Fic 2016 : Etude d’impacts sur la vie privée : suivez la méthode de la CNIL

Fic 2016 : Etude d’impacts sur la vie privée : Suivre la méthode de la CNIL

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.
Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :
• Étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
• Étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
• Étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
• Validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Denis JACOPINI EST FORMATEUR EN ETUDE D'IMPACT SUR LA VIE PRIVÉE

Réagissez à cet article

Source : *Etude d’impacts sur la vie privée : suivez la méthode de la CNIL – CNIL – Commission nationale de l’informatique et des libertés*

Fic 2016 : l’avenir du Safe Harbor fixé début février

Fic 2016 : l’avenir du Safe Harbor fixé début février

Lundi 25 Janvier, en fin de journée à Lille, lors d'une conférence plénière organisée au sein du FIC 2016, Isabelle Falque-Pierrotin a indiqué d'autre part que le G29 se réunirait début février pour savoir ce qu'il adviendra de l'annulation du Safe Harbor.

Si la présidente de la CNIL a été discrète sur le sujet, plusieurs pistes se dégagent selon nos sources. Les clauses types et les Binding Corporate Rules (ou BCR), à savoir les codes de conduite internes aux entreprises, pourraient ne pas perdurer, sans doute parce qu'elles ne rabotent en rien la curiosité des services américains. Au-delà des autorisations individuelles, la seule issue disponible pour les acteurs du Web resterait finalement les décisions d'adéquation. Avec elle, dans un État déterminé, une autorité de contrôle devrait ainsi mener une analyse approfondie des lois nationales du pays tiers pour autoriser ou interdire le transfert.
Bien entendu, une telle position pourrait être jugée inutile si les États-Unis et l'Europe parvenaient finalement à un accord sur un hypothétique #Safe Harbor 2. Sur le terrain politique, cependant, cette réalité n'est qu'un rêve encore trop lointain. Toujours au FIC, David Martinon, représentant spécial de la France pour les négociations internationales sur la société de l'information et l'économie numérique, a pointé aujourd'hui encore l'absence d'accord entre les différents pays européens sur ce dossier.

