Avec Apple, les données des collégiens migrent aux Etats-Unis

	Avec Apple, les données des collégiens migrent aux Etats-Unis

La gestion de certains iPads des collégiens des Hauts de Seine est confiée à Apple School Manager, qui stocke les données aux États-Unis. Et cela inquiète.

En septembre 2016, le Conseil Départemental des Hauts de Seine annonçait la signature d'une convention passée avec l'Etat pour « les Collèges numériques et l'innovation pédagogique », s'inscrivant dans le Plan National Numérique de l'Etat. Cet accord prévoit, pour l'année scolaire 2016/2017, la distribution de 4500 tablettes dans différents collèges du département. Coût de l'opération : 3,1 millions d'euros dont 991 000 € cofinancés par l'Etat, soit 2,1 millions d'euros à la charge du département.
Après un appel d'offres, c'est Apple et ses iPad qui ont été choisis par l'assemblée départementale. Dans certains cas, ce déploiement se fera sur la base d'une mutualisation, c'est-à-dire qu'une tablette pourra servir à plusieurs élèves ou enseignants. Pour gérer cette mutualisation, Apple propose un outil de gestion nommé School Manager. Sur le site de la firme, on apprend que la solution permet de « *créer automatiquement des identifiants Apple gérés pour tous les élèves et le personnel, configurer les réglages d'inscription des appareils et acheter et distribuer facilement apps, livres et supports pédagogiques* ».

Des données stockées aux Etats-Unis

Oui mais voilà, ce service inquiète. En effet, « *le service Apple School Manager comporte des données à caractère personnel, relatives aux élèves et aux enseignants, qui sont hébergées sur le territoire des Etats-Unis* », peut-on lire dans une lettre du recteur de l'Académie de Versailles. Toujours sur le site d'Apple, un document relatif à « *la confidentialité des données des établissements scolaires* » souligne, dans un paragraphe sur le transfert des données à l'international : « *avec Apple School Manager, les identifiants Apple gérés, iTunes U et iCloud, les données personnelles peuvent être stockées ailleurs que dans leur pays d'origine. Où que les données soient stockées, elles sont assujetties aux mêmes normes et exigences rigoureuses en matière de stockage des données*. » Et de préciser que le transfert transatlantique des données est soumis au Safe Harbor (invalidé en octobre 2015) ou à ses successeurs, en l'occurrence le Privacy Shield (déjà contesté). Ainsi, que par « *les clauses contractuelles types de l'UE/l'Accord de Transmission à l'étranger de la Suisse, qui ont été ajoutés à l'Accord Apple School Manager* ».
Face à cette problématique de localisation des données, le rectorat explique qu'Apple School Manager doit faire l'objet « *d'une déclaration normale auprès de la CNIL et d'une information auprès des usagers* ». Au nom de l'autonomie des établissements, c'est donc aux principaux des Collèges concernés de faire cette déclaration auprès de la CNIL.

Les Hauts de Seine temporisent

Nous avons sollicité l'avis des différents protagonistes dans cette affaire. En premier lieu, le Conseil Départemental des Hauts de Seine se dit conscient du problème : « *dans le cadre du Plan numérique national des collèges, le Département des Hauts-de-Seine a remis à ce jour 3 568 tablettes personnelles à des collégiens et professeurs, sur les 4 500 prévues sur l'année scolaire 2016/2017. Le logiciel Apple School Manager n'est donc actuellement pas utilisé, puisque seules les tablettes mutualisées sont concernées par cette problématique qui retient toute l'attention du Département.* »
Il ajoute que « *les 932 tablettes restantes, qui seront mutualisées, seront remises après qu'une solution définitive soit trouvée* » (sic). Cette dernière phrase montre que la solution Apple School Manager n'est pas encore mise en œuvre et que des solutions alternatives pourraient être envisagées comme des outils de MDM (Mobile Device Management)…[lire la suite]

Réagissez à cet article

Source : *Avec Apple, les données des collégiens migrent aux Etats-Unis*

La CNIL face au compte à rebours de la nouvelle loi européenne

La CNIL face au compte à rebours de la nouvelle loi européenne

---

La Commission nationale de l'informatique et des libertés doit préparer l'application, en mai 2018, du nouveau règlement européen sur les données personnelles. Le temps presse.

