22e Sitem : « Les sanctions en matière de protection des données seront appliquées » (M. Jean-Baptiste)

Paris - Publié le vendredi 26 janvier 2018 à 11 h 00 - Actualité n° 111560

« Nous en sommes là aujourd'hui avec le RGPD parce que les sanctions qui étaient encourues par les personnes et grandes sociétés qui violaient les principes de protections de données étaient trop faibles (…). Aujourd'hui les sanctions ont vocation à être appliquées. Dès le mois de mai 2018, la CNIL va se mettre en chasse, des contrôles seront effectués. Quand on est un organisme public ou un organisme en vue, forcément on peut servir d'exemple. La sanction très dissuasive peut aller jusqu'à 10 millions d'euros ou 4 % du chiffre d'affaires annuel mondial en cas de manquement », indique Michelle Jean-Baptiste, avocate spécialisée dans la protection des données, lors de la conférence « Règlement européen sur la protection des données : ce qui change pour les professionnels des musées », organisée par le cabinet de conseil et d'information en billetterie My Open Tickets, dans le cadre du Sitem, le 24/01/2018.

Le nouveau règlement européen sur la protection des données personnelles, ou RGPD, entrera en application le 25/05/2018. L'objectif de ce texte est de renforcer les droits des personnes, de responsabiliser les acteurs traitant des données et de crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données. La conférence visait elle à « expliquer comment préparer son arrivée dans [les] établissements, ses principaux impacts sur [les] billetteries et bases de données ».

« La démarche pour la mise en conformité c'est planifier et identifier les traitements, les acteurs, les risques, les zones de vigilance, réaliser un état des lieux avec les outils imposés, contrôler des mesures et effectuer veille juridique et technologique », explique Merwann Bensiali, expert RGPD, ActeCil et ancien consultant de la CNIL.

News Tank rend compte des échanges.

© News Tank

Intervenants

- Merwann Bensiali, expert RGPD, ActeCil et ancien consultant de la CNIL
- Michelle Jean-Baptiste, avocate spécialisée dans la protection des données
- Alexandre Poltoratzsky, responsable des ventes chez Irec Ticketing Technology
- Thierry Rosset, chef du département accueil, vente, individuels et groupes chez Universcience
- Modération : Corinne Lefebvre, responsable de ventes freelance

« La mise en conformité, un engagement éthique et de qualité » (Merwann Bensiali)

- « Le RGPD est né en 2016. Historiquement, il y a eu la loi informatique et liberté (1978), puis une directive européenne (1995) qu'il a fallu transposer.
- Est ensuite venue l'idée de mettre en place un règlement européen qui sera applicable pour tous à partir de mai 2018. Le grand axe est une responsabilisation et un rééquilibrage de tous les acteurs. Ce règlement renforce le droit des personnes et vise à assurer une meilleure coopération de la part des autorités de contrôle.
- En matière de collecte de données, les structures vont être amenées à mettre en place un certain nombre de traitements. Le règlement européen aura pour vocation de cibler tous les traitements de données à caractère personnel pour les résidents européens.
- Au niveau de la co-responsabilité, le responsable de traitement est considéré comme le donneur d'ordre. Le sous traitant sera le prestataire, il agit pour "pour le compte de". Mais le règlement européen prévoit maintenant une tenue des registres pour l'ensemble des acteurs.
- Les principaux changements pour être en phase avec les nouveaux concepts du RGPD sont :
- L'"accountability" : l'obligation de documenter l'ensemble des procédures qui permettent d'être en conformité avec la loi en temps réel
- Le registre de traitement obligatoire pour les organismes de plus de 250 salariés ou si les traitements sont "à risque"
- L'obligation pour tous les organismes de désigner un délégué à la protection des données qui sera le chef d'orchestre de la conformité au sein de l'organisme
- Le "privacy by design" / "privacy by default" : principes de protection de la vie privée dès la conception / protection de la vie privée par défaut. Consiste à agir de manière proactive et préventive
- Le profilage : toute forme de traitement automatisée qui vise à évaluer certains aspects du comportement d'une personne
- La pseudonymisation : vise à, dans la mesure du possible, traiter en priorité de la donnée pseudonyme
- L'analyse d'impact : outil obligatoire qui permet d'identifier les risques et de mettre en place des outils afin de les réduire.
- Pourquoi se mettre en conformité ? C'est un engagement éthique et de qualité, c'est un moyen efficace de lutte contre les violations de données qui peuvent être importantes, tant sur le plan financier que sur le plan de l'image, cela réduit le risque juridique.