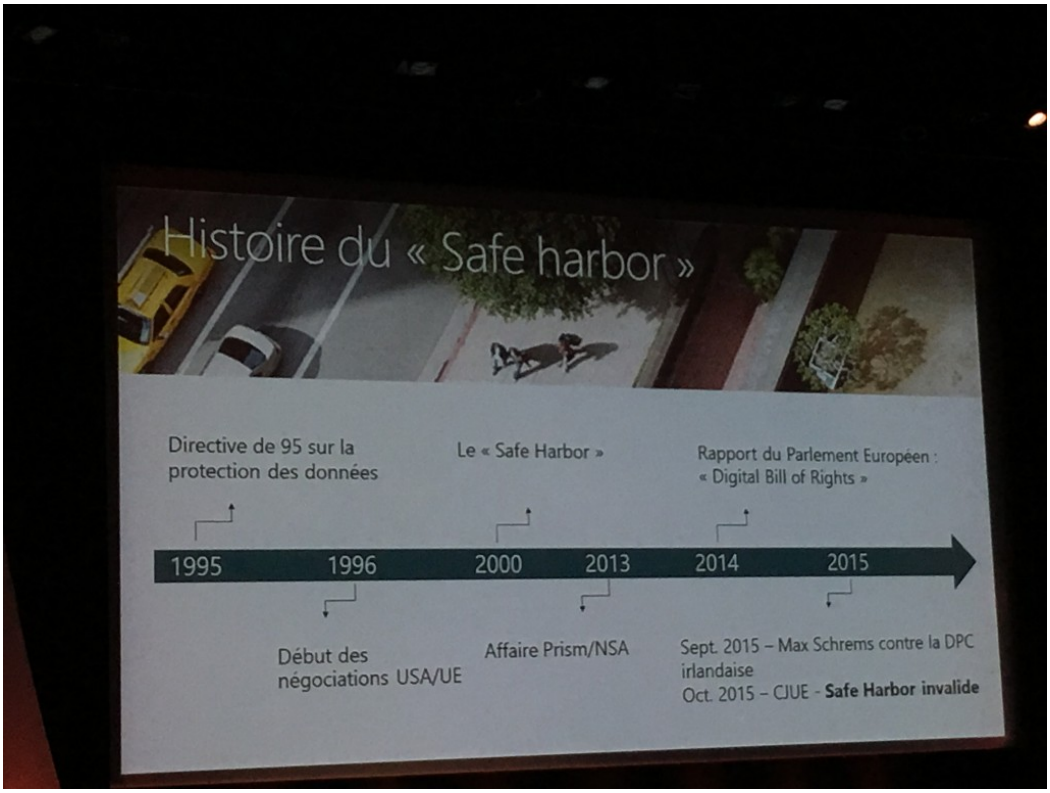
Réagissez à cet article

Source : *Données personnelles : l'avenir du Safe Harbor fixé début février*

Fic 2016 : Comment mériter la confiance à l’heure de la remise en question du Safe Harbor

	Fic 2016 : Comment mériter la confiance à l’heure de la remise en question du Safe Harbor

Le 6 octobre, la cours de justice de l'union européenne a invalidé le Safe Harbor. Cette session a pour but d'expliquer comment il est possible de mériter la confiance et de respecter la loi pour un fournisseur de service Cloud comme Microsoft.



Pour rassurer le groupe de travail de l'article 29, et pour venir compléter des mesures de sécurité se basant sur la norme iso 27001, plusieurs pistes ont été envisagées par Microsoft dont :
Faire appel à des contrôleurs de mises en conformité indépendants
S'engager à fournir la liste des sous-traitants…
Modifier ses conditions générales de ventes
S'engager à conserver confidentielles les données stockées hors cadre judiciaire

---

Réagissez à cet article

Source : *FIC 2016*

Quels changements anticiper ? Le règlement européen sur les données personnelles annoncé pour le printemps :

	Quels changements anticiper Le règlement européen sur les données personnelles annoncé pour le printemps : ?

Ce règlement, dont le premier projet remonte à 2012, est appelé à remplacer la directive de 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ». Son objectif est d'uniformiser les règles en matière de protection des données personnelles en Europe, de garantir la libre circulation de ces données sur le territoire de l'Union et de simplifier l'exercice de leurs droits par les citoyens européens.

Après des débats parfois acharnés entre les acteurs en présence, que ce soit les CNIL européennes, les acteurs de l'internet et du Big-Data ou encore les représentants des consommateurs, une version consolidée a été arrêtée et diffusée le 15 décembre 2015.
De la loi du 6 janvier 1978 au futur règlement, la législation en matière de protection des données personnelles est allée dans le sens d'une complexité et d'une incertitude toujours plus grande. Les entreprises peuvent-elles attendre plus de sécurité juridique du futur règlement ? La réponse est contrastée.

Un projet de texte stabilisé… mais pas encore adopté
Il convient tout d'abord de tempérer l'enthousiasme affiché des institutions européennes : le texte définitif n'est pas encore adopté. Après un premier vote du Parlement européen en mars 2014, le Conseil de l'Union européenne donnait mandat au Luxembourg en juin 2015, dans le cadre de la présidence tournante de l'Union européenne, pour parvenir à un consensus sur le projet de règlement au plus tard fin décembre de la même année. Au terme de discussions intenses, Parlement et Conseil sont parvenus à un accord *in extremis* avant la trêve des confiseurs sur un document de pas moins de 200 pages…
Cet accord n'est pour le moment que politique, et la prochaine étape est un vote en deuxième lecture par le Parlement européen pour adoption définitive.
Le règlement européen sera ensuite applicable dans un délai de deux ans après son adoption. La différence essentielle par rapport à la directive de 1995 est que ce texte sera directement applicable au sein de l'Union européenne, sans que chacun des 27 états ne doive adopter des lois nationales de transposition, ce qui aurait nécessairement nui à l'objectif d'harmonisation. Les règles européennes nouvelles remplaceront donc automatiquement les règles nationales existantes incompatibles. Ainsi, pour ses 40 ans, la Loi française du 6 janvier 1978 dite « Informatique et Libertés » va se retrouver fortement vidée de sa substance.
Les entreprises ont donc encore un peu de temps devant elles pour se préparer à la mise en œuvre des nouvelles règles. Quels sont les changements majeurs à anticiper ?