De l'aveu de sa présidente, Isabelle Falque-Pierrotin, l'année 2016 a été *« intense »* pour la Commission nationale de l'informatique et des libertés (CNIL). La présidente de l'instance chargée de la protection des données personnelles en a donné la mesure, lundi 27 mars lors de la présentation de son rapport annuel, en égrenant les principaux dossiers qui ont concerné l'institution lors de l'année passée : adoption du nouveau règlement européen sur les données personnelles ; actions lancées contre plusieurs géants du Net ; débat sur le chiffrement ; loi pour la république numérique ; polémique autour du fichier biométrique TES ; début des processus électoraux…
Ce surcroît d'activité ne s'est cependant pas traduit dans le nombre de procédures traitées par la Commission. En 2016, elle a reçu plus de 7 703 plaintes, un peu moins que l'année précédente (7 908), procédé à 430 contrôles (501 en 2015), prononcé 82 mises en demeure (93 en 2015) et infligé 13 sanctions dont 4 financières (10 en 2015).
C'est plutôt du point de vue législatif que l'année 2016 a été chargée, marquée par l'adoption de *« trois textes qui bouleversent la protection des données personnelles »* dans le sens d'*« une plus grande maîtrise de leurs données par les individus »*, a expliqué Mme Falque-Pierrotin.

Le défi du règlement européen

La loi pour une république numérique a été publiée au *Journal officiel* le 7 octobre, et l'accord Privacy Shield est entré en vigueur, après de longues négociations, le 1er août. Mais c'est surtout l'adoption définitive, en mai, du nouveau règlement européen sur les données personnelles qui a constitué, selon Mme Falque-Pierrotin, *« une étape majeure pour la protection des données personnelles en Europe »*. Ce règlement institue notamment des sanctions plus importantes pour les entreprises, de nouveaux droits pour les citoyens et une meilleure coordination des autorités de protection des données. Il nécessite à la fois des adaptations de la part des entreprises, mais aussi un travail législatif au niveau français pour toiletter la loi informatique et libertés de 1978. Le temps presse : le règlement s'appliquera dès le 25 mai 2018. *« 2017, c'est la cote d'alerte »*, a ainsi prévenu Mme Falque-Pierrotin.
Les entreprises *« doivent se mettre en marche »* pour se conformer au règlement, a-t-elle expliqué, insistant sur le rôle d'accompagnement de la Commission. Consciente de l'effort requis, elle a tenté de rassurer : *« Nous sommes convaincus qu'il n'y a pas d'innovation sans protection des données personnelles »* : *« Il est possible d'innover et que, loin de la contraindre, la protection des données permet de développer l'innovation. »*
Autre obstacle de taille, législatif cette fois : pour être appliqué dès le mois de mai 2018, la nouvelle loi informatique et liberté *« devra être déposée en conseil des ministres avant l'été »*. *« Pour le moins délicat »*, a euphémisé Mme Falque-Pierrotin…[lire la suite]
Téléchargez le rapport annuel 2016

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *En 2017, la CNIL face au compte à rebours de la nouvelle loi européenne*

Data Protection Officer : Qui seras-tu ?

Data Protection Officer : Qui seras-tu ?

Dès la mi-2018, la nouvelle directive européenne baptisée GDPR est appelée à remplacer les dispositions de la Loi Informatique et Libertés. Celle-ci va rendre obligatoire la nomination d'un DPO (Data Protection Officer) dans de nombreuses organisations pour lesquelles la protection des données représente un enjeu majeur. Selon l'étude « CIO Concern Management » de Janco Associates, la sécurité arrive en tête des préoccupations des DSI à hauteur de 68%. De la même manière, les fuites de données observées chez des majors du Web et largement relayées dans les médias ont participé à construire ce climat anxiogène.

