le produit, comme une fonctionnalité de base. Enfin, sauf s'il n'y a pas de risques pour les droits et libertés des individus, tous les responsables de traitements, quel que soit leur secteur d'activité, se verront imposer une obligation de notification des violations de données à caractère personnel à l'autorité de contrôle sans délai et, si possible, au plus tard dans les 72 heures. S'agissant des sanctions susceptibles d'être prononcées

en cas de manquement, elles pourront désormais aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total d'une entreprise. Ce mécanisme de sanction particulièrement renforcé constitue une des principales innovations et rapproche cette matière du droit de la concurrence. Autres points clés du RGPD à relever : un champ d'application matériel et géographique étendu ; le renforcement des conditions du consentement à un traitement et en particulier du consentement parental ; l'encadrement du profilage ; la désignation obligatoire d'un *Data Protection Officer* ; ou encore la consécration attendue du droit à l'oubli et du droit à la portabilité des données.

PROCHAINES ÉTAPES

L'adoption d'un règlement constitue un véritable enjeu puisqu'il s'agit d'un acte normatif à portée générale et contraignant pour les États membres, sans transposition nationale, et donc favorisant une mise en œuvre uniforme. Le Règlement entrera en vigueur 20 jours après sa publication au *Journal officiel* de l'UE. Ses dispositions seront directement applicables dans tous les États membres deux ans après cette date, soit courant mai 2018. ~

CE QU'IL FAUT RETENIR

Le Règlement apporte des changements significatifs auxquels les entreprises doivent se préparer, dans le cadre du délai d'application de 2 ans laissé pour se mettre en conformité, notamment au regard de l'alourdissement des sanctions.