***« Accountability »* et « *Privacy by Design* » sont des termes qui doivent devenir familiers**
Quelles données pourront être traitées ? Quelle durée de conservation appliquer ? Quels outils techniques installer ? Quelles formalités accomplir ?
Si le règlement uniformise la réponse à ses questions au sein de l'Union européenne… il ne les simplifie par nécessairement. Une large place sera faite à l'interprétation des dispositions nouvelles.

La **définition des données personnelles** ne change pas fondamentalement. Le règlement s'applique aux traitements des données identifiantes ou permettant d'identifier une personne, que ce soit directement ou indirectement. Le projet de règlement ajoute toutefois une série d'exemples de données qui permettent d'identifier une personne : son nom, mais également un numéro d'identification, une donnée de localisation, un identifiant d'un compte en ligne, ainsi que des références à des informations relatives à l'identité physique, génétique, mentale, économique, sociale ou culturelle d'une personne. Ces précisions sont dans la logique de la position actuelle des juridictions européennes et françaises.
S'agissant des **modalités de traitement** des données personnelles, il est abondamment fait référence dans le texte à la notion de *Privacy by Design*.
Qu'est-ce que cela signifie concrètement ? Les entreprises seront désormais tenues d'anticiper les sujets relatifs aux traitements de données dès les premières étapes de leurs projets informatiques, afin qu'il soit vérifié en amont que les développements à intervenir, où les logiciels à implémenter, seront conformes aux exigences imposées par le règlement.
Le responsable du traitement devra ainsi « *implémenter les mesures techniques et organisationnelles appropriées, telles que l'anonymisation, qui sont conçues pour mettre en œuvre les principes de protection des données, […] d'une manière effective et d'intégrer les protections nécessaires dans les traitements de manière à respecter les exigences du règlement et à protéger les droits des intéressés.* »
Une pondération devra en effet être faite entre coûts, état de l'art, contexte, finalités des traitements concernés, risques pour les droits et libertés des individus, etc. Autant de concepts dont la cohabitation laissera une grande place à une appréciation au cas par cas. Le règlement envisage qu'un mécanisme de certification soit mis en place, probablement afin de faciliter cette appréciation, bien que les procédures de certifications pèchent parfois par leur complexité.
Comme en l'état actuel de la législation, le règlement ne prévoit pas expressément de **durée de conservation des données**, et l'on peut le regretter. L'appréciation d'une durée de conservation des données sous une forme identifiante « *qui n'excède pas la durée nécessaire aux finalités pour lesquelles [les données] sont collectées et traitées* », place souvent le responsable de traitement dans une situation d'insécurité juridique. En revanche, dans sa dernière version, le projet de règlement prévoit que cette durée de conservation, ou *a minima* les critères retenus pour fixer cette durée, devront être portés à l'attention de la personne concernée dès la collecte. Les responsables de traitements devront donc apporter une attention particulière à ce sujet avant la mise en œuvre du traitement.
Les **formalités administratives** seront allégées : moins de notifications préalables aux autorités nationales, moins d'interlocuteurs. Un des objectifs principaux de ce texte est de garantir la libre circulation des données au sein de l'Union européenne. Ainsi, pour les groupes ayant des établissements dans plusieurs pays d'Europe, ou une activité ciblant plusieurs Etats-Membres, le principe du « guichet unique » permettra que les formalités requises ne soient effectuées qu'auprès de l'autorité de l'Etat Membre dans lequel le groupe a son établissement principal, les autorités des différents Etats Membres devant ensuite coopérer entre elles.
Les sociétés établies en dehors de l'Union européenne, mais ayant une activité ciblant le public européen, devront quant à elles désigner un représentant sur le territoire de l'Union, qui agira comme point de contact unique, tant pour les autorités que pour les personnes dont la société en question traite les données. A l'instar des pratiques en matière de fiscalité, cette dernière exigence incitera très probablement les grands acteurs du numérique non établis en Europe à désigner un représentant dans un Etat Membre dont l'autorité nationale de protection des données aura des règles réputées plus souples, ou disposera de moins de moyens pour diligenter des contrôles ou engager des procédures de sanction. Ces disparités devraient toutefois être tempérées par la coordination qu'assurera la nouvelle autorité européenne instaurée par le règlement.
En revanche, les **procédures internes seront quant à elles décuplées…** Un contrôleur à la protection des données devra être désigné dans les entités publiques et dans les entreprises traitant des données personnelles à une échelle importante. Il convient de souligner qu'il n'y a pas de seuil chiffré permettant à une entreprise de déterminer si elle doit ou non désigner une telle personne. Sa désignation est requise lorsque l'activité de l'entreprise implique le traitement de données personnelles de manière régulière et systématique sur une large échelle…
Le contrôleur pourra alternativement être salarié ou prestataire de service. Le responsable de traitement devra également tenir à jour des registres des traitements mis en œuvre sur le même modèle que ce qui existe actuellement pour les CIL. Dans la logique du principe d'« *accountability* », ces mesures devront permettre au responsable de traitement de démontrer que les traitements qu'il met en œuvre se font en conformité avec le règlement.
Afin de faciliter aux entreprises la mise en œuvre de telles procédures, et la démonstration de conformité du responsable de traitement à ses obligations, le règlement renvoie ici encore à un mécanisme de certification ou à des codes de conduite.