Pour être efficace, un DPO doit considérer les deux fonctions principales de sa mission que sont la protection des données personnelles et la protection de la confidentialité des données.
La protection des données personnelles fait appel à des exigences en termes de moyens et processus à mettre en œuvre qui peuvent être très variables d'un pays à l'autre. Dans un contexte de développement à l'international, le DPO sera un soutien précieux afin d'appréhender les différents aspects réglementaires.
La protection de la confidentialité des données est quant à elle un peu plus poussée puisqu'il s'agit de garantir que chaque donnée soit protégée à hauteur de ses enjeux pour l'entreprise. Autrement dit, ce n'est plus la loi mais le client qui fixe les règles !
Toutes les données informatiques n'ont pas la même valeur. Une plaquette commerciale où le plan détaillé d'un prototype en cours de conception n'auront pas le même effet s'ils se retrouvent révélés. Le DPO doit donc, avec son client, mesurer le risque de divulgation de chaque donnée et son impact pour l'entreprise. De données « publiques » à « très secrètes », il doit être capable de garantir au client que ses exigences soient remplies en termes de sécurité… et même si l'on met en place assez facilement des méthodes de chiffrements sur les disques, cela ne résout pas tout !
La plus grande faille sécuritaire qu'il puisse exister réside finalement dans l'humain lui-même. Pour être totalement rassuré quant à la confidentialité de ses données, le client doit être certain que même les équipes système de son prestataire ne puisse pas les lire…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Data Protection Officer : Qui seras-tu ? – Global Security Mag Online*

Développement de l'outil PIA (Privacy Impact Assessment, étude d'impact sur la vie privée) de la CNIL

Développement de l'outil PIA (Privacy Impact Assessment, étude d'impact sur la vie privée) de la CNIL

Date remise des offres: Mercredi, 29 mars, 2017…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation

Professionnelle n°93 84 03041 84).
Plus d’informations sur notre page formations.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

RGPD : Ce qui va changer pour les professionnels de santé

RGPD : Ce qui va changer pour les professionnels de santé

Fin des déclarations Cnil, demandes de consentement et sanctions renforcées, une nouvelle réglementation européenne* va venir chambouler la gestion des données personnelles en magasin. En tant que commerçants et professionnels de santé, vous collectez et transmettez des données relatives à vos clients. Le GDPR (General Data Protection Régulation) devra donc s'appliquer à votre point de vente. Zoom sur ce qui change dès le 25 mai 2018.

Registre des traitements et désignation d'un délégué à la protection des données

Quotidiennement vous gérez, stockez et envoyez les données de santé de vos clients que ce soit pour la pratique du tiers payant ou effectuer une commande auprès de vos fournisseurs. Identité, numéro de Sécurité sociale, facturation, prescription… vous êtes amenés à traiter des données personnelles, qui doivent actuellement faire l'objet d'une déclaration auprès de la Cnil (Commission nationale de l'informatique et des libertés). Mais bientôt, vous n'aurez plus besoin de cette formalité préalable.

En effet, le règlement européen sur la protection des données personnelles repose sur une logique de conformité, dont les acteurs seront désormais responsables. En d'autres termes, le poids de la procédure administrative va être transféré de la Cnil. **Dès le 25 mai 2018, vous devrez être en possession et tenir un « registre des traitements mis en œuvre ».** Ce dernier devra notamment spécifier :

- les catégories de données traitées ;
- la finalité ;
- les différents destinataires ;
- la durée de conservation.

« Ce registre informatisé permettra au professionnel de se ménager des preuves vis-à-vis de la Cnil. Il prouve son adhésion à un code de conduite, explique Maître Cécile Vernudachi, avocate au Barreau de Paris. Les grandes enseignes pourront également désigner un délégué à la protection des données, qui deviendra le point de contact avec la Cnil et un véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Dans les plus petites structures, ce ne sera pas une obligation », précise-t-elle.