- La démarche pour la mise en conformité c'est planifier et identifier les traitements, les acteurs, les risques, les zones de vigilance, réaliser un état des lieux avec les outils imposés, contrôler des mesures et effectuer veille juridique et technologique. »

Merwann Bensiali, expert RGPD, ActeCil et ancien consultant de la CNIL

« Avec la RGPD, les sanctions seront à la hauteur de l'infraction » (Michelle Jean-Baptiste)

- « Nous en sommes là aujourd'hui avec le RGPD parce que les sanctions qui étaient encourues par les personnes et grandes sociétés qui violaient les principes de protection de données étaient trop faibles.
- Le principe du RGPD est de dire que les sanctions doivent être à la hauteur de l'infraction.
- En 1978, la sanction maximale encourue était de 150 000 euros. Cette dernière a augmenté lors de la directive de 1995, mais de manière insuffisante.
- Aujourd'hui les sanctions ont vocation à être appliquées. Le RGPD, c'est dire "on veut frapper fort, on ira rechercher les responsabilités".
- Dès le mois de mai 2018, la CNIL va se mettre en chasse, des contrôles seront effectués. Quand on est un organisme public ou un organisme en vue, forcément on peut servir d'exemple.
- La sanction très dissuasive est fixée jusqu'à 10 millions d'euros ou à 2 % du chiffre d'affaires annuel mondial, en cas de manquement au privacy by design / privacy by default.
- La première étape va être d'identifier le type de données collectées, de voir comment elles sont collectées, si l'organisme est collecteur gestionnaire de la donnée ou juste co-collecteur ou sous-traitant ou prestataire de service.
- Il existe un autre niveau de sanction à 4 % du chiffre d'affaires annuel mondial appliqué en cas de manquement constaté sur les données à caractère personnel. Cela relève de la protection des personnes. Sur ce sujet, il y a eu trop d'abus.
- Nous rentrons dans une dynamique où il faudra mettre en place des registres, être en capacité en cas de contrôle de présenter ce qui est fait exactement des données. »

Michelle Jean-Baptiste, avocate spécialisée dans la protection des données

« Les musées ont de plus en plus envie de référencer les données » Alexandre Poltoratzsky

- « Le logiciel de billetterie est un logiciel de vente multicanal avec un ensemble de produits qui sont associés, la plupart du temps, à un système de contrôle d'accès.
- Dans la plupart des cas, les données de billetterie sont anonymes. Mais, de plus en plus, dans les pratiques des musées, vous avez la volonté de référencer de plus en plus de données contact pour pouvoir fidéliser les visiteurs.

- Lorsqu'un musée vend des adhésions, lorsque le visiteur fait une réservation et lors de la vente en ligne, l'établissement rentre dans le champ du règlement européen.
- Quel est le rôle de l'éditeur de système de gestion des publics ? En théorie, le propriétaire de la donnée est le seul responsable et propriétaire des données. Mais, en faisant une lecture plus restrictive du règlement, on s'aperçoit que l'éditeur participe à déterminer les moyens de traitement des données. L'éditeur de logiciel fournit les moyens techniques qui vont permettre de capter et d'enregistrer les données.
- Le règlement a un champ d'application très large. Il faut attendre que la CNIL intervienne pour donner des précisions sur les modalités d'intervention. »

Alexandre Poltoratzsky, responsable des ventes chez Irec Ticketing Technology

« La collecte de datas crée plus d'obligations » (Thierry Rosset)

- « Les nouveaux usages que nous observons depuis un an se concentrent surtout autour des réservations. Or, si un visiteur réserve, il s'identifie. De fait, nous avons de plus en plus de datas. C'est intéressant pour organiser, bien préparer le site, mais cela crée également des obligations.
- Au sein de notre organisation, nous avons différents outils qui traitent les données contact. Nous avons constaté que ces données étaient éparpillées, même si chaque entité qui gère ses données était respectueuse du cadre défini. Il nous est apparu important de refaire un tour de piste, de vérifier que l'organisation de ces données était conforme à la réglementation. Nous avons également saisi cette opportunité pour imaginer une optimisation de ce dispositif.
- Nous avons engagé une politique de sécurité des systèmes d'information pour le traitement des datas et les traitements maîtrisés. Nous avons fait une cartographie complète de ces données et nous avons envisagé une analyse de risque et d'impact.
- Pour le moment, nous sommes dans un processus d'optimisation sur nos bases de données pour aussi mieux les maîtriser.
- Nous tendons à aller vers un outil unique. »

Thierry Rosset, chef du département accueil, vente, individuels et groupes chez Universcience