Et côté personnes physiques, quels droits ? Quelles protections nouvelles ?
Les personnes dont les données sont traitées devront bénéficier d'une **information plus large** sur les traitements qui les concernent. Outre les informations qui doivent déjà être fournies lors de la collecte de données en application de la Loi Informatique et Libertés, le responsable de traitement doit notamment préciser le fondement juridique du traitement, ainsi que la possibilité de déposer plainte auprès d'une autorité compétente d'un Etat Membre. Les mentions d'informations fournies par les responsables de traitement devront donc être ajustées.
Les personnes dont les données sont traitées bénéficieront d'un **droit à la portabilité de leurs données**. Les responsables de traitement devront donc être en mesure de restituer aux personnes dont les données sont traitées lesdites données, et ce dans un format standard et exploitable, afin qu'elles puissent être communiquées à un autre prestataire de services. Cette communication de données pourra même se faire directement au nouveau prestataire sur demande de la personne concernée.
Le projet de règlement prévoit des règles nouvelles encadrant **les traitements de données relatives aux enfants**. Ainsi, l'article 8 du projet de règlement prévoit une disposition visant à interdire aux services de la société de l'information destinés aux mineurs de 16 ans de recueillir leurs données personnelles sans autorisation préalable d'un titulaire de l'autorité parentale. Les Etats Membres pourront décider d'abaisser cette limite d'âge jusqu'à 13 ans. Le texte ajoute que le responsable de traitement devra fournir des efforts raisonnables, au regard des technologies disponibles, pour vérifier que le consentement est bien fourni par le titulaire de l'autorité parentale.
Les éléments détaillés ci-dessus ne sont que quelques points d'attention extraits parmi les 209 pages du projet de règlement dans sa dernière version. Les subtilités se cachent dans les détails et les 4 années de modifications et de reformulations du texte depuis sa première mouture ont pu altérer sa cohérence. Les deux années avant l'entrée en vigueur des dispositions nouvelles ne seront pas de trop pour permettre aux entreprises de se mettre en conformité. D'autant qu'en cas de manquement, les sanctions administratives pourront désormais aller jusqu'à 20 000 000 d'euros ou 4% du chiffre d'affaires mondial… ce qui est sans commune mesure avec les 150 000 euros d'amende que peut à ce jour prononcer la CNIL.

Réagissez à cet article

Source : *Le règlement européen sur les données personnelles annoncé pour le printemps : Quels changements anticiper ? – Féral-Schuhl Sainte-Marie*

La Cnil pourra infliger jusqu'à 20 millions d'euros d'amende

La Cnil pourra infliger jusqu'à 20 millions d'euros d'amende

Pourtant hostile au départ, le gouvernement est désormais favorable à un renforcement du pouvoir de sanction de la Cnil : jusqu'à 20 millions d'euros en cas de récidive. Et la portabilité des données ? « Ce sont les gros qui sont énervés » répond Axelle Lemaire.