Consentement renforcé et transparence

Le règlement européen impose également la mise à disposition d'une information claire, intelligible et aisément accessible à vos clients. Il définit en ce sens l'expression du consentement : « **les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer.** La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe », précise le document.

En d'autres termes, avant chaque devis ou chaque vente, vous êtes tenus d'obtenir le consentement de votre porteur pour pouvoir traiter et transmettre ses données personnelles. « Concernant la correction, seul le patient peut donner son accord pour la transmission de cette donnée, souligne Maître Vernudachi. **Son consentement doit obligatoirement être écrit.** Dans le cadre de l'exécution d'un contrat, il n'y a alors plus de restriction. Toutefois, il est interdit d'utiliser cette information pour la vendre à un tiers ou à des fins marketings et commerciales ».

Spécificité pour les moins de 16 ans :

Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Des sanctions encadrées et graduées

Les responsables de traitement, autrement dit les dirigeants ou chef d'entreprise, les plateformes de services et les complémentaires santé, peuvent enfin faire l'objet de **sanctions administratives importantes en cas de non-conformité au nouveau règlement**. Les autorités de protection peuvent notamment :

- prononcer un avertissement ;
- mettre en demeure l'entreprise ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des amendes dans le cas d'une entreprise, elles peuvent s'élever de 2% à 4% du chiffre d'affaires annuel mondial, en fonction de la catégorie de l'infraction.

Notons que selon l'étude « Crossing the Line » du cabinet KPMG**, les Français sont 2ème sur le podium des consommateurs les plus vigilants quant au traitement de leurs données personnelles. Aussi, le règlement européen sera en vigueur dès le 25 mai 2018. Il vous faut donc être vigilant et vous y préparer dès maintenant !

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

****étude publiée en novembre 2016***

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Ce qui va changer dans les magasins pour le traitement des données personnelles | Acuité*

Nouvelles tensions autour du Privacy Shield entre l'Europe et les USA

Nouvelles tensions autour du Privacy Shield entre l'Europe et les USA

Une coalition d'associations demande à la Commission européenne de suspendre le nouvel accord sur les données personnelles, intitulé Privacy Shield, si les États-Unis ne réforment pas leur politique en matière de renseignement.

Le rejet envers le Privacy Shield ne faiblit pas. Dans une lettre ouverte datée de mars, une coalition d'associations européennes et internationales, dont La Quadrature du Net, demandent aux États-Unis et à l'Union européenne de suspendre l'exécution de ce mécanisme juridique. L'accord transatlantique « *ne donne pas assez de garanties à la protection des données personnelles des Européens* » jugent-elles.
Le **Privacy Shield** est l'accord qui encadre les transferts des données personnelles vers les États-Unis. Il remplace l'ancien Safe Harbor que la Cour de justice de l'Union européenne a invalidé fin 2015 parce que les protections apportées par le droit européen n'étaient pas assurées aux USA.
La raison ? Les lois américaines sur le renseignement actuellement en vigueur outre-Atlantique. « *Au moment de l'adoption de cet accord, plusieurs groupes ont souligné que la loi américaine était inadaptée pour protéger les données des européens et ne satisfaisait pas le critère d'« équivalence substantielle » imposé par la Cour de justice de l'Union européenne* », écrivent les signataires.
Ils rappellent qu'ils « *ont à plusieurs reprises pointé du doigt les défauts présents dans les mécanismes américains de recours et de supervision des violations de la vie privée, les insuffisances dans les limitations de la collecte, l'accès et l'utilisation des données personnelles, et les incertitudes des garanties écrites* ». Pour toutes ces raisons, et sans action du côté américain, la suspension est l'unique solution.
« *Sans réelle réforme de la surveillance, nous pensons qu'il est de votre responsabilité, à défaut d'une meilleure option, de suspendre le Privacy Shield. Nous vous exhortons à clarifier ce positionnement pour vos homologues américains* » ajoutent les associations. Sinon, « *nous considèrerons cela comme un message fort envoyé à l'Union européenne déclarant que nos droits sont sans importance* ».