Le projet de loi République numérique présenté par Axelle Lemaire est actuellement débattu par les députés. De nombreux amendements sont à l'étude, dont certains rejetés par le gouvernement. Celui-ci s'est en revanche rallié à une proposition des parlementaires en faveur d'un renforcement du pouvoir de sanction de la Cnil, l'autorité en charge de la protection des données personnelles.
Selon Les Echos, le gouvernement soutient donc désormais un amendement prévoyant, en cas de récidive, de permettre à la Cnil d'infliger une sanction pouvant atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. A ce jour, en cas de récidive, la sanction ne peut pas dépasser les 300.000 euros.

Les « gros » sont « énervés »

Une autre mesure portant sur les données fait grincer des dents au sein de plusieurs organisations d'entreprises du numérique : la portabilité des données entre plateformes.
« Par son caractère large, il impose des contraintes extrêmement lourdes à des secteurs dans lesquels la portabilité n'apporte pas d'intérêt du point de vue des consommateurs et sur le plan de la concurrence. En l'état, il menace directement les investissements massifs réalisés par les entreprises du secteur afin d'améliorer leurs services » dénonçaient-elles notamment dans un communiqué du 14 janvier.
Message reçu au sein du gouvernement ? Difficile à dire puisque la ministre du numérique déclarait lundi 18 janvier sur RMC vouloir « protéger la concurrence ». « Ce sont les gros qui sont énervés, pas les petits » ajoutait-elle.

Réagissez à cet article

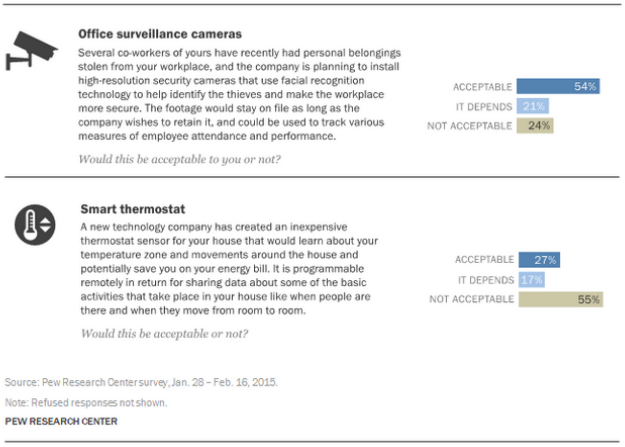
Source : *La Cnil pourra infliger jusqu'à 20 millions d'euros d'amende*

Données personnelles : les Américains sont prêts à faire des concessions

	**Données personnelles : les Américains sont prêts à faire des concessions**

Selon une étude de Pew Research Center, une large proportion d'Américains est prête à dévoiler des informations personnelles en échange d'un bien ou d'un service. Du gagnant-gagnant ?

La protection de la vie privée serait un concept à géométrie variable pour les Américains, selon une étude menée par le **Pew Research Center**. Selon lui, une majorité d'Américains ne verraient pas d'inconvénient à partager avec des tiers leurs données personnels, en échange d'un produit, d'un service, ou pour d'autres bénéfices.
Ainsi, 54% d'entre eux estiment qu'il est acceptable pour un employeur d'installer des caméras de surveillance dans les locaux de l'entreprise, pour dissuader – officiellement- d'éventuels voleurs et 47% sont enclins à délivrer des infos personnels pour disposer d'une carte de fidélité.
Alors que, paradoxalement, 55% des personnes interrogées sont réticentes à l'idée d'utiliser au sein de leur foyer un thermostat connecté, susceptibles de relayer auprès de prestataires des informations sur les us et coutumes d'une maisonnée.



En outre, les Américains sondés sont aussi réfractaires aux sollicitations que ne leur « rapportent » rien en échange : ils n'apprécient ainsi que très peu les envois de spams et les demandes de contacts intempestives qui arrivent après avoir partagé avec une entreprises des données personnelles.
Les plus réfractaires au partage d'informations privées mettent surtout en exergue le fait qu'ils ne sont pas tenus au courant des types d'entreprises qui ont accès à ces données. L'anonymisation ne se fait qu'en un seul sens…
Ils s'interrogent aussi sur intentions qui motivent ce type d'entrepris, ravivant ainsi une certaine peur du « Big Brother ».

Crédit image : Gajus – Shutterstock.com

Réagissez à cet article

Source : *Données personnelles : les Américains sont prêts à faire des concessions | ITespresso.fr*

Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros

	Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros

Les députés de la commission des lois ont renforcé cette semaine les attributions de la Commission nationale de l'informatique et des libertés (CNIL), mais n'ont pas augmenté le montant des amendes pouvant être infligées par l'institution.

Le pouvoir de réprimande de la CNIL, qui peut actuellement prononcer des sanctions pécuniaires de 150 000 euros maximum en cas de premier manquement, c'est « cacahuète », dixit Axelle Lemaire ! Pour autant, l'intéressée s'est opposée dans le cadre de l'examen du projet de loi numérique à revoir ce niveau de sanctions… La secrétaire d'État au Numérique a en effet émis un avis défavorable sur les amendements visant à relever ce plafond (de 20 millions à 100 millions d'euros, selon les propositions des parlementaires).
En cause ? L'adoption imminente du règlement européen sur les données personnelles, sur lequel les institutions européennes sont parvenues à un accord fin 2015. « *La logique qui est poursuivie par le gouvernement jusqu'à présent, c'est de n'anticiper cette entrée en vigueur du texte européen que lorsqu'une marge de manœuvre est laissée à l'État membre. Ce n'est pas le cas en l'occurrence, même si je comprends tout à fait l'objectif posé par ces amendements* », s'est justifiée Axelle Lemaire. Le problème est surtout que le règlement n'a pas encore été officiellement traduit en français, ce qui ne permet pas de graver dès aujourd'hui dans le marbre des dispositions dont le législateur ne peut être certain qu'elles seront conformes au règlement européen…

« Marquer le coup maintenant face à des gens qui se gavent toujours plus chaque mois »

Pour certains députés, à l'instar de Philippe Gosselin (Les Républicains) et Isabelle Attard (Écologiste), la France aurait pourtant intérêt à anticiper l'entrée en vigueur du règlement – qui sera d'application directe mais sous deux ans à compter de l'adoption définitive du texte. « *Je pense que c'est important de marquer le coup maintenant face à des gens qui se gavent toujours plus chaque mois* » a ainsi plaidé l'élue du Calvados, reprenant une demande de la CNIL elle-même.

Crédits : Assemblée nationale

Invités par la secrétaire d'État au Numérique à retirer leurs amendements, les députés Gosselin, Attard et Martin-Lalande n'ont pas plié, Axelle Lemaire ne leur ayant donné que trop peu de gages. « *Je peux prendre l'engagement de tenter d'avancer sur ce sujet, sans vous assurer d'avoir une rédaction propre et définitive qui arrive dans quelques jours* [pour les débats en séance publique, ndlr]. *Je crois que les amendements que vous avez déposés ont le mérite de poser cette question. Si elle n'est pas suffisamment mûre à l'Assemblée nationale, elle aura peut-être mûri au Sénat, notamment parce que la traduction officielle sera disponible à ce moment-là* » a-t-elle déclaré, expliquant qu'un amendement gouvernemental sur ce sujet devrait être préparé en interministériel, notamment avec l'appui de la Chancellerie.
Tous leurs amendements ont cependant été rejetés (87, 265 et 454).

Vote de la saisine parlementaire de la CNIL, publicité de ses avis…

D'autres amendements concernant la CNIL ont en revanche été adoptés. L'autorité administrative pourra par exemple être consultée par le président de l'Assemblée nationale ou du Sénat sur une proposition de loi, sauf si le parlementaire à l'origine du texte s'y oppose. La gardienne des données personnelle est également autorisée à saisir l'ARCEP sur toute question relevant de sa compétence, et inversement.
Les amendements rendant obligatoire la publication des avis de la CNIL sur les projets de loi, alors que l'institution ne le fait aujourd'hui que sur demande du président de la commission des lois du Sénat ou de l'Assemblée nationale, ont d'autre part été votés. Il en ira de même pour les délibérations portant sur des décrets ou arrêtés pour lesquels la loi prévoit un avis de la gardienne des données personnelles.