INQUIÉTUDE EN EUROPE

Les associations civiles ne sont pas les seules à s'alarmer des faiblesses du Privacy Shield. L'été dernier, le groupe de l'article 29 (G29), qui rassemble au niveau européen toutes les autorités de protection des données et de la vie privée, comme la Commission nationale de l'informatique et des libertés en France, a ainsi fait part de son inquiétude, après avoir critiqué le Privacy Shield dans un avis du 13 avril 2016…[lire la suite]

Réagissez à cet article

Source : *Privacy Shield : levée de boucliers contre l'accord sur les données personnelles entre l'Europe et les USA – Politique – Numerama*

Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr

Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr

---

Yahoo donne les détails des hacks qui ont touché plus d'un milliard de comptes, et en révèle un nouveau. Et la patronne se serait fait sucrer ses primes.

La crucifixion de **Yahoo** continue, et si ce n'est pas déjà fait, on ne peut que vous recommander à ce stade de supprimer votre éventuel compte Yahoo. Dans un communiqué, l'entreprise est revenue par le menu sur toutes les attaques qui ont gravement entaché la réputation de l'entreprise depuis 2014. On y apprend en prime que dernièrement, des hackers ont obtenu du code propriétaire de Yahoo et ont pu fabriquer de faux cookies.
Cela leur aurait permis d'accéder à 32 millions de comptes entre 2015 et décembre 2016. Sur cette masse, seuls 26 utilisateurs auraient été prévenus. L'entreprise explique également collaborer avec les autorités depuis que son enquête a révélé la possible implication de **hackers** soutenus par un état dans ces piratages. En tout, plus d'un milliard de comptes Yahoo ont été compromis depuis 2014…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

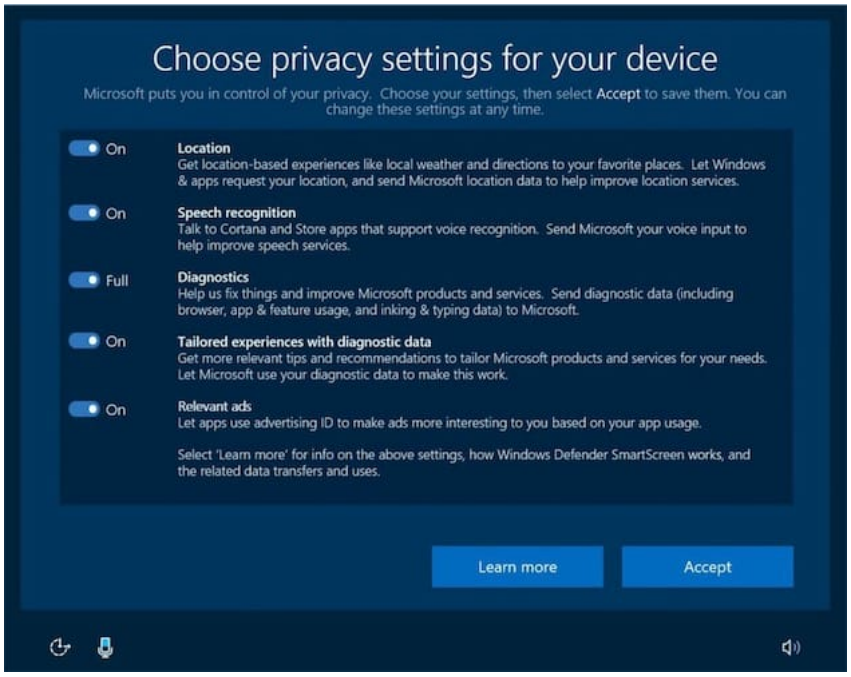
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