Réagissez à cet article

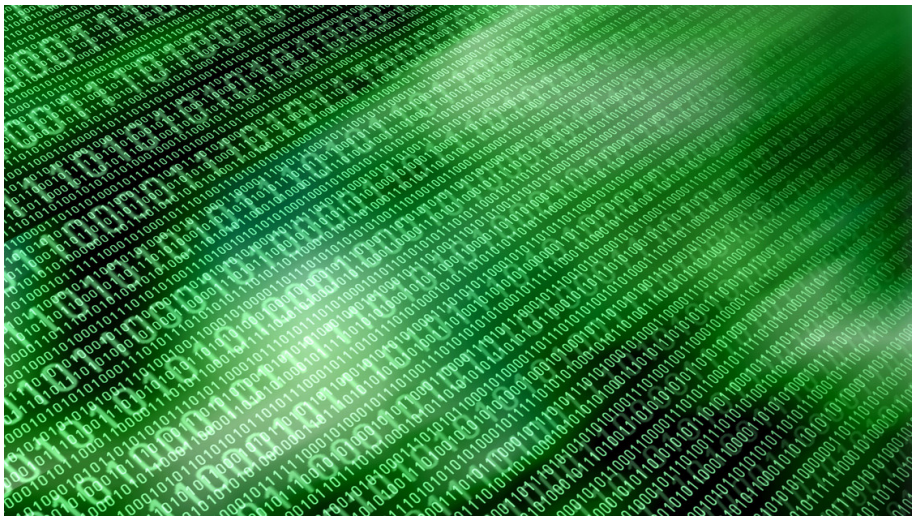
Source : *Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros | Tech24*

Le département des Alpes Maritimes salué par la CNIL pour sa politique

départementale de sécurité des données personnelles

Le département des Alpes Maritimes salué par la CNIL pour sa politique départementale de sécurité des données personnelles

Le Département des Alpes-Maritimes ,1er organisme français à obtenir le Label Gouvernance Informatique et Libertés de la CNIL.



Le Département a depuis longtemps intégré le numérique comme nouvelle dimension de la vie de l'usager. Il s'est ainsi engagé formellement dans le respect du droit des personnes au travers de la mise en oeuvre d'un cadre de confiance autour de l'économie numérique en établissant une politique de gestion des données à caractère personnel. Un engagement récompensé au niveau national pour la première fois en France.
Le 22 octobre 2015, la CNIL a délivré au Département des Alpes-Maritimes le premier Label Gouvernance Informatique et Libertés tous secteurs confondus. L'obtention de ce label vient récompenser le travail des services départementaux, ainsi que l'attachement éthique du Département à la protection des données relatives aux usagers ou à celles de ses agents.
Cette distinction et les bonnes pratiques qui en découlent, illustrent ainsi, à juste titre, le comportement responsable et loyal que la collectivité a engagé en matière de réalisation et d'exploitation des données à caractère personnel.
Le Lab 06 a ouvert ses portes le 25 septembre 2015 au cœur du Centre administratif départemental. Il incarne la volonté du Département des Alpes-Maritimes de s'engager davantage dans la voie de la transformation numérique avec la création de #E-zy06 dont l'ambition est d'offrir un service public encore plus accessible quelle qu'en soit la modalité : physique, téléphonique ou numérique.
L'objectif est de faire des Alpes-Maritimes un département pionnier dans le numérique, capable d'apporter le plus grand service aux usagers.

Réagissez à cet article

Source : *La politique départementale de sécurité des données personnelles saluée par la CNIL – Département des Alpes-Maritimes*

Comment protéger les données de vos enfants des pirates informatiques

Comment protéger les données de vos enfants des pirates informatiques

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Après l'annonce du piratage début novembre de VTech, le leader mondial des tablettes ludo-éducatives, c'est maintenant au tour d'Hello Kitty d'être accusée de mal sécuriser les données de ses utilisateurs. Pendant près d'un mois, les données personnelles de 3,3 millions de membres de la communauté en ligne du fabriquant japonais Hello Kitty (dont, évidement, beaucoup d'enfants) auraient été exposées en raison d'une faille de sécurité.

A quelques jour de Noël, ces deux affaires montrent clairement à quel point il est facile aujourd'hui pour les hackeurs de dérober des informations sensibles.Et aussi le danger qui peut en découler, comme le rappelle à metronews la Commission nationale de l'informatique et des libertés (CNIL) : « Nous constatons que certains secteurs industriels ajoutent une connectivité à leurs produits sans disposer historiquement d'une culture en sécurité informatique ».

► Vérifiez si votre mail est piraté
Il existe un moyen simple de savoir si votre adresse mail a été touchée. Pour cela, il faut se rendre sur le site haveibeenpwned.com. Entrez votre adresse mail, puis cliquez sur « pwned ? » pour lancer la recherche.
► Changez votre mot de passe
Par précaution, il est recommandé aux utilisateurs des services qui ont connu des intrusions de ce genre de changer leurs mots de passe. « Il doit être composé d'au moins 3 types de caractères différents parmi les quatre types de caractères existants : majuscules, minuscules, chiffres et caractères spéciaux ». Pour en savoir plus, rendez-vous sur le site de la CNIL.
► Ne communiquez que le minimum d'infos
Pour les enfants (et leurs parents), la CNIL recommande ainsi d'utiliser des pseudonymes sur les services en lignes, et de ne communiquer que le minimum d'informations. Par exemple, saisissez une date de naissance au 1er janvier si le système a besoin d'une indication de tranche d'âge.
► Veillez à bien lire les conditions d'utilisation
Outre les risques de sécurité révélés par la faille VTech, les parents doivent être vigilants concernant les possibilités de réutilisation des données collectées (profilage publicitaire) et s'assurer de la possibilité d'y accéder et de les supprimer.

Réagissez à cet article

Source : *Piratages VTech et Hello Kitty : comment protéger les données de vos enfants – metronews*

Carte de paiement sans contact – Le client n’est pas toujours roi

Carte de paiement sans contact – Le client n’est pas toujours roi

---

Refuser les cartes bancaires équipées du paiement sans contact n’est pas toujours simple. Un client du Crédit agricole l’a appris à ses dépens.

En avril 2015, un adhérent de l’UFC-Que Choisir de Senlis saisit l’association locale de ses difficultés avec son agence du Crédit agricole de Rixheim (68). Celle-ci lui a adressé en renouvellement une carte bancaire Visa munie de la fonction paiement sans contact. Ayant lu dans Que Choisir que cette fonction n’était pas sans faille, ce consommateur demande à sa banque le remplacement de sa carte par une même carte Visa mais sans cette nouvelle fonction. Refus de son agence, puis de la direction régionale du Crédit agricole qui affirme que c’est impossible et lui propose en échange soit une carte Visa avec débit différé, soit un autre type de carte bancaire. Pas d’accord, le particulier fait part de ce blocage à l’association locale de l’UFC-Que Choisir de Senlis.

Client à la porte

L’intervention de cette dernière auprès de la banque n’aura pas plus de succès. Face à un tel refus, elle saisit la Cnil (Commission nationale de l’informatique et des libertés) au motif que le Crédit agricole viole une de ses recommandations qui impose aux banques d’offrir à leurs clients la possibilité de refuser la fonction paiement sans contact.

La Cnil rejette la plainte de l’association locale, déclarant ne pas pouvoir imposer aux banques un changement de carte à l’identique mais rappelle que le particulier a la possibilité de faire désactiver la fonction.

Fort de cette réponse, le consommateur demande à son agence cette désactivation.

Pour toute réponse, la banque a mis son client à la porte, le sommant de restituer tous ses moyens de paiement. La Cnil a été avertie d’un tel comportement.

Réagissez à cet article

Source : *Carte de paiement sans contact – Le Crédit agricole a la main leste – UFC Que Choisir*