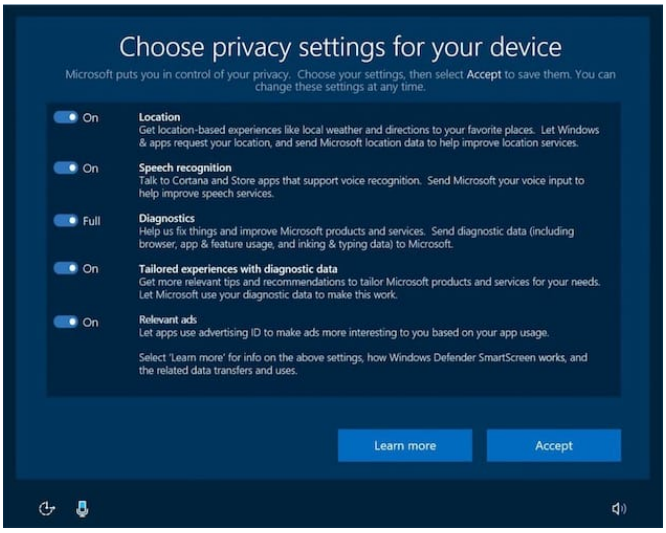
Source : *Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr*

Les CNIL européennes toujours insatisfaites de la politique de confidentialité de Windows 10



Les CNIL européennes toujours insatisfaites de la politique de confidentialité de Windows 10

En dépit des mesures annoncées par Microsoft, le groupement des autorités européennes de protection des données s'inquiète toujours de la politique de confidentialité de Windows 10, jugée trop évasive.
Reuters rapporte que le G29 a adressé un nouveau courrier à l'éditeur pour lui indiquer que les changements proposés n'étaient pas suffisants. Microsoft envisage de présenter cinq nouvelles options durant le processus d'installation pour limiter ou couper la collecte de données de localisation, reconnaissance vocale, diagnostics, recommandations et publicités ciblées.



Les nouveaux réglages de confidentialité proposés par Microsoft. Cliquer pour agrandir
« *Microsoft devrait clairement expliquer quels types de données personnelles sont exploitées et à quelles fins. Sans cette information, l'utilisateur ne peut pas être renseigné et, par conséquent, son consentement n'est pas valide* », insistent les CNIL européennes…[lire la suite]

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Les CNIL européennes toujours insatisfaites de la politique de confidentialité de Windows 10*

La commission de contrôle des élections veillera au ‘risque d’attaque informatique’

Saisir les autorités en cas de cyberattaque, veiller au respect du principe d'égalité entre les candidats à l'élection présidentielle… La Commission nationale de contrôle de la campagne a été installée ce soir au Conseil d'Etat par le ministre de la Justice.

La commission portera « une vigilance particulière au risque d'attaque informatique de la campagne », a déclaré le garde des Sceaux Jean-Jacques Urvoas. En décembre, l'Agence nationale de la sécurité des systèmes d'information (Anssi) et le Secrétariat général de la défense et de la sécurité nationale (SGDSN) avaient souligné « le risque de cyberattaque à motif politique », a rappelé Jean-Jacques Urvoas.

» Lire aussi : L'Élysée inquiet d'une cyber-menace étrangère pesant sur la présidentielle

« Si un candidat estime qu'il fait l'objet d'une attaque susceptible d'affecter le déroulement de sa campagne, il pourrait saisir la commission », a confirmé son président Jean-Marc Sauvé, à la tête du Conseil d'Etat. Mais il revient d'abord aux candidats et à leurs partis politiques de « mettre en oeuvre les solutions adéquates » pour y faire face, a-t-il toutefois précisé. Si une attaque devait être avérée, la commission – en lien avec le Conseil constitutionnel – demanderait des investigations…[lire la suite]

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;

• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *La commission de contrôle des élections veillera au ‘risque d’attaque informatique’*

Les collectivités territoriales cibles des Pirates Informatiques

Les collectivités territoriales cibles des Pirates Informatiques

---

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

FOCUS

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

À LIRE AUSSI
• Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

À LIRE AUSSI
Notre dossier : Données personnelles, un gisement sous haute protection

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*